opentext™

OpenText™ ScanCentral DAST

Software Version: 26.4.0
Linux® operating systems

Configuration and Usage Guide

Document Release Date: November 2026
Software Release Date: November 2026

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2020-2026 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Trademark Notices

“OpenText” and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

Documentation updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on November 03, 2026.

Contents

Preface 30
Contacting Customer Support 30
For more information 30
Product feature videos 30

Change log 31

Chapter 1: Introduction 39
Options for deployment 39
Audience 39
Documentation scope 39
Product name changes 40
What is ScanCentral DAST? 40
Application Security 41
Kafka 41
LIM 41
ScanCentral DAST API 41
ScanCentral DAST Utility Service 42
ScanCentral DAST Global Service 42
ScanCentral DAST database 43
Fortify DAST sensor 43
Core components 44
ScanCentral DAST with two-factor authentication 44
2FA Server 44
Installation recommendation 45
2FA Server versions 45
Permissions in Application Security 45
Tasks requiring Universal access permissions 46
Aviator permissions 46
Configuration checklist 47
Related documents 49
All products 49
ScanCentral DAST 50

Application Security 50
Fortify DAST 51

Chapter 2: Manually configuring the ScanCentral DAST environment 53
Installation best practices 53
Important information about SSL 53
Requesting access to Fortify Docker repository 53
Before you begin 54
Understanding the installation process 54
Upgrading ScanCentral DAST 56
Requirements for upgrading 58
Recommendation for upgrading 58
Effect of upgrades on scheduled scans 58
Order of orchestration 58
ScanCentral DAST database 59
ScanCentral DAST API 59
ScanCentral DAST Utility Service 59
ScanCentral DAST Global Service 60
ScanCentral DAST Sensor Service 60
Setting up Docker 60
Creating and using a settings file 60
Using special characters in YAML files 61
Placeholder text in setting samples 61
Database settings 61
Configuring a DBO-level account 62
Configuring a standard account 62
JSON example 62
YAML example 63
Parameter descriptions 63
Miscellaneous ScanCentral DAST settings 66
JSON example 66
YAML example 67
Parameter descriptions 68
72
SSC settings 72
Important guidelines for the service account 72
JSON example 73
YAML example 73

Parameter descriptions ... 74
ScanCentral DAST API settings ... 76
JSON example ... 76
YAML example ... 76
Parameter descriptions ... 77
LIM settings ... 78
JSON example ... 78
YAML example ... 78
Parameter descriptions ... 78
Utility Service settings ... 79
JSON example ... 80
YAML example ... 80
Parameter descriptions ... 80
Environment settings ... 80
Using a proxy ... 80
JSON example ... 81
YAML example ... 81
Parameter descriptions ... 81
Known issue with host name, machine name, and container name ... 83
SecureBase settings ... 83
JSON example ... 83
YAML example ... 84
Parameter descriptions ... 84
Client-side library analysis and Debricked settings ... 85
NVD information ... 85
Debricked health metrics ... 85
Debricked content contingent upon access ... 85
Configuring access to Debricked ... 85
JSON example ... 86
YAML example ... 86
Fortify Connect server settings ... 86
JSON example ... 86
YAML example ... 87
Parameter descriptions ... 87
JSON sample file ... 89
YAML sample file ... 91
Using the Configuration Tool CLI ... 93
Versions available ... 93
About the images on DockerHub ... 93
Deciding which Configuration Tool CLI to use ... 94

Using the executable file ... 94
Locating the EXE file ... 94
Launching the CLI ... 94
Using the Configuration Tool CLI ... 95
Accessing the help ... 95
Using the Configuration Tool CLI Docker image ... 95
Getting the image from DockerHub ... 95
Running the container ... 95
Understanding the Docker CLI options ... 97
Exporting an existing settings file ... 97
Understanding the createSettingsFile command ... 97
Configuring the environment ... 99
Before you begin ... 99
Understanding the configureEnvironment command ... 99
Applying updated settings to containers ... 100
Using environment variables ... 100
How replacement works ... 100
Format and usage ... 100
Encrypting values ... 101
Generating a migration script ... 101
Migration script name ... 101
Understanding the generateMigrationScript command ... 102
Generating a connection string ... 103
Understanding the generateConnectionString command ... 103
Understanding the Docker compose and environment files ... 105
Versions available ... 105
Configuring the TLS environment file for core components ... 106
Database/datastore settings ... 106
Fortify DAST sensor API settings ... 107
ScanCentral DAST API settings ... 107
ScanCentral DAST Utility Service settings ... 108
Optional Fortify Connect settings ... 109
Configuring the TLS environment file for the scanner service ... 109
Datastore setting ... 110
Two-factor authentication setting ... 110
Generating a 2FA master token ... 110
Fortify DAST sensor API settings ... 111
ScanCentral DAST scanner service settings ... 111
Configuring the mTLS environment file for core components ... 112
Database/datastore settings ... 112

Fortify DAST sensor API settings ... 113
ScanCentral DAST API settings ... 113
ScanCentral DAST API mTLS certificate settings ... 114
ScanCentral DAST Utility Service settings ... 116
ScanCentral DAST Utility Service mTLS certificate settings ... 117
Shared client certificate settings ... 118
Optional Fortify Connect settings ... 120
Configuring the mTLS environment file for the scanner service ... 120
Datastore setting ... 120
Two-factor authentication setting ... 121
Generating a 2FA master token ... 121
Fortify DAST sensor API settings ... 121
ScanCentral DAST scanner service settings ... 122
Shared client certificate settings ... 122
Using the TLS compose file for core components ... 123
Using the compose file ... 123
Using the TLS compose file for the sensor ... 124
Using the compose file ... 124
Using the mTLS compose file for core components ... 125
Using the compose file ... 125
Using the mTLS compose file for the sensor ... 126
Using the compose file ... 126
Using Fortify DAST with the sensor service ... 127
Important information about licenses ... 127
Important prerequisite ... 127
Enabling composite settings in Fortify DAST ... 128
Configuring the Fortify DAST REST API ... 128
Installing and configuring the DAST sensor service ... 130

Chapter 3: Understanding the user interface ... 132
ScanCentral DAST user interface ... 132
Hiding the navigation menu ... 133
Showing the navigation menu ... 133
Scan visualization ... 134
Resizing the display areas ... 135
Hiding and showing a display area ... 135
Working with tables ... 136
Customizing table views ... 136

Updating or creating a view 137
Selecting a different view 137
Managing columns in tables 137
Rearranging the columns 137
Adding and removing columns 138
When new columns are available 138
Understanding basic filters in tables 139
Guidelines 139
Using basic filters in tables 139
Accessing the basic filter feature 140
Filtering by Application, Version, Name, or URL 140
Filtering by date, scan status, publish status, or scan type 140
Clearing the filter 141
Understanding advanced filters in tables 142
Understanding the operators 142
Understanding conditions and field filters 143
Using advanced filters in tables 143
Accessing the advance filter feature 143
Creating an advanced filter 143
Editing an advanced filter condition 144
Removing an advanced filter condition 144
Clearing filters 145
Sorting data in columns 145
Known issue with sorting 146
Sorting directly in the table 146
Sorting in the table preferences panel 147
Searching in input boxes 147
Clearing data from input boxes 147
Viewing content on multiple pages 148
Changing the number of items displayed 148
Navigating multiple pages 148
Changing the number of items displayed in the table preferences panel 149

Chapter 4: Configuring a scan 150
What is a scan? 150
Important consideration about API definition files 150
Important information about gRPC proto files 150

Known limitations of gRPC scans ... 151
Preparing your system for audit ... 151
Sensitive data ... 151
Firewalls, anti-virus software, and intrusion detection systems ... 151
Effects to consider ... 152
Helpful hints ... 152
Accessing scan settings configuration from Application Security ... 153
Accessing from the DAST Scans list ... 154
Accessing from the Settings List ... 154
Restricting or allowing edits ... 154
What's next? ... 154
Using key stores in settings ... 155
Guidelines for Key Store Usage ... 155
Using a Key Store Placeholder ... 155
Viewing, clearing, or replacing the key store entry value ... 156
Manually editing a key store placeholder in settings ... 156
What's next? ... 157
Using artifacts from a repository in settings ... 157
Navigating in the repository ... 158
What's next? ... 158
Getting started ... 159
What's next? ... 161
Configuring a standard scan ... 161
What’s next? ... 164
Configuring a workflow-driven scan ... 164
Types of macros supported ... 164
Configuring a workflow-driven scan ... 164
What’s next? ... 167
Configuring an API scan ... 167
What’s next? ... 173
Configuring proxy settings ... 173
What's next? ... 175
Configuring authentication for standard and workflow-driven scans ... 175
Configuring site authentication ... 175
Using Aviator for login macro creation ... 176
Validating the login macro ... 177
Downloading the Macro Recorder tool ... 177
Using a client certificate ... 178

Configuring network authentication ... 178
Configuring OAuth 2.0 bearer credentials ... 179
What's next? ... 181
Configuring authentication for API scans ... 181
Using a client certificate ... 181
Configuring network authentication ... 181
Fetching a token value ... 183
Configuring OAuth 2.0 bearer credentials ... 184
Downloading the Macro Recorder tool ... 185
Using custom headers ... 186
Configuring SOAP settings ... 186
What's next? ... 188
Configuring scan details ... 188
What's next? ... 188
Configuring API content and filters ... 188
Specifying the preferred content type ... 189
Defining specific operations to include ... 189
Defining specific operations to exclude ... 189
Editing specific operations ... 190
Removing specific operations ... 190
Defining parameter rules ... 190
Editing a parameter rule ... 192
Removing a parameter rule ... 192
Understanding parameter type matches ... 193
Adding and managing allowed hosts ... 194
Adding allowed hosts ... 194
Editing or removing allowed hosts ... 195
Configuring scan priority ... 195
Changing the priority ... 195
Understanding advanced scan prioritization ... 196
Priority and sensor pools ... 196
Priority and scan status ... 196
Priority and sensors ... 197
When advanced scan prioritization is disabled ... 197
Configuring data retention ... 198
Scanning single-page applications ... 198
The challenge of single-page applications ... 198
Configuring SPA support ... 198
Enabling traffic monitor ... 199
Option must be enabled ... 199

Enabling traffic monitor logging ... 199
Creating and managing basic exclusions ... 199
Creating exclusions ... 200
Exclusion examples ... 201
Editing or removing exclusions ... 201
Understanding and creating inclusive exclusions ... 201
Understanding inclusive exclusion regular expressions ... 202
Example one ... 202
Example two ... 203
Configuring redundant page detection ... 204
Enabling SAST correlation ... 205
Reviewing scan settings ... 205
Saving the settings to Application Security ... 206
Scheduling a scan ... 206
Running a scan ... 207
Using the scan settings in the DAST API ... 208
Accessing the DAST API Swagger UI ... 209
Using the Swagger UI ... 209
Conducting an automated scan with FAST ... 209
Automation overview ... 210
FAST versions available ... 210
Using the FAST Windows version ... 210
Installation recommendation ... 210
Before you begin ... 210
Process overview ... 210
Downloading the FAST installer ... 212
Understanding the FAST options for Windows ... 212
Using the FAST Linux version ... 213
Options for accessing your functional tests ... 213
Process overview ... 214
Pulling the FAST image ... 215
Running the FAST container ... 215
Stopping the container ... 216
Understanding the run command options ... 217

Chapter 5: Working with Advanced scan settings ... 219
Accessing the Advanced settings view ... 219
Searching for a setting ... 219
Using advanced settings in the API ... 220

Facts about using advanced settings in the API 220
Searching for settings to use in the API 221
Getting default advanced setting values 221
Configuring method settings 222
Configuring the Crawl and Audit Mode 222
Configuring the crawl and audit details 223
Configuring general settings 224
Configuring Scan Details 224
Configuring Crawl Details 226
Configuring tag attributes 229
Adding tag attributes 230
Editing existing tag attributes 230
Deleting a tag attribute 230
Configuring JavaScript settings 230
Configuring requestor settings 231
Using a shared requestor 232
Using separate requestors 232
Configuring Requestor Settings 232
Configuring Connectivity Settings 233
Configuring response codes 234
Adding response codes 235
Editing existing response codes 235
Deleting a response code 235
Configuring session exclusions 236
Session exclusions for scan settings, crawl settings, and audit Settings 236
Rejecting versus excluding 236
Adding a file extension exclusion 237
Adding a host exclusion 238
Adding a URL exclusion 238
Adding a MIME-type exclusion 238
Editing existing session exclusions 239
Deleting a session exclusion 239
Configuring HTTP parameters used for state 239
Understanding HTTP parameters used for state 239
Adding HTTP parameters used for state 240
Editing an existing HTTP parameter 240
Deleting an HTTP parameter 241
Enabling CSRF 241
Understanding CSRF 241

Using CRSF tokens ... 242
Enabling CSRF ... 242
Configuring URL expressions for determining state ... 242
Enabling URL expressions for determining state ... 242
Adding a URL expression ... 242
Editing existing URL expressions ... 243
Deleting a URL expression ... 243
Configuring response state rules ... 243
Enabling response state rules ... 243
Adding a response state rule ... 244
Editing an existing rule ... 245
Deleting a rule ... 245
Configuring HTTP parameters used for navigation ... 245
Understanding HTTP parameters used for navigation ... 246
Adding HTTP parameters used for navigation ... 246
Editing an existing HTTP parameter ... 246
Deleting an HTTP parameter ... 247
Configuring advanced HTTP parsing ... 247
Specifying the default encoding ... 247
Handling query parameters without values ... 247
Configuring custom parameters ... 248
About URL rewriting ... 248
About RESTful services ... 249
Creating a custom parameter rule ... 249
Disabling and enabling a rule ... 250
Editing an existing rule ... 250
Deleting an existing rule ... 250
Enabling automatic seeding of rules that were not used during scan ... 250
Double-encoding URL parameters ... 251
Path matrix parameters ... 251
Definition of path segment ... 252
Special elements for rules ... 252
Asterisk placeholder ... 253
Benefit of using placeholders ... 254
Multiple rules matching a URL ... 254
Configuring filters ... 254
Adding an HTTP request filter ... 255
Adding an HTTP response filter ... 255
Configuring HTTP content filter settings ... 255

Editing an existing filter ... 256
Enabling or disabling an existing filter ... 256
Deleting a filter ... 256
Configuring custom cookies and headers ... 256
Configuring standard header parameters ... 257
Appending custom cookies ... 257
Adding a custom cookie ... 257
Appending custom headers ... 258
Adding a custom header ... 258
Editing an existing custom cookie or custom header ... 258
Deleting a custom cookie or custom header ... 259
Configuring multi-user site authentication ... 259
Before you begin ... 259
Known limitations ... 259
Enabling multi-user login ... 260
Adding user login credentials ... 260
Editing user login credentials ... 261
Deleting user login credentials ... 261
Configuring file-not-found settings ... 261
Using HTTP response codes to determine FNF ... 261
Adding a response code for never FNF ... 262
Adding a response code for always FNF ... 262
Editing a response code ... 262
Using custom 404 page notifications ... 263
Editing an existing signature ... 263
Deleting a signature ... 263
Using auto detection of FNF ... 263
Configuring crawl link parsing ... 264
Adding a specialized link parsing pattern ... 264
Editing an existing pattern ... 264
Deleting a pattern ... 265
Configuring crawl link sources ... 265
Pattern-based parsing ... 265
DOM-based parsing ... 265
Form actions, script includes, and stylesheets ... 270
Miscellaneous options ... 271
Limitations of link source settings ... 272
Configuring crawl session exclusions ... 272
Rejecting versus excluding ... 272

Adding a file extension exclusion ... 273
Adding a host exclusion ... 274
Adding a URL exclusion ... 274
Adding a MIME-type exclusion ... 275
Editing existing session exclusions ... 275
Deleting a session exclusion ... 275
Configuring audit session exclusions ... 275
Rejecting versus excluding ... 276
Adding a file extension exclusion ... 276
Adding a host exclusion ... 277
Adding a URL exclusion ... 277
Adding a MIME-type exclusion ... 278
Editing existing session exclusions ... 278
Deleting a session exclusion ... 278
Configuring audit attack exclusions ... 279
Excluding parameters ... 279
Adding a parameter to exclude ... 279
Excluding cookies ... 279
Adding a cookie to exclude ... 280
Excluding headers ... 280
Adding a header to exclude ... 280
Editing an excluded parameter, cookie, or header ... 280
Deleting an excluded parameter, cookie, or header ... 281
Configuring audit attack expressions ... 281
Configuring vulnerability filtering ... 281
Enabling and disabling vulnerability filters ... 282
Suppressing off-site vulnerabilities ... 282
Configuring Smart Scan settings ... 282
Enabling or disabling Smart Scan ... 282
Configuring Smart Scan options ... 283
Configuring custom server/application type definitions ... 283
Editing an existing custom definition ... 284
Deleting a signature ... 284

Chapter 6: Working with scans ... 285
Accessing the DAST Scans view ... 285
User role determines capabilities ... 285
Understanding the Scans view ... 285
Pending Aviator jobs ... 290

Understanding the scan detail panel ... 290
Findings by severity ... 291
Additional scan details ... 291
Understanding the scan EVENTS tab ... 292
Understanding the scan LOGS tab ... 292
Working with active scans ... 292
Pausing a scan ... 293
Stopping a scan ... 293
Resuming a scan ... 293
Re-importing a scan ... 293
Working with alerts ... 294
Identifying scans with active alerts ... 294
Accessing alerts ... 294
Understanding the ALERTS Tab ... 295
Acknowledging new alerts ... 295
Managing the DAST Scans view ... 296
Starting a new scan ... 296
Refreshing the Scans view ... 296
Searching for scans ... 296
Publishing to Application Security ... 296
Deleting scans ... 297
Using the force delete option ... 297
Importing a scan ... 297
Rescanning an application ... 299
Rescan and key store placeholders ... 299
Downloading DAST scans, settings, and logs ... 299
Important information about settings ... 300
Settings that include key store placeholders ... 300
Paused scans ... 300
License Unavailable scan status ... 300
File types available ... 301
Downloading a file ... 302
Performing actions on multiple scans ... 303
Viewing scan results ... 304
Working with the Site Tree ... 304
Site Tree icons ... 304
Using breadcrumbs ... 305
Understanding the Findings table ... 306

Available columns ... 306
Known limitation with suppressed findings ... 307
Understanding vulnerability severity ... 307
Severity descriptions ... 307
How severity is determined ... 307
Working with Findings ... 308
Viewing the Vulnerability Description ... 308
Viewing the Request and Response ... 308
Viewing Steps ... 309
Working with suppressed findings ... 309
Understanding suppressed findings and issues ... 309
How suppressed issues are synced ... 310
Known limitation with suppressed findings ... 310
Audits in imported scans ... 310
Including and hiding suppressed findings ... 310
Understanding the Traffic table ... 311
Available columns ... 311
Working with Traffic ... 314
Viewing the Request and Response ... 314
Viewing Parameters ... 314
Viewing Steps ... 315
Understanding the logs table ... 315
Available columns ... 315
Understanding SPA Coverage ... 316

Chapter 7: Working with Fortify Connect for private application scanning ... 317
Scenario 1: OpenText DAST (Fortify WebInspect) sensor running in the cloud (remote mode) ... 317
Scenario 2: Fortify DAST sensor running on premises (local mode) ... 318
Fortify Connect client service ... 318
Fortify Connect client REST API ... 319
Proxy server ... 319
Fortify Connect server ... 319
Configuring and using Fortify Connect ... 319
Requirements for validating API definitions and saving settings ... 321
Requirements for running an API scan ... 321
Configuring certificate settings for Fortify Connect ... 321
General guidelines ... 322

Configuring TLS authentication ... 322
Configuring mTLS authentication ... 322
Configuring certificate forwarding settings ... 324
Accessing the Fortify Connect view ... 324
User Role Determines Capabilities ... 325
Understanding the Fortify Connect view ... 325
Understanding the client detail panel ... 326
Understanding the Ports tab ... 326
Creating a Fortify Connect client ... 327
Managing Fortify Connect clients ... 328
Downloading the start script ... 328
Editing a client ... 328
Refreshing the Fortify Connect view ... 329
Deleting a client ... 329
Managing client ports ... 329
Ports in local mode ... 329
Viewing all client ports ... 329
Closing a port's connection ... 330
Refreshing the client ports ... 332

Chapter 8: Working with sensors, sensor pools, and auto scale job templates ... 333
Working with sensors ... 333
Accessing the ScanCentral DAST Sensors view ... 333
User role determines capabilities ... 333
Understanding the Sensors view ... 333
Excluding or including auto-scaled sensors ... 335
Understanding the sensor detail panel ... 335
Enabling or disabling sensors ... 336
Facts about disabled sensors ... 336
Enabling or disabling a sensor ... 336
Working with sensor pools ... 337
Accessing the ScanCentral DAST Sensor Pools view ... 337
User role determines capabilities ... 338
Understanding the Sensor Pools view ... 338
Understanding the pool detail panel ... 339
Creating a ScanCentral DAST sensor pool ... 339
Configuring a WISE client ... 340
WISE StatefulSet YAML file ... 341
WISE headless service YAML file ... 342

WISE StatefulSet scaling ... 342
Configuring sensor auto scaling ... 342
Important facts about sensor auto scaling ... 342
Understanding sensor auto scaling ... 343
Important information about privileges for service account tokens ... 343
Managing sensor pools ... 343
Facts about managing sensor pools ... 343
Editing a sensor pool ... 344
Refreshing the Sensor Pools View ... 344
Deleting a sensor pool ... 344
Changing the default sensor pool ... 344
Working with auto scale job templates ... 345
Accessing the Auto Scale Job Templates view ... 345
User role determines capabilities ... 345
Understanding the auto scale job templates view ... 345
Managing auto scale job templates ... 346
Importing a job template ... 346
Editing a job template ... 346
Deleting a job template ... 347
Refreshing the Auto Scale Job Templates view ... 347

Chapter 9: Working with scan settings ... 348
Accessing the ScanCentral DAST scan Settings List view ... 348
User role determines capabilities ... 348
Understanding the Settings List view ... 348
Pending Aviator jobs ... 350
Understanding the scan settings detail panel ... 350
Understanding the settings LOGS tab ... 352
Managing scan settings ... 352
Creating new settings ... 352
Editing settings ... 352
Converting settings ... 352
Editing settings that need to be converted ... 353
Downloading settings ... 353
Deleting settings ... 354
Copying the Settings ID for use in the API ... 354

Chapter 10: Working with scan schedules ... 356
Accessing the ScanCentral DAST Scan Schedules view ... 356

User role determines capabilities ... 356
Understanding the Scan Schedules view ... 356
Understanding the schedule detail panel ... 357
Copying the settings identifier GUID ... 357
Understanding the schedule LOGS tab ... 358
Managing schedules ... 358
Creating a new schedule ... 358
Editing a schedule ... 360
Enabling or disabling schedules ... 361
Deleting a schedule ... 361

Chapter 11: Working with deny intervals ... 362
Deny intervals apply to applications ... 362
Deny intervals are global settings ... 362
Accessing the Deny Intervals view ... 362
User role determines capabilities ... 363
Understanding the Deny Intervals view ... 363
Understanding the deny intervals detail panel ... 363
Creating a deny interval ... 364
Managing deny intervals ... 366
Facts about editing a deny interval ... 367
Editing a deny interval ... 367
Deleting a deny interval ... 367
Refreshing the Deny Intervals view ... 367

Chapter 12: Working with policies ... 369
Accessing the Policies view ... 369
User role determines capabilities ... 369
Understanding the Policies view ... 369
Understanding the policy detail panel ... 370
Importing a custom policy ... 370
Managing policies ... 371
Editing a policy ... 371
Deleting a policy ... 372
Refreshing the Policies view ... 372

Chapter 13: Working with base settings ... 373
Differences between base settings and templates ... 373
Base settings are global settings ... 373
Accessing base settings in Application Security ... 373
User role determines capabilities ... 374
Restricting or allowing edits ... 374
Using key stores in base settings ... 374
Using artifacts from a repository in base settings ... 374
Understanding the Base Settings view ... 374
Converting base settings ... 375
Pending Aviator jobs ... 376
Understanding the base settings detail panel ... 376
Creating base settings ... 377
What's next? ... 377
Configuring base settings for a standard scan ... 377
What’s next? ... 380
Configuring base settings for a workflow-driven scan ... 380
Types of macros supported ... 380
Configuring base settings for a workflow-driven Scan ... 380
What’s next? ... 382
Configuring base settings for an API scan ... 383
What’s next? ... 388
Configuring proxy settings in base settings ... 389
What's next? ... 390
Configuring authentication in base settings for standard and workflow-driven scans ... 391
Configuring site authentication ... 391
Using Aviator for login macro creation ... 391
Validating the login macro ... 392
Downloading the Macro Recorder tool ... 392
Using a client certificate ... 393
Configuring network authentication ... 394
Configuring OAuth 2.0 bearer credentials ... 394
What's next? ... 396
Configuring authentication in base settings for API scans ... 396
Using a client certificate ... 396
Configuring network authentication ... 396
Fetching a token value ... 398
Configuring OAuth 2.0 bearer credentials ... 399

Downloading the Macro Recorder tool ... 400
Using custom headers ... 401
Configuring SOAP settings ... 401
What's Next? ... 403
Configuring base settings details ... 403
What's next? ... 403
Configuring API content and filters in base settings ... 403
Specifying the preferred content type ... 404
Defining specific operations to include ... 404
Defining specific operations to exclude ... 404
Editing specific operations ... 404
Removing specific operations ... 405
Defining parameter rules ... 405
Editing a parameter rule ... 407
Removing a parameter rule ... 407
Adding and managing allowed hosts in base settings ... 407
Adding allowed hosts ... 408
Editing or removing allowed hosts ... 408
Configuring scan priority in base settings ... 408
Changing the priority ... 409
Configuring data retention in base settings ... 409
Scanning single-page applications in base settings ... 409
The challenge of single-page applications ... 409
Configuring SPA support ... 410
Enabling traffic monitor in base settings ... 410
Option must be enabled ... 410
Enabling traffic monitor logging ... 411
Creating and managing basic exclusions in base settings ... 411
Creating exclusions ... 411
Exclusion examples ... 412
Editing or removing exclusions ... 413
Configuring redundant page detection in base settings ... 413
Enabling SAST correlation in base settings ... 414
Applying base settings to applications ... 414
What's next? ... 414
Reviewing and saving base settings ... 414

Working with Administration settings ... 415
Configuration ... 415
ScanCentral DAST ... 416

ScanCentral DAST 416
Service credentials 416

Chapter 14: Working with application settings 418
Application settings are global settings 418
Priority 418
Data retention 418
Applicable scans for domain restrictions 418
Accessing the Application Settings view 419
User role determines capabilities 419
Understanding the Application Settings view 419
Understanding the application setting detail panel 420
Managing application settings 420
Editing application settings 421
Refreshing the Application Settings view 423
Creating or editing an application domain restriction 423
Creating or editing an application private data setting 424

Chapter 15: Working with two-factor authentication 425
How scanning with two-factor authentication works 425
Recommendation 425
Known limitations 425
Facts about Gmail accounts 426
Configuring two-factor authentication in ScanCentral DAST 426
Conducting a scan using two-factor authentication 426
Accessing the Two Factor Authentication view 427
User role determines capabilities 427
Understanding the Two Factor Authentication view 428
Understanding the two-factor authentication detail panel 429
Creating a 2FA Server 429
Configuring a mobile device 430
Installing and configuring the Fortify2FA mobile app 431
Managing 2FA Servers 438
Editing a 2FA Server 438
Deleting a 2FA Server 438

Refreshing the 2FA Server list ... 438
Configuring a mobile device ... 438

Chapter 16: Working with global restrictions and private data settings ... 440
Working with global restrictions ... 440
Applicable scans ... 440
Accessing the Global Restrictions view ... 440
User role determines capabilities ... 440
Understanding the Global Restrictions view ... 441
Creating a global restriction ... 441
Managing global restrictions ... 442
Editing a global restriction ... 442
Deleting a global restriction ... 443
Refreshing the Global Restrictions view ... 443
Working with private data settings ... 443
Accessing the Private Data Settings view ... 443
User role determines capabilities ... 443
Understanding the Private Data Settings view ... 444
Default Private Data Settings ... 444
Creating private data settings ... 444
Managing private data settings ... 445
Editing a private data setting ... 445
Deleting a private data setting ... 445
Refreshing the Private Data Setting view ... 445

Chapter 17: Working with key stores and artifacts repositories ... 446
Understanding key stores ... 446
Benefit of using key stores ... 446
Key store placeholder format ... 446
Placeholder text in exported/imported settings ... 447
Types of key store entries and their usage ... 447
URL key store entry validation ... 447
Key stores in login macros ... 447
Accessing the Key Stores view ... 447
User role determines capabilities ... 448
Understanding the Key Stores view ... 448
Understanding the key store detail panel ... 448
Understanding the key store usage tab ... 448
Creating a key store ... 449

Managing key stores ... 451
Editing a key store ... 451
Hiding a key store ... 451
Viewing hidden key stores ... 452
Managing key store entries ... 452
Editing a key store entry ... 452
Hiding a key store entry ... 453
Understanding artifacts repositories ... 453
Benefits of using artifacts repositories ... 453
Supported artifacts ... 453
Supported repositories ... 453
Using a proxy with the repository ... 454
Artifacts in XML settings files ... 454
Accessing the Artifacts Repositories view ... 454
User role determines capabilities ... 454
Understanding the Artifacts Repositories view ... 454
Understanding the artifacts repositories detail panel ... 455
Understanding the artifacts repositories USAGE tab ... 456
Understanding the artifacts repositories LOGS tab ... 456
Creating an artifacts repository ... 456
Before you begin ... 457
Creating an artifacts repository ... 457
Managing artifacts repositories ... 459
Editing a repository ... 459
Validating a repository connection ... 459
Deleting a repository ... 459
Migrating artifacts ... 460

Chapter 18: Working with scan compliance and health policies ... 461
Facts about scan compliance and health policies ... 461
Accessing the Scan Compliance and Health view ... 461
User role determines capabilities ... 462
Understanding the Scan Compliance and Health view ... 462
Creating a compliance and health policy ... 463
Configuring check definition alert priorities ... 465
Using input boxes ... 465
Using sliders ... 466

Managing compliance and health policies ... 467
Facts about deleting policies ... 467
Editing a policy ... 467
Deleting a policy ... 467
Refreshing the Scan Compliance and Health view ... 468
Understanding the scan health Overview ... 468
Application Versions With Alerts ... 468
Facts about alerts on scan health Overview and Scans view ... 470
Working with alerts on the scan health Overview ... 470
Filtering by policy ... 470
Alerts By Priority ... 471
Alerts By Check Definition ... 471
Corrective actions for scan health alerts ... 473

Chapter 19: Working with Aviator auto-generated macros ... 475
When macros are generated ... 475
Macro generation process ... 475
Enabling Aviator ... 476
Accessing the Aviator view ... 476
User role determines capabilities ... 476
Aviator configuration ... 476
Understanding the Aviator view ... 477
Aviator Configuration Settings ... 477
Credits Summary ... 477
Aviator Entitlements ... 478
Managing Aviator jobs ... 479
Retrying generation ... 479
Viewing generation ... 479
Canceling generation ... 479
Downloading auto-generated macros ... 480
Understanding Aviator Jobs ... 480
Understanding Aviator macro generation progress views ... 481
Startup view ... 482
Intermediate view ... 482
Full view ... 482
Compact view ... 483
Bubble view ... 483

Appendix A: Troubleshooting ScanCentral DAST 484
Locating log files 484
Event log files in the UI 484
Log file names 484
Locating log files inside the Docker Windows containers 484
Locating log files inside the Docker Linux containers 485
Exporting log files 486
Troubleshooting the Configuration Tool CLI 486
CLI return codes 486
Troubleshooting tips 486
Troubleshooting upgrade issues 488
Troubleshooting the ScanCentral DAST API 489
Troubleshooting Fortify Connect 491
Troubleshooting Kafka 491
Troubleshooting artifacts repositories 492
Troubleshooting ScanCentral DAST scans 492
Troubleshooting sensors and the sensor service 494
Checking the sensor service status in a classic Fortify WebInspect installation 495
Restarting the sensor service in a classic Fortify WebInspect installation 495
Checking the sensor service status in ScanCentral DAST sensor in Windows 495
Checking the sensor service status in ScanCentral DAST sensor in Linux 496
Restarting the sensor service in ScanCentral DAST sensor in Windows 496
Restarting the sensor service in ScanCentral DAST sensor in Linux 496
Troubleshooting alerts 496
Disabling alerts 497
Alerts troubleshooting table 497
Testing login macros 498
Validation tests performed 498
Troubleshooting tips 499
Checking and restarting the OpenText DAST (Fortify WebInspect) REST API service 500
Checking the Fortify DAST REST API service status in a classic Fortify DAST installation 500
Restarting the service in a classic Fortify DAST installation 500
Checking the Fortify DAST REST API service status 501
Restarting the service for Fortify DAST 501

Appendix B: Scanning with a Postman collection 502
What is Postman? 502
Benefits of a Postman collection 502
Known limitations with Postman variables 502
Postman prerequisites 503
Tips for preparing a Postman collection 503
Ensure valid responses 503
Order of requests 503
Handling authentication 503
Using static authentication 504
Using dynamic authentication 504
Using a Postman login macro 504
Postman auto-configuration 505
Sample Postman scripts 505
Manually configuring Postman login for dynamic tokens 505
What are dynamic tokens? 505
Before you begin 506
Process overview 506
Identifying and isolating the login request 506
Creating a logout condition with regular expressions 507
Creating a response state rule for a bearer token 507
Creating a response state rule for an API key 508

Appendix C: Working with the Regex Editor 509
Accessing the Regex Editor in ScanCentral DAST 509
Finding matching text 509
Replacing text 510
Using regular expression options 511
Understanding the options 511
Working with sample snippets 512
Filtering sample snippets 512
Viewing sample snippet details 512
Adding a snippet to your regular expression 513
Understanding common sample snippets 513
Understanding web helper sample snippets 515
Understanding the regular expression extensions 516
Examples of extension usage 517

Understanding the regular expression operators 517
Examples of operator usage 517

Appendix D: Reference lists 519
Policies 519
About OAST-related checks 519
Best Practices 519
By Type 521
Custom 523
Hazardous 523
Deprecated checks and policies 523
HTTP status codes 525

Send Documentation Feedback 529

Preface

Contacting Customer Support

Visit the Customer Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

For more information

For more information about OpenText Application Security Testing products, visit OpenText Application Security.

Product feature videos

You can find videos that highlight OpenText Application Security Software products and features on the Fortify Unplugged YouTube™ channel.

Change log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
26.4.0	Added: • SC DAST Administration settings: Service Credentials. • Environment settings: `useProxy` • "Exporting an existing settings file" on page 97: `internalIdentityProviderSettings` • "Configuring requestor settings" on page 231: HTTP/2. Updated: • Aviator auto-generated macros • "Configuring sensor auto scaling" on page 342 and "Database settings" on page 61 for `scannerAutoScalingRestrictions`. • "Miscellaneous ScanCentral DAST settings" on page 66 updated with `internalIdentityProviderSettings`, `SCDASTServiceAuthenticationSettings`. • "Understanding the Aviator view" on page 477 with Aviator Configuration Settings, Credits Summary, and Aviator Entitlements, and Aviator Jobs to "Understanding Aviator Jobs" on page 480. Removed: • All references to Scan Scaling as this has been removed in this release. • All references to Windows container images and Windows options in "Understanding the auto scale job templates view" on page 345.
26.2.0	Added: • Content for scan compliance and health policies. See

Software Release / Document Version	Changes
	"Working with scan compliance and health policies" on page 461. • Content for macro validation (previously undocumented). See the following topics: • "Configuring authentication for standard and workflow-driven scans" on page 175 • "Configuring authentication in base settings for standard and workflow-driven scans" on page 391 • "Testing login macros" on page 498 • Content for Aviator autogen macros. See "Working with Aviator auto-generated macros" on page 475. Updated: • Permissions to include scan compliance and health policies and Aviator. See "Permissions in Application Security" on page 45. • Content related to Aviator autogen macros. See the following topics: • "Configuring authentication for standard and workflow-driven scans" on page 175 • "Configuring authentication in base settings for standard and workflow-driven scans" on page 391 • "Understanding the Scans view" on page 285 • "Understanding the Settings List view" on page 348 • "Understanding the Base Settings view" on page 374 • Content for Linux, macOS, and Windows cURL samples. See "Using the scan settings in the DAST API" on page 208. • Scan schedule content with CICD identifier. See the following topics: • "Understanding the Scan Schedules view" on page 356 • "Understanding the schedule detail panel" on page 357 • Policies content with Created, Created By, and Modified By columns. See the following topics:

Software Release / Document Version	Changes
	• "Understanding the Policies view" on page 369 • "Understanding the policy detail panel" on page 370 Removed: • Content related to Microsoft Windows® Docker® images. Only Linux® versions of ScanCentral DAST images are available.
25.4.0 / December 2025	Updated: • Important information about SSL to clarify requirements. See "Manually configuring the ScanCentral DAST environment" on page 53. • Content related to scan scaling. See the following topics: • Understanding scan scaling • "Configuring a WISE client" on page 340 (new content) • "Configuring sensor auto scaling" on page 342
25.4.0 / November 2025	Updated: • The following content related to using a classic OpenText DAST (Fortify WebInspect) installation with the ScanCentral DAST sensor service: • ASP.NET Core Runtime version prerequisite • Procedure for installing and configuring the DAST sensor service with edits to the `appsettings.json` file See "Using Fortify DAST with the sensor service" on page 127. • Key store details to include specific information about login macros. See "Understanding key stores" on page 446.
25.4.0	Added: • Content for new Docker compose and environment files related to mTLS. See the following topics: • "Configuring the mTLS environment file for core components" on page 112

Software Release / Document Version	Changes
	• "Configuring the mTLS environment file for the scanner service" on page 120 • "Using the mTLS compose file for core components" on page 125 • "Using the mTLS compose file for the sensor" on page 126 Updated: • Installation and upgrade processes to include mTLS. See "Understanding the installation process" on page 54 and "Upgrading ScanCentral DAST" on page 56. • Docker compose and environment files overview with information about mTLS and PostgreSQL® sensor database. See "Understanding the Docker compose and environment files" on page 105. • Setting up the environment with content for creating the Docker network connection. See "Using the TLS compose file for core components" on page 123 and "Using the mTLS compose file for core components" on page 125. • Fortify Connect content to clarify proxy tunnel description. See "Working with Fortify Connect for private application scanning" on page 317. • Process for configuring Fortify Connect to include mTLS settings. See "Configuring certificate settings for Fortify Connect" on page 321. • Advanced settings content with new predefined regular expression statements for response state rules. See "Configuring response state rules" on page 243. • Artifacts Repositories content with support for GitLab. See the following topics: • "Understanding artifacts repositories" on page 453 • "Understanding the Artifacts Repositories view" on page 454 • "Creating an artifacts repository" on page 456 Removed:

Software Release / Document Version	Changes
	• System requirements for ScanCentral DAST components. These have been added back to the *OpenText™ Application Security Software System Requirements* document. • The useLimRestApi / "UseLimRestApi" setting from the JSON and YAML CLI sample settings files. ScanCentral DAST no longer supports using the LIM SOAP service (“LIM.Service”).
25.2.0 / July 2025	Updated: • RedHat versions in System Requirements.
25.2.0 / June 2025	Added: • Information related to deploying classic OpenText DAST (Fortify WebInspect) with the ScanCentral DAST sensor service. See "Using Fortify DAST with the sensor service" on page 127. Updated: • Fixed typo in Configuration Tool CLI RedHat Linux image name. See "Using the Configuration Tool CLI" on page 93. • Corrected mapping syntax error in Docker run command for Linux image. See "Using the Configuration Tool CLI Docker image" on page 95.
25.2.0	Added: • Content describing product name changes. See "Introduction" on page 39. • System requirements for ScanCentral DAST components. • Content for new Docker compose and environment files. See the following topics: • "Understanding the Docker compose and environment files" on page 105 • "Configuring the TLS environment file for core components" on page 106 • "Configuring the TLS environment file for the scanner service" on page 109 • "Using the TLS compose file for core components" on

Software Release / Document Version	Changes
	page 123 • "Using the TLS compose file for the sensor" on page 124 • Content related to using the Advanced view for scan settings. See "Working with Advanced scan settings" on page 219. • Content related to logs table in scan visualization. See "Understanding the logs table" on page 315. Updated: • ScanCentral DAST architecture diagrams to remove classic OpenText DAST (Fortify WebInspect) deployed with the ScanCentral DAST sensor service. See "What is ScanCentral DAST?" on page 40 and "ScanCentral DAST with two-factor authentication" on page 44. • Installation process with new Docker compose and environment files. See "Understanding the installation process" on page 54. • Page navigation with procedure for accessing a specific page. See "Viewing content on multiple pages" on page 148. • Process for configuring Fortify Connect to include TLS settings. See "Configuring and using Fortify Connect" on page 319 and "Configuring certificate settings for Fortify Connect" on page 321. • Scan settings content with new multiple policies feature. See the following topics: • "Configuring a standard scan" on page 161 • "Configuring a workflow-driven scan" on page 164 • "Configuring an API scan" on page 167 • "Configuring base settings for a standard scan" on page 377 • "Configuring base settings for a workflow-driven scan" on page 380 • "Configuring base settings for an API scan" on page 383 • Settings List view content with details about composite and XML settings and converting settings. See "Understanding

Software Release / Document Version	Changes
	the Settings List view" on page 348 and "Managing scan settings" on page 352. • Sensors view content with details about Sensor Type column. See "Understanding the Sensors view" on page 333. • Key store content with new Password type. See the following topics: • "Understanding key stores" on page 446 • "Creating a key store" on page 449 • "Managing key store entries" on page 452 • 2FA server configuration (now handled in the scanner service Docker compose file and environment file for Linux containers). See the following topics: • "Configuring the TLS environment file for the scanner service" on page 109 • "Working with two-factor authentication" on page 425 Removed: • Information related to deploying classic OpenText DAST (Fortify WebInspect) with the ScanCentral DAST sensor service. • Information about DAST API SSL settings, Utility Service SSL settings, Configuration Tool CLI Docker image Windows and Linux TAR files, Configuration Tool CLI launch artifacts, and using script files to pull and start containers. • Validate button and Authentication Header box descriptions from API scan configuration content. The sensor now attempts to validate access using the authentication that is configured in the API Network Authentication settings.
24.4.0 / December 2024	Updated: • Introduction with deployment options. See "Introduction" on page 39. Removed: • Content related to integrating with Kubernetes for scan

Software Release / Document Version	Changes
	scaling. Scan scaling is only available in DAST environments managed in Kubernetes.
24.4.0	Added: • Description of new "Created By" field in the scan detail panel. See "Understanding the scan detail panel" on page 290. • Troubleshooting content for artifacts repositories. See "Troubleshooting artifacts repositories" on page 492. Updated: • Fortify Software Security Center permissions to correct permission for managing Fortify Connect settings. See "Permissions in Application Security" on page 45. • SSC settings content with guidelines about the service account used to integrate ScanCentral DAST with Fortify Software Security Center. See "SSC settings" on page 72. • LIM settings content to clarify LIM URL. See the following topics: • "LIM settings" on page 78 • "JSON sample file" on page 89 • "YAML sample file" on page 91 • Troubleshooting content to include tips for Fortify Connect client. See "Troubleshooting Fortify Connect" on page 491. Removed: • References to the ADVANCED SETTINGS panel.

Chapter 1: Introduction

ScanCentral DAST enables you to download and run a set of Docker containers, configure a connection with your instance of OpenText™ Application Security, and then configure and conduct dynamic scans of your web applications from Application Security.

Options for deployment

You can manually configure an ScanCentral DAST environment using the processes and procedures described in "Manually configuring the ScanCentral DAST environment" on page 53.

You can configure and use the following Helm charts for complete ScanCentral DAST container orchestration in Kubernetes:

- The `helm-scancentral-dast-core` Helm chart deploys the ScanCentral DAST core applications and infrastructure. You can find the core components Helm chart at https://hub.docker.com/r/fortifydocker/helm-scancentral-dast-core/.
- The `helm-scancentral-dast-scanner` Helm chart deploys the ScanCentral DAST scanner applications and infrastructure. You can find the scanner Helm chart at https://hub.docker.com/r/fortifydocker/helm-scancentral-dast-scanner/.

Note: Helm charts might not be available immediately upon product release. When Helm charts for the current release are available, Helm chart documentation will be available on the Product Documentation website.

Audience

This document is intended for users who have experience installing, configuring, and using Docker. Experience with Helm charts and Kubernetes is also recommended if those technologies will be used.

Documentation scope

This document includes OpenText recommended best practices. Other options may be available, but the details for those options are not included in this document.

Product name changes

OpenText is in the process of changing the following product names:

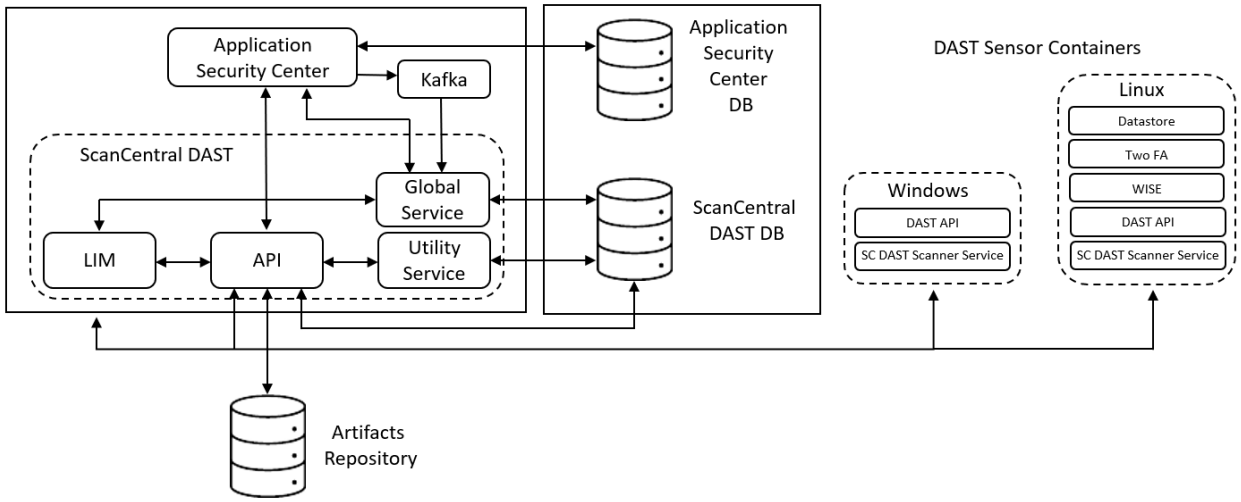
Previous name	New name
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Fortify DAST (Fortify DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
Fortify Applications and Tools	OpenText™ Application Security Tools

The product names have changed on product splash pages, mastheads, login pages, and other places where the product is identified. The name changes are intended to clarify product functionality and to better align the Fortify Software products with OpenText. In some cases, such as on the documentation title page, the old name might temporarily be included in parenthesis. You can expect to see more changes in future product releases.

What is ScanCentral DAST?

ScanCentral DAST is a dynamic application security testing tool that is comprised of the OpenText™ Fortify DAST (DAST) sensor service and other supporting technologies that you can use in conjunction with Application Security.

The following diagram illustrates the ScanCentral DAST architecture.



The following paragraphs describe these components in more detail.

Note: The version numbers included in the image names in this document are accurate at the time of publication. However, Docker images may be updated between releases. Refer to the Read Me file accompanying the image for information about the specific version.

Application Security

The Application Security user interface (UI) provides a way to view the ScanCentral DAST scans list, sensors list, sensor pools, settings, scan schedules, and scan results. You can also access the ScanCentral DAST Settings Configuration wizard from the UI.

ScanCentral DAST communicates with Application Security by way of the Application Security Rest API.

ScanCentral DAST retrieves Application and Version information and user permissions from the Application Security database. ScanCentral DAST uploads scans for triage to the database as FPR files.

Kafka

As an optional configuration, the Kafka messaging service deployed with Application Security forwards messages about issue audit changes to the Global Service. The Global Service syncs the audit changes with the ScanCentral DAST database.

LIM

The OpenText™ Fortify License and Infrastructure Manager (LIM) Docker image provides the licensing service for the ScanCentral DAST components. For more information about the LIM, see the *OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide*.

Note: The architecture diagram shows a LIM Docker container. However, you may use a LIM that is installed on an IIS server.

ScanCentral DAST API

The ScanCentral DAST REST API Docker image provides communication between the sensor and the ScanCentral DAST database. It also communicates with the LIM for licensing, and Application Security. It communicates with the Utility Service for Postman validation.

Optionally, it communicates with a configured artifacts repository to retrieve referenced artifacts to use in a scan.

The Microsoft Windows® image name is `scancentral-dast-api:26.4`. The Linux® image name is `scancentral-dast-api:26.4ubi.9`.

ScanCentral DAST Utility Service

The ScanCentral DAST Utility Service handles lightweight executable utilities without regard to whether a sensor is running and available. It provides support for Postman scans, creates scan settings, and imports scans to the ScanCentral DAST database. The WebInspect API and datastore containers support the ScanCentral DAST Utility Service functions. (These containers are not shown in the architecture diagram.) Running the ScanCentral DAST Utility Service container as part of the core ScanCentral DAST components is dependent upon the WebInspect API Core and the datastore core containers.

The Microsoft Windows® image name is `scancentral-dast-utilityservice:26.4`.

The Linux image name is `scancentral-dast-utilityservice:26.4ubi.9`.

Important! Before you can run the Microsoft Windows® version of the ScanCentral DAST Utility Service container, you must install Microsoft update KB4561608 on the host machine. For more information, see https://support.microsoft.com/en-us/topic/june-9-2020-kb4561608-os-build-17763-1282-437af506-e3ef-a8a1-09e7-26cc94e509c7.

ScanCentral DAST Global Service

The ScanCentral DAST Global Service Docker image does the following:

- Communicates with the LIM to acquire a license
- Starts scans (including scheduled scans), manages scan prioritization, and builds the site tree for completed scans
- Communicates with the ScanCentral DAST database to insert, update, and select messages for the system, including scan statistics from the sensor
- Imports scan results to the Application Security database
- Performs additional background tasks, such as message queuing and processing deny intervals
- Optionally (if Kafka is configured), syncs audit changes in Application Security with the ScanCentral DAST database
- Uses SmartUpdate to obtain the most recent SecureBase updates

Important! If the Global Service is not running, system messages will not be processed, and the sensor may not be able to retrieve a license from the LIM or appear in the ScanCentral DAST UI. If the sensor starts while the Global Service is running, it may start a scan. If the Global Service is not running after the scan starts, the sensor will be able to get a license and will appear in the UI. However, scan data will not be received if the Global Service is not running.

The Windows image name is `scancentral-dast-globalservice:26.4`. The Linux image name is `scancentral-dast-globalservice:26.4ubi.9`.

ScanCentral DAST database

The database stores configuration settings for ScanCentral DAST, as well as dynamic scan settings and dynamic scans. The ScanCentral DAST REST API and Global Service connect to the database on start up to retrieve configuration settings. The Utility Service imports scans to the ScanCentral DAST database.

Fortify DAST sensor

The Fortify DAST sensor is available in Microsoft Windows® or Linux®Docker® versions.

The Microsoft Windows® version includes the following images:

- webinspect:26.4, which includes:
  - WebInspect script engine (WISE) for JavaScript execution and Web Macro Recorder macro playbacks
  - 2FA server to synchronize two-factor authentication requests (used only if the scan is configured to playback a two-factor authentication login macro)
  - Database for scan data
- scancentral-dast-scannerservice:26.4

The Linux® version includes the following images:

- dast-scanner:26.4.ubi.9
- wise:26.4.ubi.9 - WebInspect script engine (WISE) for JavaScript execution and Web Macro Recorder macro playbacks
- fortify-2fa:26.4.ubi.9 - 2FA server to synchronize two-factor authentication requests (used only if the scan is configured to playback a two-factor authentication login macro)
- Database for scan data
- scancentral-dast-scannerservice:26.4.ubi.9

Note: The sensor may also be a Windows computer with both OpenText DAST (Fortify WebInspect) and the ScanCentral DAST sensor service installed. For more information, see "Using Fortify DAST with the sensor service" on page 127.

The sensor does the following:

- Starts and runs scans
- Reports scan statistics to the ScanCentral DAST database by way of the API; the

Global Service retrieves and processes statistics from the database

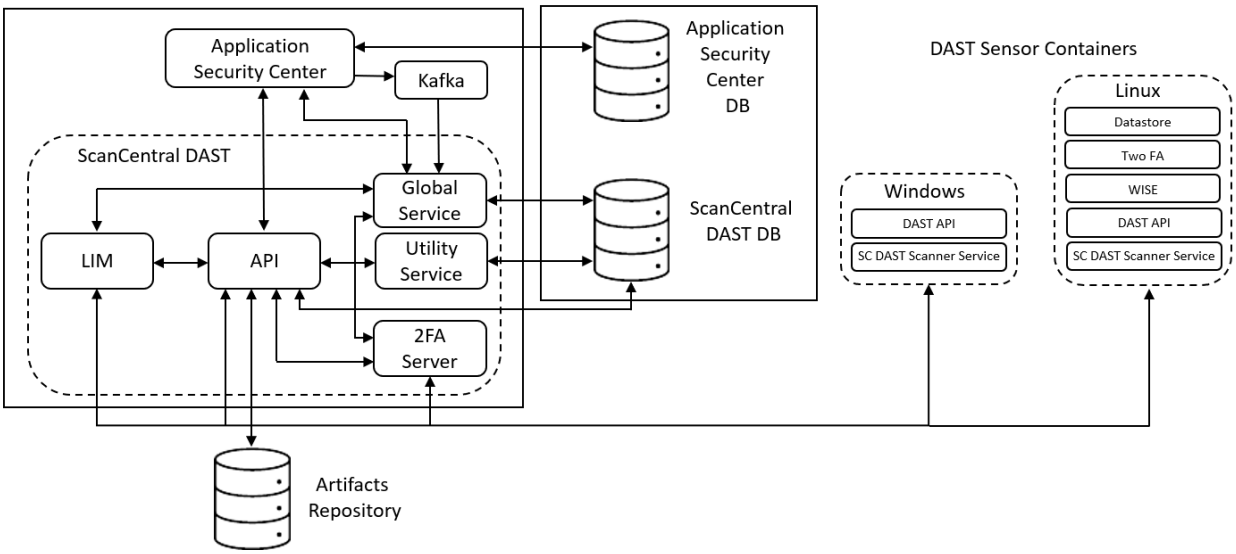
- Uploads the scan to the API

Core components

The ScanCentral DAST REST API, ScanCentral DAST Utility Service along with its supporting WebInspect API Core and the datastore core containers, and ScanCentral DAST Global Service are considered the ScanCentral DAST core components.

ScanCentral DAST with two-factor authentication

The following diagram illustrates the ScanCentral DAST architecture when the optional two-factor authentication server is deployed.



2FA Server

The 2FA Server Docker image provides support for scans that require two-factor authentication. The 2FA Server container communicates with the following components:

- ScanCentral DAST API to generate the QR code used to register a mobile phone for two-factor authentication
- Global Service to indicate that the 2FA Server is up and running
- Fortify DAST sensor to process two-factor authentication requests and responses

Installation recommendation

OpenText recommends that you run the 2FA Server on a host or VM that is separate from any other ScanCentral DAST component–API, Global Service, Utility Service, WebInspect API, or sensor.

2FA Server versions

The image is available for Linux operating systems. The image names are as follows:

- Red Hat Linux - `fortify-2fa:26.4ubi.9`
- Ubuntu Linux - `fortify-2fa:26.4.alpine.3.18`

Permissions in Application Security

The permissions designated by your user role in Application Security determine the types of tasks that you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and global features such as deny windows and base settings. The following table describes the predefined roles in Application Security that allow dynamic-related tasks.

ScanCentral DAST Tasks	Application Security Tester	Developer	Manager	Security Lead	View-only
Manage pools and sensors			x	x	
View data	x	x	x	x	x
Create, run, change, and delete scans, schedules, and settings; manage compliance and health policies	x			x	
Run scans from existing templates and base settings	x	x		x	
Download artifacts (settings, scans, and logs)	x	x		x	
Manage deny intervals, application priority level, and retention policy				x	
Manage global				x	

ScanCentral DAST Tasks	Application Security Tester	Developer	Manager	Security Lead	View-only
restrictions, restricted scan settings, and private data settings					
Manage key stores and artifacts repositories				x	

For information about creating custom user roles, see the *OpenText™ Application Security User Guide*.

Tasks requiring Universal access permissions

The following ScanCentral DAST tasks require **Universal access** permissions in Application Security:

- Creating and maintaining custom policies
- Creating and maintaining base settings
- Force deleting scans from the ScanCentral DAST database
- Managing Fortify Connect settings

Aviator permissions

To be able to administrate the ScanCentral DAST Aviator feature, a user must be granted the **Manage DAST Aviator** permission in Application Security. This new permission grants access to the Aviator configuration page in ScanCentral DAST.

Configuration checklist

The ScanCentral DAST environment includes multiple components that you must configure in a settings file as part of the installation process. The following checklist is provided to aid you in configuring these settings.

Component	Selection
What is the installation environment?	☐ Amazon Web Services (AWS) ☐ Azure ☐ Google Cloud Platform ☐ Local
Which deployment method will you use?	☐ Docker Compose ☐ Kubernetes / Helm Chart ☐ Standalone Containers ☐ Other (Not Recommended): _____
Which operating system will the containers use?	☐ Linux (Red Hat) ☐ Windows
Does your environment use SSL certificates? If yes, the certificate is located at: _____ If yes, is the certificate self-signed? ☐ Yes ☐ No	☐ Yes ☐ No
Which Configuration Tool version will you use?	☐ CLI Executable ☐ Docker Hub Image
Which type of configuration file will you use?	☐ json ☐ yaml
Which type of SQL database will you use? Database server name or IP address: _____	☐ AmazonRdsPostgreSQL ☐ AmazonRdsSQLServer ☐ AzurePostgreSQL ☐ AzureSQLServer ☐ PostgreSQL ☐ SQLServer
Do you want to allow the Global Service to move a scan to a different sensor? For more information, see "Miscellaneous	☐ Yes / DisableAdvancedScanPrioritization = false ☐ No / DisableAdvancedScanPrioritization = true

Component	Selection
ScanCentral DAST settings" on page 66.	
Do you want to save scans in the sensor container after uploading to the ScanCentral DAST database? For more information, see "Miscellaneous ScanCentral DAST settings" on page 66.	☐ Yes / RetainCompletedScans = true ☐ No / RetainCompletedScans = false
Do you want to enable global restrictions? For more information, see "Miscellaneous ScanCentral DAST settings" on page 66.	☐ Yes / EnableRestrictedScanSettings = true ☐ No / EnableRestrictedScanSettings = false
Do you want to allow audit history changes in OpenText™ Application Security to sync with ScanCentral DAST? For more information, see "SSC settings" on page 72.	☐ Yes / KafkaSettings – IsEnabled = true ☐ No / KafkaSettings – IsEnabled = false If yes, Kafka broker and Kafka topic settings are required. Ask your Application Security administrator for these details.
Do you want to disable all origins for Cross-Origin Resource Sharing (CORS) policy? For more information, see "ScanCentral DAST API settings" on page 76.	☐ Yes / DisableCorsOrigins = true ☐ No / DisableCorsOrigins = false
Do you want to allow ScanCentral DAST components to accept self-signed (untrusted) certificates when communicating with other Fortify products? For more information, see "Environment settings" on page 80.	☐ Yes / AllowNontrustedServerCertificates = true ☐ No / AllowNontrustedServerCertificates = false
Is a proxy required for communications in your ScanCentral DAST environment? For more information, see "Environment settings" on page 80.	☐ Yes / UseProxy = true ☐ No / UseProxy = false
Do you want to update SecureBase after installation? For more information, see "SecureBase settings" on page 83.	☐ Yes / ApplySecureBase = true ☐ No / ApplySecureBase = false
Do you want to scan an application that is hidden behind a firewall? For more information, see "Fortify Connect server settings" on page 86.	☐ Yes / DisableFortifyConnectServer = false ☐ No / DisableFortifyConnectServer = true

Related documents

This topic describes documents that provide information about OpenText Application Security Software products.

Note: Most guides are available in both PDF and HTML formats. Product help is available within the Fortify DAST product.

All products

The following documents provide general information for all products. Unless otherwise noted, these documents are available on the Product Documentation website for each product.

Document / file name	Description
About OpenText Application Security Software Documentation appsec-docs-n-*<version>*.pdf	This paper provides information about how to access OpenText Application Security Software product documentation. **Note:** This document is included only with the product download.
What's New in OpenText Application Security Software <version> appsec-wn-*<version>*.pdf	This document describes the new features in OpenText Application Security Software products.
OpenText Application Security Software Release Notes appsec-rn-*<version>*.pdf	This document provides an overview of the changes made to OpenText Application Security Software for this release and important information not included elsewhere in the product documentation.

ScanCentral DAST

The following documents provide information about ScanCentral DAST. These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-ScanCentral-DAST.

Document / file name	Description
OpenText™ ScanCentral DAST Configuration and Usage Guide sc-dast-ugd-<*version*>.pdf	This document provides information about how to configure and use ScanCentral DAST to conduct dynamic scans of Web applications.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-<*version*>.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide dast-docker-ugd-<*version*>.pdf	This document describes how to download, configure, and use Fortify DAST and Fortify OAST that are available as container images on the Docker platform. The Fortify DAST image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as an ScanCentral DAST sensor and used in conjunction with Application Security. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.

Application Security

The following document provides information about OpenText Application Security Center (Software Security Center). This document is available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-software-security-center.

Document / file name	Description
OpenText™ Application	This document provides Application Security users

Document / file name	Description
Security User Guide ssc-ugd-<*version*>.pdf	with detailed information about how to deploy and use Application Security. It provides all the information you need to deploy, configure, and use Application Security. It is intended for use by system and instance administrators, database administrators (DBAs), enterprise security leads, development team managers, and developers. Application Security provides security team leads with a high-level overview of the history and status of a project.

Fortify DAST

The following documents provide information about OpenText DAST (Fortify WebInspect). These documents are available on the Product Documentation website at https://www.microfocus.com/documentation/fortify-webinspect.

Document / file name	Description
OpenText™ Fortify DAST Installation Guide dast-igd-<*version*>.pdf	This document provides an overview of Fortify DAST and instructions for installing and activating the product license.
OpenText™ Fortify DAST User Guide dast-ugd-<*version*>.pdf	This document describes how to configure and use Fortify DAST to scan and analyze Web applications and Web services. **Note:** This document is a PDF version of the Fortify DAST help. This PDF file is provided so you can easily print multiple topics from the help information or read the help in PDF format. Because this content was originally created to be viewed as help in a web browser, some topics may not be formatted properly. Additionally, some interactive topics and linked content may not be present in this PDF version.
OpenText™ Dynamic Application Security Testing and OAST on	This document describes how to download,

Document / file name	Description
Docker User Guide dast-docker-ugd-*<version>*.pdf	configure, and use Fortify DAST and Fortify OAST that are available as container images on the Docker platform. The Fortify DAST image is intended to be used in automated processes as a headless sensor configured by way of the command line interface (CLI) or the application programming interface (API). It can also be run as an ScanCentral DAST sensor and used in conjunction with Application Security. Fortify OAST is an out-of-band application security testing (OAST) server that provides DNS service for the detection of OAST vulnerabilities.
OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide lim-ugd-*<version>*.pdf	This document describes how to install, configure, and use the Fortify License and Infrastructure Manager (LIM), which is available for installation on a local Windows server and as a container image on the Docker platform.
OpenText™ Fortify DAST Tools Guide dast-tgd-*<version>*.pdf	This document describes how to use the Fortify DAST diagnostic and penetration testing tools and configuration utilities packaged with Fortify DAST and Fortify WebInspect Enterprise.
OpenText™ Dynamic Application Security Testing Agent Installation and Rulepack Guide dast-agent-igd-*<version>*.pdf	This document describes how to install the Fortify DAST Agent and describes the detection capabilities of the Fortify DAST Agent Rulepack Kit. Fortify DAST Agent Rulepack Kit runs atop the Fortify DAST Agent, allowing it to monitor your code for software security vulnerabilities as it runs. Fortify DAST Agent Rulepack Kit provides the runtime technology to help connect your dynamic results to your static ones.

Chapter 2: Manually configuring the ScanCentral DAST environment

This chapter provides processes and procedures for manually installing and subsequently managing the ScanCentral DAST components without using Helm charts for integration with Kubernetes.

Installation best practices

Docker container configuration is complex and each environment is unique. OpenText makes the following recommendations as a best practice:

- Install and manage the ScanCentral DAST API, Global Service, Utility Service, and WebInspect API containers on a VM, and each Fortify DAST sensor service on its own, separate VM.
- Do not mix operating systems for the ScanCentral DAST API, Global Service, Utility Service, and WebInspect API containers. Select either Windows or Linux.
- Run the LIM on a host or VM that is separate from any other ScanCentral DAST component–API, Global Service, Utility Service, WebInspect API, or sensor.
- Run the 2FA Server on a host or VM that is separate from any other ScanCentral DAST component–API, Global Service, Utility Service, WebInspect API, or sensor.
- Containers run under a named account rather than root privileges. Keep this in mind if you encounter issues with bind mounts and the Docker compose files.

Important information about SSL

You cannot deploy Application Security with a certificate authority (CA) certificate and ScanCentral DAST without a certificate and vice versa. Mixing secure and non-secure content is not supported.

You cannot use a CA certificate for Application Security and a self-signed certificate for ScanCentral DAST. Mixing self-signed and trusted CA certificates is not supported.

Requesting access to Fortify Docker repository

Access to the Fortify Docker repository requires credentials and is granted through your Docker ID. To access the Fortify Docker repository, email your Docker ID to mfi-fortifydocker@opentext.com.

Before you begin

Ensure that you have met the following prerequisites before you begin configuring your ScanCentral DAST components:

- You must have an OpenText™ Fortify License and Infrastructure Manager (LIM) container downloaded, configured, and running in your environment or have a LIM installed on an IIS server.
  - The LIM must be accessible to the network where your VMs will be running ScanCentral DAST components.
  - You must know the LIM URL and LIM user credentials to configure licensing for ScanCentral DAST.
- You must know the Application Security URL and user credentials to connect ScanCentral DAST to Application Security.
- You must have a database installed and accessible to the VMs on which you install your ScanCentral DAST environment and to your instance of Application Security.

Understanding the installation process

The following table describes the process you must use to install and configure the ScanCentral DAST environment.

Stage	Description
1.	Receive the following licenses from OpenText: • ScanCentral DAST Server License (server-type license) • Fortify DAST Concurrent License
2.	Do the following: 1. Install a LIM from the Docker Hub or by using the MSI. 2. Add the licenses received in Stage 1 to the LIM. For information about how to install the LIM and add licenses, see the *OpenText™ Fortify License and Infrastructure Manager Installation and Usage Guide*.
3.	Do the following: 1. Download and deploy Application Security 26.4.0 from the OpenText Software License and Downloads (SLD) portal.

Stage	Description
	2. Create user accounts for users who will access ScanCentral DAST. For information about how to install and configure Application Security, see the *OpenText™ Application Security User Guide*.
4.	Set up Docker on the host that will run the core ScanCentral DAST containers (API, Global Service, and Utility Service). For more information, see "Setting up Docker" on page 60.
5.	Download the ScanCentral DAST 26.4.0 package from the OpenText SLD portal.
6.	Create a JSON or YAML configuration settings file for ScanCentral DAST. **Tip:** You can edit one of the two sample settings files that are included in the Configuration Tool CLI download package. For more information, see "Creating and using a settings file" on page 60.
7.	Use the ScanCentral DAST Configuration Tool CLI to configure and initialize the ScanCentral DAST database. For more information, see "Using the Configuration Tool CLI" on page 93.
8.	Configure the environment file settings that are used by the ScanCentral DAST API, Global Service, and Utility Service. For more information, see the following topics: • "Configuring the TLS environment file for core components" on page 106 • "Configuring the mTLS environment file for core components" on page 112 • "Configuring the TLS environment file for the scanner service" on page 109 • "Configuring the mTLS environment file for the scanner service" on page 120
9.	Use a Docker compose file to pull and launch the core ScanCentral DAST API, Global Service, and Utility Service containers. For more information, see the following topics: • "Using the TLS compose file for core components" on page 123 • "Using the mTLS compose file for core components" on page 125
10.	Log in to Application Security and enable ScanCentral DAST in the

Stage	Description
	Administration view. **Important!** You must provide the ScanCentral DAST server URL to the Application Security administrator. The URL should be similar to the following: `https://<DAST_API_Hostname>:<Port>/api/` `https://<DAST_API_IP_Address>:<Port>/api/` Make sure that you include the trailing `/api/` in the URL. The URL can use the `http` protocol instead. For more information, see the *OpenText™ Application Security User Guide*.
11.	Use a Docker compose file to pull and launch the Fortify DAST sensor containers. For more information, see the following topics: • "Using the TLS compose file for the sensor" on page 124 • "Using the mTLS compose file for the sensor" on page 126 **Tip:** Optionally, you can deploy classic Fortify DAST with the ScanCentral DAST sensor service. For more information, see "Using Fortify DAST with the sensor service" on page 127.

Tip: If you plan to conduct scans using two-factor authentication, see "Working with two-factor authentication" on page 425 for information about getting and configuring the 2FA Server Docker image.

Upgrading ScanCentral DAST

After initial installation and configuration of the ScanCentral DAST environment, you may need to upgrade the environment. The upgrade process is similar to the installation process. As part of the installation process, however, you will already have received licenses and setup LIM, Application Security, and Docker.

The following table describes the upgrade process.

Stage	Description
1.	Download the ScanCentral DAST 26.4.0 package from the OpenText Software License and Downloads (SLD) portal.

Stage	Description
2.	Edit your JSON or YAML DAST configuration settings file with necessary changes. For more information, see "Creating and using a settings file" on page 60.
3.	Use the ScanCentral DAST Configuration Tool CLI 26.4.0 to configure the ScanCentral DAST database with the latest database schema, if applicable. **Tip:** If a time out occurs while updating the ScanCentral DAST database with the latest database schema, you can use the `commandTimeout` database setting in the settings file to override the default setting of `600` seconds. For more information, see "Database settings" on page 61. You can also use the `generateMigrationScript` as a workaround. For more information, see "Generating a migration script" on page 101.
4.	Configure the environment file settings that are used by the ScanCentral DAST API, Global Service, and Utility Service. For more information, see the following topics: • "Configuring the TLS environment file for core components" on page 106 • "Configuring the mTLS environment file for core components" on page 112 • "Configuring the TLS environment file for the scanner service" on page 109 • "Configuring the mTLS environment file for the scanner service" on page 120
5.	Use a Docker compose file to pull and launch the core ScanCentral DAST API, Global Service, and Utility Service containers. For more information, see the following topics: • "Using the TLS compose file for core components" on page 123 • "Using the mTLS compose file for core components" on page 125
6.	Use a Docker compose file to pull and launch the Fortify DAST sensor containers. For more information, see the following topics: • "Using the TLS compose file for the sensor" on page 124 • "Using the mTLS compose file for the sensor" on page 126

Requirements for upgrading

When upgrading your ScanCentral DAST environment, follow these requirements:

- Use the ScanCentral DAST Configuration Tool CLI that is packaged with the version of ScanCentral DAST software that you downloaded. Do *not* use a previous version of the tool.
- Upgrade your Application Security to the current compatible version. For version compatibility, see "Software integrations for ScanCentral DAST" in the *OpenText™ Application Security Software System Requirements*.
- Upgrade all ScanCentral DAST components, including the database, API container, Global Service container, Utility Service container, and the Fortify DAST on Docker image or the classic Fortify DAST installation with the ScanCentral DAST sensor service.

Recommendation for upgrading

OpenText recommends that you stop all ScanCentral DAST containers and services before upgrading your environment. Many settings that you configure in the ScanCentral DAST Configuration Tool CLI are applied immediately to the database when the `configureEnvironment` command is run. These changes, however, are not recognized by containers that have not been upgraded. If stopping containers and services is not possible because scans are running, then you must upgrade those containers later for any database changes to be recognized.

Effect of upgrades on scheduled scans

When upgrading your ScanCentral DAST environment, you cannot upgrade existing containers. You can only create new containers based on updated images.

When you create a new Fortify DAST sensor container with an updated Fortify DAST on Docker image, any scheduled scans that were assigned to the sensor and configured with the **Use this sensor only** option will not start on the new container. You must edit the scheduled scan settings to use the new sensor container.

Order of orchestration

For proper operation of the ScanCentral DAST environment, some of the components must be started in a specific order or with specific prerequisites. Limited functionality can result when prerequisite components are not running and accessible. The following paragraphs describe these prerequisites.

ScanCentral DAST database

The ScanCentral DAST database must be up and running, and the ScanCentral DAST Configuration Tool CLI must have been run prior to any other containers being started.

Tip: You may use an init container–a specialized container that runs before application containers in Kubernetes–to ensure that the database is up and running. Init containers contain utilities or setup scripts that are not included in an application image.

ScanCentral DAST API

The ScanCentral DAST database must be available to start the ScanCentral DAST API container. If no database is available, then the API service will stop.

If Application Security is not running, then you cannot use the ScanCentral DAST API even though the container is running. ScanCentral DAST must get an authentication token, validate permissions, validate application access, and so forth from Application Security.

If the ScanCentral DAST Utility Service is not running, then the following features will not work in the ScanCentral DAST API:

- Validating Postman collections
- Importing scans
- Converting `.burp` and `.har` files to `.webmacro` files

ScanCentral DAST Utility Service

The ScanCentral DAST database must be available to start the ScanCentral DAST Utility Service container. If no database is available, then the Utility Service will stop.

Postman validation is initiated by the ScanCentral DAST API. If the API is not running, then the Utility Service will not receive a request for validation.

Scan import is initiated by way of the ScanCentral DAST user interface or API, and the API is required to complete the import process. If the API is not available after a scan import begins, then the scan import will fail.

Converting a `.burp` or `.har` file to a `.webmacro` file is initiated in the ScanCentral DAST user interface (which calls the ScanCentral DAST API) or in the API directly. After the file is converted, it is returned to the API. If the API is not running, this process cannot be started.

ScanCentral DAST Global Service

The ScanCentral DAST database must be available to start the ScanCentral DAST Global Service container. If no database is available, then the Global Service will stop.

If Application Security is not running, then certain backend process will fail and prevent syncing data with Application Security.

ScanCentral DAST Sensor Service

The ScanCentral DAST API must be running and available to start the Sensor Service. If the API is not available during start up, then the Sensor Service will try to connect every 10 seconds until it is able to connect.

Setting up Docker

Before you can run Docker containers, you must set up Docker on the host that will run the containers. Set up Docker according to the process described in the following table.

Stage	Description
1.	Download and install the appropriate Docker version on the host machine. **Note:** Follow Docker recommendations for the Docker engine version to use for the Red Hat Enterprise Linux (RHEL) 9.x x86_64 host operating system.
2.	Download and install Compose on Linux. This enables you to use compose files to pull and run the ScanCentral DAST containers.
3.	Configure your machine for Docker containers.
4.	Register and start the Docker service.

For Docker documentation, see https://docs.docker.com/.

Creating and using a settings file

You can use the ScanCentral DAST Configuration Tool CLI to generate a settings file from an existing ScanCentral DAST environment. For more information, see "Exporting an existing settings file" on page 97. You can also create a settings file or edit an existing settings file by hand, and then use the file with the Configuration Tool CLI to create or maintain an environment.

For the `new`, `upgrade`, and `autodeploy` modes, you must provide all of the settings in the settings file. For the `manage` mode, you must provide only the setting or settings that you are managing. For example, if you want to change your Application Security URL, then you need to provide only the SSC settings. For more information about these modes, see "Configuring the environment" on page 99.

Note: The settings contents in this section appear in the order in which the settings appear by default in the sample settings file.

Using special characters in YAML files

When using a YAML settings file, enclose in double quotation marks (") any value that includes one or more of the following special characters:

`:`, `{`, `}`, `[`, `]`, `,`, `&`, `*`, `#`, `?`, `|`, `-`, `<`, `>`, `=`, `!`, `%`, `@`, `\`, `` ` ``

Placeholder text in setting samples

The sample settings in this document use placeholder text to help illustrate the types of information needed in the settings. Placeholder text is encapsulated with angle brackets (<>), such as "*<directory_path>*", *<ip_address>*, and '*<string>*'. Your settings file should not include any placeholder text. You must replace the placeholder text with values that are specific for your environment. If the setting is not applicable to your environment, then provide empty quotes rather than the placeholder text.

For example, if your proxy settings do not require a username and password, then change the placeholder text in the settings from this:

```
proxyUserName: '<string>'
proxyPassword: '<string>'
```

To this:

```
proxyUserName: ''
proxyPassword: ''
```

Database settings

Use the database settings to configure connections to an existing database or create a new database with the information you provide.

Important! To avoid automatically upgrading the database schema when you are managing an existing ScanCentral DAST environment, the Configuration Tool CLI checks to see if the database schema is up to date. If the schema is not up to date, the Configuration Tool CLI stops executing and writes a warning to the log file.

Configuring a DBO-level account

You must configure a connection to the database using an existing database owner (DBO) server-level account that has full access to the database. DBO access is required to create the schema on the database server. Ensure that the following permissions requirements are met:

- If you are creating a new database, the DBO account must have the `CREATE ANY DATABASE` server-level permission.
- If you are managing or updating an existing database, the DBO account must be a member of the `db_owner` database-level role.
- If available, the DBO account may use the `dbcreator` server-level role in lieu of the previously mentioned permission and role.

  Note: The `dbcreator` role is not available in the Amazon Relational Database Service (Amazon RDS).

- If you are creating a login, the DBO account must have the `ALTER ANY LOGIN` permission, which is part of the `securityadmin` server-level role. To give the new login access to a database, the account must have the `ALTER ANY USER` permission.

Configuring a standard account

You must configure a standard user account for everyday use, preferably with non-DBO credentials. This account must have one of the following sets of permissions:

- Both the `db_datareader` and `db_datawriter` database-level roles
- All of the `SELECT`, `INSERT`, `UPDATE`, and `DELETE` privileges on the database

JSON example

The following example shows the database settings in a JSON file.

```
"DatabaseSettings":{
  "DatabaseProvider": "<database_type>",
  "Server": "<ip_address>,<port>",
  "Database": "<database_name>",
  "CommandTimeout": 600,
  "DboLevelDatabaseAccount": {
    "Username": "<string>",
    "Password": "<string>",
    "UseWindowsAuthentication": false
    "AdditionalConnectionProperties": null
},
"StandardDatabaseAccount": {
```

```
    "Username": "<string>",
    "Password": "<string>",
    "CreateLogin": false,
    "AdditionalConnectionProperties": null
   }
```

YAML example

The following example shows the database settings in a YAML file.

```
databaseSettings:
  databaseProvider: <database_type>
  server: <ip_address>,<port>
  database: <database_name>
  commandTimeout: 600
  dboLevelDatabaseAccount:
    username: <string>
    password: <string>
    useWindowsAuthentication: false
    additionalConnectionProperties: null
  standardDatabaseAccount:
    username: <string>
    password: <string>
    createLogin: false
    additionalConnectionProperties: null
```

Parameter descriptions

The following table describes the parameters for the database settings.

Parameter	Description
`CommandTimeout`	Optional setting that indicates the command timeout, in seconds, during deployment. If not configured, the default setting of `600` seconds is used. **Note:** If the SQL command times out during deployment, then the Configuration Tool CLI will fail. If more time is needed, increase the default timeout.
`DatabaseProvider`	Required setting that identifies the type of SQL

Parameter	Description
	database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`Server`	Required setting that specifies the database server name or the server IP address. **Important!** If SQL Server Browser is not running and you are using a port other than 1433, then you must also specify the port. Use the following format: *<server_name>*,*<port>* *<ip_address>*,*<port>* Note that a comma separates the values.
`Database`	Optional setting that specifies the name of the database. If you are upgrading or managing an existing ScanCentral DAST environment, then you must use an existing database. **Caution!** An existing database might be upgraded during this process. Be sure to create a backup of the existing database before proceeding.
`DboLevelDatabaseAccount`	Optional setting that specifies the database owner (DBO) server-level account that has full access to the database. You must provide the following parameters: • `Username` – Indicates the DBO account user name • `Password` – Indicates the DBO account

Parameter	Description
	password • `UseWindowsAuthentication` – Uses the credentials of the user who is currently logged into Windows Options are `true` or `false`. If set to `true`, then `Username` and `Password` are not required.
`StandardDatabaseAccount`	Required setting that specifies the standard user account for everyday use, preferably with non-DBO credentials. This account should have select, insert, update, and delete functions, but should not be able to create tables and so forth. **Tip:** You may use the same credentials as the DBO-level account. However, it is generally considered a safer option to provide limited access for general use after the schema has been created. You must provide the following parameters: • `Username` – Indicates the database account user name • `Password` – Indicates the database account password • `CreateLogin` – Creates a login for the standard user to connect to the database Options are `true` or `false`. If set to `false`, no changes will be made to the login or user account.
`AdditionalConnectionProperties`	Optional setting that specifies any additional connection properties for the database, such as `trustServerCertificate`. For more information on additional connection properties, refer to your SQL database documentation.
`scannerAutoScalingRestrictions`	Determines if scanner auto-scaling settings are managed through the deployment configuration

Parameter	Description
	or in the ScanCentral DAST user interface. • `true` - Sensor Auto Scaling restrictions are turned on. The **Auto Scale Job Templates** menu item and page are not visible in ScanCentral DAST. • `false` - Sensor Auto Scaling restrictions are turned off. The **Auto Scale Job Templates** menu item and page are visible in ScanCentral DAST. **Note:** When the `scannerAutoScalingRestrictions` setting is set to true using the Configuration Tool CLI, the following are not displayed in sensor pool information: **Sensor Scaling Host**, **Sensor Scaling Namespace**, and **Sensor Scaling Template Name**. For more information, see "Understanding the Sensor Pools view" on page 338 and "Configuring sensor auto scaling" on page 342. For more on Sensor Auto Scaling, see Configuring sensor auto scaling.

Miscellaneous ScanCentral DAST settings

You can specify ScanCentral DAST settings for licensing and SmartUpdate, as well as other miscellaneous settings.

JSON example

The following example shows these settings in a JSON file.

```
{
     "RetainCompletedScans": false,
     "DisableAdvancedScanPrioritization": false,
     "EnableRestrictedScanSettings": false,
     "ServiceToken": "<string>",
     "SmartUpdateSettings": {
```

```
      "SmartUpdateUrl": "https://smartupdate.fortify.microfocus.com/",
      "LicensingUrl": "https://licenseservice.fortify.microfocus.com/"
    "InternalIdentityProviderSettings"" {
      "IsEnabled": true,
      "Audience": "scdast",
      "Scope": "scdast-service",
      "SigningKey": "encrypted-signing-key",
      "ServiceCredentialsSettings": {
          "KubernetesHostSettings": {
              "Host": "",
              "AccessTokenType": "<StaticAPIToken>,
  <DefaultServiceAccountToken>, or <ServiceAccountTokenPath>",
              "AccessToken": "<staticAPIToken> or
  <ServiceAccountTokenPath>",
          },
          "ServiceCredentials": [{
              "Name": "service credential name",
              "KubernetesSecretName": "kubertnetes-secret-name",
              "KubernetesNameSpace": "kubernetes-secret-namespace"
          }]
      }
    }
  },
```

YAML example

The following example shows these settings in a YAML file.

```
retainCompletedScans: false
disableAdvancedScanPrioritization: false
enableRestrictedScanSettings: false
serviceToken: <string>
smartUpdateSettings:
  smartUpdateUrl: https://smartupdate.fortify.microfocus.com/
licensingUrl: https://licenseservice.fortify.microfocus.com/
internalIdentityProviderSettings:
  isEnabled: true
  audience: scdast
  scope: scdast-service
  signingKey: encrypted-signing-key
  serviceCredentialSettings:
    kubernetesHostSettings:
```

```
      host: <host>
      accessTokenType: <StaticAPIToken>, <DefaultServiceAccountToken>, or
<ServiceAccountTokenPath >
      accessToken: <staticAPIToken> or <ServiceAccountTokenPath>
    serviceCredentials:
    - name: "service credential name"
    kubernetesSecretName: "kubernetes-secret-name"
    kubernetesSecretNamespace: "kubernetes-secret-namespace"
```

Parameter descriptions

The following table describes the parameters for the miscellaneous settings.

Parameter	Description
`DisableAdvancedScan Prioritization`	Optional setting prevents or allows the ScanCentral DAST Global Service to move a scan to a different sensor, depending on the scan priority and other settings. By default, advanced scan prioritization is allowed. Options are `true` or `false`. For more information, see "Understanding advanced scan prioritization" on page 196.
`RetainCompletedScans`	Optional setting specifies whether to save scans in the sensor container. By default, scans are not saved in the sensor container after the sensor completes the scan and uploads the data to the ScanCentral DAST database. Options are `true` or `false`. **Note:** SQL Server Express is the default database for the Fortify DAST Docker images. Even with this setting enabled, each scan has its own database file with a 10 GB limit. You can have an unlimited number of scans until Docker allocates the entire Docker volume disk partition size.
`EnableRestrictedScanSettings`	Optional setting enables or disables global restrictions.

Parameter	Description
	Options are `true` or `false`. For more information, see "Working with global restrictions" on page 440.
`ServiceToken`	Required setting specifies a shared secret for all of your sensors to use to authenticate with the ScanCentral DAST API. The setting is a string with a minimum of 10 characters. The value is encrypted.
`SmartUpdateUrl`	Required setting indicates the URL for the SmartUpdate service. This setting is an element of `SmartUpdateSettings`. The default URL is `https://smartupdate.fortify.microfocus.com/`.
`LicensingUrl`	Required setting indicates the URL for the licensing service. This setting is an element of `SmartUpdateSettings`. The default URL is `https://licenseservice.fortify.microfocus.com/`.
`internalIdentityProviderSettings`	Optional setting • `isEnabled` (required) - `true` or `false`. When set to `true`, internal identity verification is activated. If using an external identity provider, such as Keycloak, this can be set to `false`. If false, or no identity verification is provided, the remaining settings are not processed. • `audience` - Required when `isEnabled` is `true`. • `scope` - Required when `isEnabled` is `true`. • `signingKey` (optional) - If not provided, a random key will be generated. If a `signingKey` is specified, it must be at least 64 characters in length to avoid an error. • `serviceCredentialSettings` - An optional

Parameter	Description
	setting used to create or update service credentials. • `kubernetesHostSettings` - Optional settings used to override the default Kubernetes client. If not provided, the `kubeconfig` must be mounted in the container. ◦ `host` - the Kubernetes host. ◦ `accessTokenType` - This is required if a `host` has been specified. This can be one of three values: `StaticAPIToken`, `DefaultServiceAccountToken`, or `ServiceAccountTokenPath`. ◦ `accessToken` - Required if `host` is set and `accessTokenType` is `StaticAPIToken` or `ServiceAccountTokenPath`. • `serviceCredentials` - The list of credentials to create or update. If the credential exists, a new secret will be generated. If the credential does not exist, new credentials will be generated. **Important!** After updating existing credentials, the Kubernetes secret might need to be refreshed. ◦ `name` - The service credential name that will be created or updated. **Note:** The `name` is required. Duplicate names will trigger an error. ◦ `kubernetesSecretName` - This is an optional value used to indicate the Kubernetes secret to be updated with the created or updated `name`. If provided, the CLI will connect to the Kubernetes instance and patch the secret. **Note:** The `kubernetesSecretName` must include the `ClientId` and `ClientSecret`:

Parameter	Description
	• `SCDASTServiceAuthenticationSettings__OAuth2Settings__ClientSettings__ClientId` • `SCDASTServiceAuthenticationSettings__OAuth2Settings__ClientSettings__ClientSecret` ◦ `kubernetesSecretNamespace` - The Kubernetes secret namespace. If not provided, `default` will be used.
`SCDASTServiceAuthenticationSettings`	This setting sets the authentication type used for the ScanCentral DAST service communication and JWT token used in client credentials. • `Mode` - The authentication type to use: `ServiceToken` or `OAuth2`. • `ServiceToken` - If `mode` is set to `ServiceToken`, this specifies a shared secret for all of your sensors to use to authenticate with the ScanCentral DAST API. The setting is a string with a minimum of 10 characters. The value is encrypted. • `OAuth2Settings` - Required if `mode` is set to `OAuth2`. The following settings are required to configure `OAuth2Settings`: ◦ `ClientSettings` - The client settings used in obtaining an access token. ◦ `TokenEndpoint` - The endpoint used to obtain the access token. The `ClientId` and `ClientSecret` for this endpoint must be used. ◦ `ClientId` - The client id used to obtain the access token. This can be encrypted (recommended) or plain text. ◦ `ClientSecret` - The client secret used to obtain the access token. This can be encrypted (recommended) or plain text. ◦ `Scope` - The scope to use when obtaining the token. For example, `scdast-service`.

Parameter	Description
	• `ServerSettings` (required) - The configuration for the authentication or authorization scheme used for the service-to-service endpoints. ◦ `ProviderType` - `SCDAST` or `JwtBearer`. ◦ `SCDAST` - Internal SC DAST, minimal OAuth2 implementation ◦ `JwtBearer` - The JwtBearer token. ◦ `JwtBearerSettings` - Required if `ProviderType` is set to `JwtBearer`. ◦ `Authority` - The authority to use when making `OpenIdConnect` calls ◦ `ValidAudience` - A valid audience value used to check against the token's audience. For example, `scdast`. • `ServerCertificateValidationSettingsName` - Configures the server certificate validation for environments using internal CA. • `ClientCertificateSettingsName` - Configures the client certificates used for mTLS.

SSC settings

You can use the SSC settings to configure the connection between ScanCentral DAST and Application Security. Optionally, you can configure Kafka settings that provide a way for Application Security to message audit history changes to ScanCentral DAST.

Important guidelines for the service account

The service account that is configured with the `ServiceAccountUserName` and `ServiceAccountPassword` settings is used to integrate ScanCentral DAST with Application Security. Follow these guidelines when configuring the service account:

- The account must be an administrator-level account that can perform service-level functions.
- The account must be a dedicated account that is only used for the integration of ScanCentral DAST and Application Security. Do not use the account for access by an ScanCentral DAST user.

Note: Individual users who log into Application Security to use ScanCentral DAST are restricted based on the permissions designated by their user role in Application Security. For more information, see "Permissions in Application Security" on page 45.

- The account must be a local user account that has the Administrator role. Do not use an externally-managed account such as an LDAP- or SCIM-based user account.

JSON example

The following example shows the SSC settings in a JSON file.

```
  "SSCSettings": {
       "SSCRootUrl": "http://<ip_address>:<port>/ssc",
       "ServiceAccountUserName": "<username>",
       "ServiceAccountPassword": "<password>"
       "KafkaSettings": {
         "IsEnabled": true,
         "BootstrapServers": "<broker1>,<broker2>,<broker3>",
         "FindingAuditGroupId": "<SCDAST_FindingAuditGroup>",
         "FindingAuditTopic": "<FindingAuditTopic>"
         "SecurityProtocolType": "SSL",
         "SSLSettings": {
           "CALocation": "/<directory_path>/<cert_name>.cer",
           "CertificateLocation": "/<directory_path>/<cert_name>.cer",
           "EnableSslCertificateVerification": true,
           "KeyLocation": "/<directory_path>/<cert_name>.key",
           "KeyPassword": "<password>"
         }
       }
     },
```

YAML example

The following example shows the SSC settings in a YAML file.

```
sSCSettings:
  sSCRootUrl: http://<hostname>:<port>/ssc
  serviceAccountUserName: <username>
  serviceAccountPassword: <password>
  kafkaSettings:
    isEnabled: true
    bootstrapServers: <broker1>,<broker2>,<broker3>
```

```
    findingAuditGroupId: <SCDAST_FindingAuditGroup>
    findingAuditTopic: <FindingAuditTopic>
    securityProtocolType: SSL
    sSLSettings:
      cALocation: /<directory_path>/<cert_name>.cer
      certificateLocation: /<directory_path>/<cert_name>.cer
      enableSslCertificateVerification: true
      keyLocation: /<directory_path>/<cert_name>.key
      keyPassword: <password>
```

Parameter descriptions

The following table describes the parameters for the SSC settings.

Parameter	Description
`SSCRootUrl`	Required setting that specifies the URL for your Application Security application. **Important!** You cannot use localhost for the Application Security URL. You must use a routable IP address or hostname. Additionally, do not use a trailing slash (`/`) at the end of the URL.
`ServiceAccountUserName`	Required setting that identifies the user name under which ScanCentral DAST will communicate with Application Security. For more information, see "Important guidelines for the service account" on page 72.
`ServiceAccountPassword`	Required setting that identifies the password for the service account. **Tip:** OpenText recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting values" on page 101.
`KafkaSettings`	Optional settings that allow audit history changes in Application Security to sync with ScanCentral DAST. `IsEnabled` – Indicates whether ScanCentral DAST will

Parameter	Description
	retrieve messages regarding changes to audit history in Application Security from the Kafka messaging system. Options are `true` and `false`. If set to `true`, then you must also provide the following parameters: • `BootstrapServers` – Specifies a comma-separated list of brokers for the Application Security Kafka instance. Ask your Application Security administrator for these details. • `FindingAuditGroupId` – Identifies the Application Security Kafka group ID for ScanCentral DAST. This ID must be a string that is unique to ScanCentral DAST, and no other Kafka consumers should use this group ID. • `FindingAuditTopic` – Indicates the Application Security Kafka topic to be used for finding audit events. Ask your Application Security administrator for these details. • `SecurityProtocolType` – Indicates the security protocol used to communicate with brokers. Options are `Plaintext` and `SSL`. If `SecurityProtocolType` is `SSL`, then you must also provide the following parameters: • `CALocation` – Identifies the file or directory path to the CA certificate for verifying the broker's key. **Tip:** On Windows, the default location of the system's CA certificates is the Windows Root certificate store. On Mac OS X, the configuration defaults to `probe`. Install OpenSSL using Homebrew to provide CA certificates. On Linux, install the distribution's ca-certificates package. If OpenSSL is statically linked or `ssl.ca.location` is set to `probe`, a list of standard paths will be probed and the first one found will be used as the default CA certificate location path. If OpenSSL is dynamically linked, then the OpenSSL library's default path will be

Parameter	Description
	used. • `CertificateLocation` – Indicates the path to the client's public key (PEM) to use for authentication. • `KeyLocation` – Indicates the path to the client's private key (PEM) to use for authentication. • `KeyPassword` – Optionally, indicates the private key password. **Important!** OpenText recommends using an encrypted password. You can encrypt the password using the `encrypt` command. For more information, see "Encrypting values" on page 101. • `EnableSslCertificateVerification` – Indicates whether OpenSSL's built-in broker (server) certificate verification is enabled. Options are `true` and `false`.

ScanCentral DAST API settings

You can use the ScanCentral DAST API settings to configure the URL for the API and configure cross-origin resource sharing (CORS) settings.

JSON example

The following example shows the ScanCentral DAST API settings in a JSON file.

```
"SCDASTApiSettings": {
     "RootUrl": "http://<hostname>:<port>",
     "DisableCorsOrigins": false,
     "CorsOrigins": [
       "http://<hostname>:<port>",
       "http://<hostname>:<port>",
       "http://<ip_address>:<port>"
     ]
   },
```

YAML example

The following example shows the ScanCentral DAST API settings in a YAML file.

```
sCDASTApiSettings:
  rootUrl: http://<ip_address>:<port>
  disableCorsOrigins: false
  corsOrigins:
  - http://<hostname>:<port>
  - http://<hostname>:<port>
  - http://<ip_address>:<port>
```

Parameter descriptions

The following table describes the parameters for the ScanCentral DAST API settings.

Parameter	Description
`RootUrl`	Required setting that specifies the URL and port where the ScanCentral DAST API service will run. **Important!** You cannot use localhost in the URL. You must use a routable IP address or hostname as shown in the following examples: `https://<SCDAST_API_hostname>:<port>` `https://<SCDAST_API_ip_address>:<port>` The URL can use the http protocol instead. The port number must be greater than 1024. Make note of this URL. It is required to enable ScanCentral DAST in Application Security.
`DisableCorsOrigins`	Optional cross-origin resource sharing (CORS) setting to restrict traffic to specific URLs or allow traffic from all URLs. By default, disable all origins for CORS policy is set to `false`. The Application Security URL is the only one that is automatically allowed. Options are: • `true` – CORS checks are not performed and requests from any origin are allowed. Use this setting when you want unrestricted access to the ScanCentral DAST API from any domain. • `false` – Only requests from origins specified in the `corsOrigins` list are allowed. Use this setting when you want to restrict ScanCentral DAST API access to specific URLs for enhanced security.

Parameter	Description
`CorsOrigins`	Specifies the allowed CORS origins list of URLs . Required when `disableCorsOrigins` is set to `false`. **Important!** When using a JSON settings file, the list must be specified as a JSON array of origins, as shown in the "JSON example" on page 76.

LIM settings

You can use the LIM settings to configure a LIM and LIM pool to associate with the default sensor pool for licensing.

JSON example

The following example shows the LIM settings in a JSON file.

```
  "LIMSettings": {
       "LimUrl": "https://<location>:<port>",
       "ServiceAccountUserName": "<string>",
       "ServiceAccountPassword": "<string>",
       "DefaultLimPoolName": "<string>",
       "DefaultLimPoolPassword": "<string>",
     },
```

YAML example

The following example shows the LIM settings in a YAML file.

```
lIMSettings:
     limUrl: https://<location>:<port>
     serviceAccountUserName: <string>
     serviceAccountPassword: <string>
     defaultLimPoolName: <string>
     defaultLimPoolPassword: <string>
```

Parameter descriptions

The following table describes the parameters for the LIM settings.

Parameter	Description
`LimUrl`	Required setting that identifies the LIM server in the format `https://<location>:<port>`, where *location* is IP address, hostname, or domain name. **Note:** If using a Windows version of the LIM prior to 24.2.0, the format is `https://<location>:<port>/<service-directory>` where: • *location* is the site specified during LIM initialization as the root website. • *service-directory* is the directory specified during LIM initialization as the Service Virtual Directory name (the default is "LIM.API").
`ServiceAccountUserName`	Required setting that specifies the LIM account username to be used for licensing.
`ServiceAccountPassword`	Required setting that specifies the password for the account. **Tip:** OpenText recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting values" on page 101.
`DefaultLimPoolName`	Required setting that specifies the LIM pool name to associate with the default sensor pool for licensing.
`DefaultLimPoolPassword`	Required setting that specifies the password for the LIM pool. **Tip:** OpenText recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting values" on page 101.

Utility Service settings

Use the Utility Service settings to configure the URL and port where the DAST Utility Service will run.

Important! You cannot use `localhost` in the URL. You must use a routable IP address or hostname as shown in the following examples:

`https://<DAST_Utility_hostname>:<port>`

`https://<DAST_Utility_ip_address>:<port>`

The URL can use the `http` protocol instead. The port number must be greater than 1024.

JSON example

The following example shows the Utility Service settings in a JSON file.

```
  "UtilityWorkerServiceSettings": {
       "RootUrl": "https://<ip_address>:<port>/"
     },
```

YAML example

The following example shows the Utility Service settings in a YAML file.

```
utilityWorkerServiceSettings:
     rootUrl: https://<hostname>:<port>/
```

Parameter descriptions

The following table describes the parameters for the Utility Service settings.

Parameter	Description
`RootUrl`	Required setting that specifies the URL for the DAST Utility Service.

Environment settings

You can use the environment settings to configure proxy settings and allow untrusted certificates.

Using a proxy

The proxy settings configured here, including the exclusions, are used for internal communications between ScanCentral DAST components. The settings also apply when communicating with OpenText Application Security Center (Software Security Center), LIM, SmartUpdate, DAST API, DAST Utility Service, and OpenAPI and OData definition URLs.

Note: ScanCentral DAST Aviator uses the existing system proxy configuration for communication with the Aviator service. When a system proxy is configured, all outbound communication is routed through that proxy. If a proxy is not configured, communication occurs directly with the Aviator service. The proxy connection string is encrypted before being passed to the OpenText DAST (Fortify WebInspect) API.

JSON example

The following example shows the environment settings in a JSON file.

```
  "EnvironmentSettings": {
    "AllowNonTrustedServerCertificate": true,
    "ProxySettings": {
      "UseProxy": false,
      "ProxyAddress": "<ip_address>",
      "ProxyPassword": "<string>",
      "ProxyUserName": "<string>",
      "ProxyBypassList": "<hostname>,<ip_address>"
    }
  },
```

YAML example

The following example shows the environment settings in a YAML file.

```
environmentSettings:
  allowNonTrustedServerCertificate: true
  proxySettings:
    useProxy: false
    proxyAddress: '<ip_address>'
    proxyPassword: '<string>'
    proxyUserName: '<string>'
    proxyBypassList: <hostname>,<ip_address>
```

Parameter descriptions

The following table describes the parameters for the environment settings.

`AllowNontrustedServerCertificates`	Optional setting that specifies whether ScanCentral DAST components can accept self-signed (untrusted) certificates when communicating with other Fortify products.

	Options are `true` or `false`.
`UseProxy`	Optional setting that specifies whether to use a proxy for communications in your ScanCentral DAST environment. Options are `true` or `false`. If set to `true`, then you must also provide the following parameters: • `ProxyAddress` – Identifies the URL or IP address and port number of your proxy server • `ProxyPassword` – If your proxy server requires authentication, specifies the qualifying password **Tip:** OpenText recommends using an encrypted password. You can encrypt the password with the `encrypt` command. For more information, see "Encrypting values" on page 101. • `ProxyUserName` – If your proxy server requires authentication, specifies the qualifying user name • `ProxyBypassList` – Lists hostnames or IP addresses that do not need to use a proxy server for access, such as internal testing sites **Tip:** Your comma separated list may contain wildcards and regular expressions. For example: `localhost,198.51.*.*,[a-z]+\.myestore\.net$` **Important!** If you use Fully Qualified Domain Names (FQDN) to define the host/location in URLs in your YAML or JSON file, then you must use the same

	in the `ProxyBypassList`. If you use IP addresses, then you must use those in the `ProxyBypassList`.

Known issue with host name, machine name, and container name

Configuring a proxy in the environment settings and then bypassing the proxy for communications with Application Security and the LIM may cause issues when using the host name, machine name, or container name for these products.

If you want to use the host name, machine name, or container name for Application Security and the LIM without a proxy, then set `UseProxy` to `false` and configure `HTTP_PROXY` and `NO_PROXY` environment variables instead. Additionally, add the host names, machine names, or container names for Application Security and the LIM to the `NO_PROXY` variable as a comma-separated list.

Refer to your OS documentation and change these environment variables.

You must also add these variables to the Docker containers' run commands as shown in the following example:

```
-e "HTTP_PROXY=http://<proxy_address>" -e "NO_PROXY=localhost,<ssc_
machine>,<lim_machine>"
```

SecureBase settings

After initializing the database, the Global Service updates the database with the latest SecureBase data from the Fortify SmartUpdate servers.

Note: Open Text recommends retrieving the default SecureBase data from the SmartUpdate servers (the default configuration), by leaving the `secureBasePath` empty and the `applySecureBase` set to `false`.

In environments lacking Internet access, however, you must contact Customer Support and request the default SecureBase ZIP file (or use a local copy already in your possession) in conjunction with the SecureBase settings to update the database.

JSON example

The following JSON example shows SecureBase settings that use the default ZIP file to seed the database.

```
  "ApplySecureBase": true,

  "SecureBasePath": "/app/logs/DefaultData.zip",
```

Note: `SecureBasePath` depends on the initial bind mount used in the Docker run command.

YAML example

The following YAML example shows SecureBase settings that do not update the database.

```
applySecureBase: false

secureBasePath: /app/logs/DefaultData.zip
```

Note: `secureBasePath` depends on the initial bind mount used in the Docker run command.

Parameter descriptions

The following table describes the parameters for the SecureBase settings.

Parameter	Description
`ApplySecureBase`	Optional setting that specifies whether to update SecureBase. Options are: • `true` - Update SecureBase • `false` - Do not update SecureBase
`SecureBasePath`	If `applySecureBase` is set to `true`, this optional setting specifies the location of the SecureBase ZIP file to use for seeding the database. If no value is provided for `SecureBasePath`, the Configuration Tool CLI will attempt to acquire a license from the LIM specified in the `LIMSettings` and download the SecureBase data using the SmartUpdate and licensing URLs specified in the `SmartUpdateSettings`. For more information, see "LIM settings" on page 78 and "Miscellaneous ScanCentral DAST settings" on page 66. To update SecureBase data in an offline environment, set the `SecureBasePath` to the directory where the DefaultData.zip file is located. In the Configuration Tool CLI run command, you will map a volume for this directory to an external location in the container. OpenText recommends that you use `/app/logs/DefaultData.zip` as the `SecureBasePath`. For more information, see "Using the Configuration Tool CLI Docker image" on page 95.

Client-side library analysis and Debricked settings

The hacker-level insights check has been enhanced to include information from the National Vulnerability Database (NVD) as well as Debricked health metrics.

NVD information

If you select a policy in your scan settings that has the **Hacker Level Insights (HLI) Detected Libraries** check enabled, and a vulnerable library is detected on the client side, information from a local copy of the NVD about common vulnerabilities and exposures (CVE) will be included in the vulnerability description.

Note: The NVD is shipped with the OpenText DAST (Fortify WebInspect) installer or with the Docker image. It is updated once per release, and is not updated between releases.

You can learn more about the National Vulnerability Database (NVD) at https://nvd.nist.gov/.

Debricked health metrics

If the detected library is open source, and you have a subscription to Debricked and have configured ScanCentral DAST with your Debricked access token, then information about the library contributors, popularity, and security will be retrieved from the Debricked database and included in the vulnerability description.

A Debricked configuration also extends the local NVD and includes the newest CVEs. If there are no records for a CVE inside the local NVD, then data about the CVE and its description will be obtained from the Debricked database.

The Debricked information may also include correlated GitHub Security Advisory (GHSA) information for open source projects.

You can learn more about the Debricked health metrics at https://portal.debricked.com/project-health-45. You can learn more about GitHub Security Advisories at https://docs.github.com/.

Debricked content contingent upon access

If the Debricked service is down or unreachable for any reason at the start of a scan, the scan will continue. However, if access to the Debricked service has not been established upon scan completion, then Debricked information will not be included in the scan results.

Configuring access to Debricked

To include the Debricked health metrics, you must provide your Debricked access token in the settings file when you install or manage your ScanCentral DAST environment.

Tip: To disable Debricked integration, run the Config Tool CLI with empty double quotation marks (`""`) in the JSON file or an empty string in the YAML file to remove the access token and return the configuration to the default state.

JSON example

The following JSON example shows the Debricked setting.

```
  "DebrickedSettings": {
     "AccessToken": "<access_token>"
   }
```

YAML example

The following YAML example shows the Debricked setting.

```
debrickedSettings:
   accessToken: <access_token>
```

Fortify Connect server settings

You can use the Configuration Tool CLI to configure Fortify Connect server settings for scanning applications that are hidden behind your firewall. For more information, see "Working with Fortify Connect for private application scanning" on page 317.

Important! When using the Configuration Tool CLI to configure Fortify Connect, an `ssh-keygen` tool must be installed on the computer where the Configuration Tool CLI will run.

Tip: If Fortify Connect is not needed, then omit `FortifyConnectServerSettings` from your settings file or set the value to null. For example:

```
"FortifyConnectServerSettings": null
```

Note: The Fortify Connect server is available as a Linux® image only. The Fortify Connect server is not supported on Microsoft Windows® containers.

JSON example

The following JSON example shows the Fortify Connect server settings.

```
  "FortifyConnectServerSettings": {
       "DisableFortifyConnectServer": false,
       "InternalHost": "<Internal_FortifyConnect_Server_Host>",
       "InternalPort": <Port_Number>,
```

```
      "ExternalHost": "<External_FortifyConnect_Server_Host>",
      "ExternalPort": <Port_Number>,
      "KeyPassphrase": "<Pass_Phrase>",
      "PrivateKeyContents": "",
      "PublicKeyContents": ""
    }
```

YAML example

The following YAML example shows the Fortify Connect server settings.

```
fortifyConnectServerSettings:
    disableFortifyConnectServer: false
    internalHost: <Internal_FortifyConnect_Server_Host>
    internalPort: <Port_Number>
    externalHost: <External_FortifyConnect_Server_Host>
    externalPort: <Port_Number>
    keyPassphrase: <Pass_Phrase>
    privateKeyContents: ''
    publicKeyContents: ''
```

Parameter descriptions

The following table describes the parameters for the Fortify Connect server settings.

Parameter	Description
`disableFortifyConnectServer`	Required setting that disables or enables Fortify Connect. Allowed values are `true`, which disables Fortify Connect, and `false`, which enables it. **Tip:** You can use this parameter to disable Fortify Connect while retaining previously saved Fortify Connect settings.
`internalHost`	Required setting that specifies the internal IP address or host name for the Fortify Connect server in the cloud.
`internalPort`	Required setting that specifies the internal port on which the Fortify Connect server will run for secure proxy connections in the cloud. The default port number is `2022`.

Parameter	Description
`externalHost`	Required setting that specifies the external IP address or host name for the Fortify Connect Server in the internal network.
`externalPort`	Required setting that specifies the external port on which the Fortify Connect server will run for secure proxy connections in the internal network. The default port number is `2022`. **Important!** This port must be open in the firewall for the client to be able to connect to the server.
`keyPassphrase`	Required setting that identifies a passphrase that is used by the Fortify Connect server for generating certificates and accepting client connections. **Important!** OpenText recommends using an encrypted key passphrase. The key passphrase can be encrypted using the Configuration Tool CLI `encrypt` command. For more information, see "Encrypting values" on page 101. To generate a new key, type a new `keyPassphrase` and set the `privateKeyContents` and `publicKeyContents` parameters to empty values (`''`).
`privateKeyContents`	Required setting that identifies the private key of the key pair used for encryption. Set this parameter to an empty value (`''`) to generate a new key or use the existing key that is stored in the ScanCentral DAST database. To use a pre-generated key, use the base64-encoded key.
`publicKeyContents`	Required setting that identifies the public key of the key pair used for encryption. Set this parameter to an empty value (`''`) to generate a new key or use the existing key that is stored in the ScanCentral DAST database.

Parameter	Description
	To use a pre-generated key, use the base64-encoded key.

JSON sample file

After you have configured the various settings in your JSON file, they should resemble the following sample.

```
{
  "DatabaseSettings":{
    "DatabaseProvider": "<database_type>",
    "Server": "<ip_address>,<port>",
    "Database": "<database_name>",
    "CommandTimeout": 600,
    "DboLevelDatabaseAccount": {
      "Username": "<string>",
      "Password": "<string>",
      "UseWindowsAuthentication": false
      "AdditionalConnectionProperties": null
  },
  "StandardDatabaseAccount": {
    "Username": "<string>",
    "Password": "<string>",
    "CreateLogin": false,
    "AdditionalConnectionProperties": null
   }
  },
  "RetainCompletedScans": false,
  "DisableAdvancedScanPrioritization": false,
  "EnableRestrictedScanSettings": false,
  "ServiceToken": "<string>",
  "SmartUpdateSettings": {
    "SmartUpdateUrl": "https://smartupdate.fortify.microfocus.com/",
    "LicensingUrl": "https://licenseservice.fortify.microfocus.com/"
  },
  "SSCSettings": {
    "SSCRootUrl": "http://<ip_address>:<port>/ssc",
    "ServiceAccountUserName": "<username>",
    "ServiceAccountPassword": "<password>"
    "KafkaSettings": {
```

```
      "IsEnabled": true,
      "BootstrapServers": "<broker1>,<broker2>,<broker3>",
      "FindingAuditGroupId": "<SCDAST_FindingAuditGroup>",
      "FindingAuditTopic": "<FindingAuditTopic>"
      "SecurityProtocolType": "SSL",
      "SSLSettings": {
        "CALocation": "/<directory_path>/<cert_name>.cer",
        "CertificateLocation": "/<directory_path>/<cert_name>.cer",
        "EnableSslCertificateVerification": true,
        "KeyLocation": "/<directory_path>/<cert_name>.key",
        "KeyPassword": "<password>"
      }
    }
  },
  "SCDASTApiSettings": {
    "RootUrl": "http://<hostname>:<port>",
    "DisableCorsOrigins": false,
    "CorsOrigins": [
      "http://<hostname>:<port>",
      "http://<hostname>:<port>",
      "http://<ip_address>:<port>"
    ]
  },
  "LIMSettings": {
    "LimUrl": "https://<location>:<port>",
    "ServiceAccountUserName": "<string>",
    "ServiceAccountPassword": "<string>",
    "DefaultLimPoolName": "<string>",
    "DefaultLimPoolPassword": "<string>",
  },
  "UtilityWorkerServiceSettings": {
    "RootUrl": "https://<ip_address>:<port>/"
  },
  "EnvironmentSettings": {
    "AllowNonTrustedServerCertificate": true,
    "ProxySettings": {
      "UseProxy": false,
      "ProxyAddress": "<ip_address>",
      "ProxyPassword": "<string>",
      "ProxyUserName": "<string>",
      "ProxyBypassList": "<hostname>,<ip_address>"
    }
```

```
  },
  "ApplySecureBase": true,
  "SecureBasePath": "/<path_to_securebase_data>/DefaultData.zip",
  "DebrickedSettings": {
    "AccessToken": "<access_token>"
    }
  "FortifyConnectServerSettings": {
    "DisableFortifyConnectServer": false,
    "InternalHost": "<Internal_FortifyConnect_Server_Host>",
    "InternalPort": <Port_Number>,
    "ExternalHost": "<External_FortifyConnect_Server_Host>",
    "ExternalPort": <Port_Number>,
    "KeyPassphrase": "<Pass_Phrase>",
    "PrivateKeyContents": "",
    "PublicKeyContents": ""
  }
}
```

YAML sample file

After you have configured the various settings in your YAML file, they should resemble the following sample.

```
databaseSettings:
  databaseProvider: <database_type>
  server: <ip_address>,<port>
  database: <database_name>
  commandTimeout: 600
  dboLevelDatabaseAccount:
    username: <string>
    password: <string>
    useWindowsAuthentication: false
    additionalConnectionProperties: null
  standardDatabaseAccount:
    username: <string>
    password: <string>
    createLogin: false
    additionalConnectionProperties: null
retainCompletedScans: false
disableAdvancedScanPrioritization: false
enableRestrictedScanSettings: false
```

```
serviceToken: <string>
smartUpdateSettings:
  smartUpdateUrl: https://smartupdate.fortify.microfocus.com/
  licensingUrl: https://licenseservice.fortify.microfocus.com/
sSCSettings:
  sSCRootUrl: http://<hostname>:<port>/ssc
  serviceAccountUserName: <username>
  serviceAccountPassword: <password>
  kafkaSettings:
    isEnabled: true
    bootstrapServers: <broker1>,<broker2>,<broker3>
    findingAuditGroupId: <SCDAST_FindingAuditGroup>
    findingAuditTopic: <FindingAuditTopic>
    securityProtocolType: SSL
    sSLSettings:
      cALocation: /<directory_path>/<cert_name>.cer
      certificateLocation: /<directory_path>/<cert_name>.cer
      enableSslCertificateVerification: true
      keyLocation: /<directory_path>/<cert_name>.key
      keyPassword: <password>
sCDASTApiSettings:
  rootUrl: http://<ip_address>:<port>
  disableCorsOrigins: false
  corsOrigins:
  - http://<hostname>:<port>
  - http://<hostname>:<port>
  - http://<ip_address>:<port>
lIMSettings:
  limUrl: https://<location>:<port>
  serviceAccountUserName: <string>
  serviceAccountPassword: <string>
  defaultLimPoolName: <string>
  defaultLimPoolPassword: <string>
utilityWorkerServiceSettings:
  rootUrl: https://<hostname>:<port>/
environmentSettings:
  allowNonTrustedServerCertificate: true
  proxySettings:
    useProxy: false
    proxyAddress: '<ip_address>'
    proxyPassword: '<string>'
    proxyUserName: '<string>'
```

```
    proxyBypassList: <hostname>,<ip_address>
applySecureBase: true
secureBasePath: /<path_to_securebase_data>/DefaultData.zip
debrickedSettings:
    accessToken: <access_token>
fortifyConnectServerSettings:
    disableFortifyConnectServer: false
    internalHost: <Internal_FortifyConnect_Server_Host>
    internalPort: <Port_Number>
    externalHost: <External_FortifyConnect_Server_Host>
    externalPort: <Port_Number>
    keyPassphrase: <Pass_Phrase>
    privateKeyContents: ''
    publicKeyContents: ''
```

Using the Configuration Tool CLI

To assist you in setting up and maintaining the ScanCentral DAST components, OpenText engineers have created the ScanCentral DAST Configuration Tool CLI. The tool uses command line parameters and a configuration file to configure the ScanCentral DAST environment. The tool enables you to perform the following tasks:

- Create and configure a new ScanCentral DAST environment
- Upgrade all ScanCentral DAST components from one version to another
- Change ScanCentral DAST settings, such as a proxy or database account information, without upgrading the version

Versions available

The Configuration Tool CLI is available as an executable (EXE) file and as Docker images.The EXE file is included in the download package. For environments lacking Internet access, TAR files *with* a SecureBase are available. Contact Customer Support for the TAR files.

About the images on DockerHub

The Configuration Tool CLI Docker images *without* SecureBase are available in the Fortify Docker repository on DockerHub.

The Fortify Docker repository uses the following naming convention for the Fortify Configuration Tool CLI images:

`fortifydocker/scancentral-dast-config:<version>`

The latest image versions that are available as of this writing are:

- `fortifydocker/scancentral-dast-config:26.4` – for Windows
- `fortifydocker/scancentral-dast-config:26.4.ubi.9` – for RedHat Linux distribution

Deciding which Configuration Tool CLI to use

OpenText recommends that you use the executable file or the DockerHub image for the following tasks which do not involve the `DefaultData.zip` file:

- Installing, updating, or managing a ScanCentral DAST environment at sites with Internet access
- Creating a settings file or migration script
- Encrypting a password or token

For more information, see "Using the executable file" below.

OpenText recommends that you use one of the TAR files for the following tasks which will seed the database with the embedded `DefaultData.zip` file:

- Installing or updating a ScanCentral DAST environment at sites lacking Internet access

Using the executable file

The following paragraphs describe where to find the EXE file and how to use the program.

Locating the EXE file

The `SCDAST.ConfigurationToolCLI.exe` file is included in the Fortify ScanCentral DAST software download package (a ZIP file).

Launching the CLI

To launch the command-line interface (CLI):

- Right-click the Windows **Command Prompt** (cmd.exe) application, and select **Run as administrator**.

  The Administrator: Command Prompt window appears.

Important! At the command prompt, use the `cd` command to change the current working directory to the directory where the Configuration Tool CLI application resides.

Using the Configuration Tool CLI

To use the Configuration Tool CLI:

- At the command prompt, use the following syntax:
  `SCDAST.ConfigurationToolCLI.exe <CLI_Command>`

For more information on the CLI commands, see the following:

- "Exporting an existing settings file" on page 97
- "Configuring the environment" on page 99
- "Using environment variables" on page 100
- "Encrypting values" on page 101
- "Generating a migration script" on page 101
- "Generating a connection string" on page 103

Accessing the help

To view the Configuration Tool CLI help:

- At the command prompt, type `SCDAST.ConfigurationToolCLI.exe -h`.

Using the Configuration Tool CLI Docker image

The Configuration Tool CLI Docker image is used in the Helm chart for Kubernetes. However, you can also use the image to configure your ScanCentral DAST environment outside of Kubernetes.

Note: The Configuration Tool CLI includes two sample settings files: `SampleSettingsFile.json` and `SampleSettingsFile.yaml`.

The procedures in this topic use these file names. For convenience, you can edit these files with settings that are specific for your environment, and use them in the Docker run command.

Getting the image from DockerHub

To pull the current version of the ScanCentral DAST Configuration Tool CLI image:

- In PowerShell, enter the following command:
  `docker pull fortifydocker/scancentral-dast-config:26.4`

Running the container

The following procedure describes how to attach the configuration file to the container as a volume.

To run the container:

1. Create a directory to store the configuration file. For example, `C:\config`.

   Important! Make sure that this directory can be read by all users. Otherwise, the container user might not be able to read the directory contents.

2. At the command prompt, enter the following command to copy the configuration file to be shared with the container to the directory you created in step 1:

   ```
   cp SampleSettingsFile.yaml C:\config\
   ```

3. Continue according to the following table.

To run this image	Use the following syntax in the Docker run command
scancentral-dast-config:26.4.ubi.9	`docker run --rm -v <Config_Dir_Full_Path>:C:/app/logs fortifydocker/scancentral-dast-config:26.4.ubi.9 <CLI_Commands>`
scancentral-dast-config:26.4	`docker run --rm -v <Config_Dir_Full_Path>:C:\app\logs fortifydocker/scancentral-dast-config:26.4 <CLI_Commands>`

   Note: Mapping the volume to the `C:\app\logs` directory on the host system in the Docker run command exposes the log file to your workstation.

   When using the Docker image, you must add CLI commands to the *end* of the Docker run command. The following example shows the `configureEnvironment` command with the `--mode` and `--settingsFile` parameters:

   ```
   docker run --rm -v C:\config:C:\app\logs fortifydocker/scancentral-
      dast-config:26.4 configureEnvironment --mode autodeploy
      --settingsFile C:\app\logs\SampleSettingsFile.yaml
   ```

   You must pass in command parameters by way of environment variables *before* the image name reference, as shown in the following example:

   ```
   docker run --rm -v <Config_Dir_Full_Path>:C:\config\ -e
      "<environmentVariableName>=<value>" fortifydocker/scancentral-dast-
      config:26.4 <CLI_Commands>
   ```

The following run command updates SecureBase in an offline environment with `SecureBasePath` set to `/app/logs/DefaultData.zip` as recommended by Open Text:

```
docker run --rm -v ~/scdast:/app/logs fortifydocker/scancentral-dast-
   config:26.4.ubi.9 configureenvironment --mode autodeploy --
   settingsFile /app/logs/<SampleSettingsFile>.yaml
```

For more information on the CLI commands, see the following:

- "Exporting an existing settings file" below
- "Configuring the environment" on page 99
- "Using environment variables" on page 100
- "Encrypting values" on page 101
- "Generating a migration script" on page 101
- "Generating a connection string" on page 103

Understanding the Docker CLI options

The following table describes the Docker CLI options used in "Running the container" on page 95.

Option	Description
--rm	Automatically removes the container when it exits.
-v	Maps the volume (or folder) from the container to a folder on the host system. Separate multiple folder names with a colon.

Exporting an existing settings file

If you have an existing ScanCentral DAST environment, you can use the `createSettingsFile` command to export a settings file that contains the current settings for the existing environment.

Understanding the createSettingsFile command

The `createSettingsFile` command includes the parameters shown in the following syntax sample.

```
SCDAST.ConfigurationToolCLI.exe createSettingsFile
   --dbProvider <SQLServer | PostgreSQL | AzureSQLServer |
   AzurePostgreSQL | AmazonRdsSQLServer | AmazonRdsPostgreSQL>
   --server <string> --database <string> --username <string>
```

```
    --password <string> --useWindowsAuthentication
    --additionalConnectionProperties <string>
    --settingsFileType <yaml | json> --outputDirectory <string>
```

The following table describes the `createSettingsFile` parameters.

Parameter	Description
`--dbProvider`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`--server`	Specifies the database server name or the server IP address. **Important!** If SQL Server Browser is not running and you are using a port other than 1433, then you must also specify the port. Use the following format: *<server_name>*,*<port>* *<ip_address>*,*<port>* Note that a comma separates the values.
`--database`	Specifies the name of the database.
`--username`	Indicates the database account user name. **Note:** With an existing database, you can use the non-DBO credentials.
`--password`	Indicates the database account password.
`--settingsFileType`	Specifies the file type for the settings file. Options are `json` or `yaml`.
`--outputDirectory`	Specifies the directory path where the settings

Parameter	Description
	file will be written.
`--internalIdentityProviderSettings`	Specifies the internal identity provider that is used for service-to-service communication. For more information, see Miscellaneous ScanCentral DAST settings.

Configuring the environment

After you configure your settings file, you can use the Configuration Tool CLI to configure the database and default data.

Before you begin

All ScanCentral DAST components must be offline (not running) when using the CLI tool.

Understanding the configureEnvironment command

The `configureEnvironment` command includes the parameters shown in the following syntax sample.

```
SCDAST.ConfigurationToolCLI.exe configureEnvironment
   --mode <new | upgrade | manage | autodeploy>
   --settingsFile <string>
```

The following table describes the `configureEnvironment` parameters.

Parameter	Description
`--mode`	Indicates the intended function of the settings file. Options are: • `new` – Creates and configures a new ScanCentral DAST environment • `upgrade` – Upgrades all ScanCentral DAST components from one version to another • `manage` – Changes ScanCentral DAST settings, such as a proxy or database account information, or uploads new SecureBase content, without upgrading the version • `autodeploy` – Detects whether the database exists. If no, then the `new` function is performed. Otherwise, the database is updated or managed.

Parameter	Description
`--settingsFile`	Specifies the directory path and name of the settings file to use for creating, managing, or upgrading a ScanCentral DAST environment. The file can be either JSON or YML file type.

Applying updated settings to containers

When you use the Configuration Tool CLI with the `--mode manage` parameter, you may need to apply the updated settings to one or more of your containers.

The following list describes how to apply settings based on the settings that changed:

- Changing any database setting requires new DAST API, Utility Service, and Global Service containers.
- Changing service ports requires a new container for the service whose port was changed.
- Changing DAST API SSL settings requires a new container for the DAST API.
- Changing Utility Service SSL settings requires a new container for the Utility Service.
- All other changes are picked up automatically by each service within two minutes of making the change or upon restarting the containers.

Using environment variables

The Configuration Tool CLI enables you to replace placeholders in a settings file with environment variables. This feature protects your sensitive data and supports the use of Kubernetes secrets. For more information on Kubernetes secrets, refer to your Kubernetes configuration documentation.

How replacement works

Each environment variable placeholder in the settings file is replaced with an environment variable value. If no environment variable value is available, then the value will not be replaced.

The replacement values are not written to the source settings file. Instead, the Configuration Tool CLI creates a temporary copy of the settings file that contains the values to be used.

Format and usage

The format of the placeholder in the settings file is as follows:

```
${environment variable name}
```

The following sample shows an environment variable with the name `my_secret_password` in a YAML settings file.

```
databaseSettings:
  databaseProvider: SQLServer
  server: .
  database: DAST
  dboLevelDatabaseAccount:
    username: myusername
    password : ${my_secret_password}
    useWindowsAuthentication: false
    additionalConnectionProperties:
```

Encrypting values

The Configuration Tool CLI provides the `encrypt` command that encrypts a value. This feature enables you to encrypt sensitive data, such as passwords, to use in a settings file.

If the value to be encrypted contains spaces, then the value must be enclosed in double quotation marks (").

The `encrypt` command is shown in the following sample.

```
SCDAST.ConfigurationToolCLI.exe encrypt "<string>"
```

The encrypted value is logged to the console as "`encrypt result: {encrypted value}`".

Generating a migration script

The Configuration Tool CLI provides the `generateMigrationScript` command that generates a migration script that you can run on the database server. This feature is useful in environments where policies do not allow applications to change database schema and require a manual script to run.

All non-optional parameters are required and are validated upon execution. If any parameter fails validation, a message is written to the log file and the application exits with a -1.

Migration script name

The generated migration script is named: `SCDAST-Migration-MMddyyyyHHmmss.sql`. The time stamp in the name is composed of the following:

- `MM` – Month, with a leading 0
- `dd` – Day, with a leading 0

- `yyyy` – 4-digit year
- `HH` – 24-hour clock hour, with a leading 0
- `mm` – Minutes, with a leading zero
- `ss` – Seconds, with a leading zero

Understanding the generateMigrationScript command

The `generateMigrationScript` command includes the parameters shown in the following sample.

```
SCDAST.ConfigurationToolCLI.exe generateMigrationScript
   --dbProvider <SQLServer | PostgreSQL | AzureSQLServer |
   AzurePostgreSQL | AmazonRdsSQLServer | AmazonRdsPostgreSQL>
   --server <string> --database <string> --username <string>
   --password <string> --useWindowsAuthentication
   --additionalConnectionProperties <string> --outputDirectory <string>
```

The following table describes the parameters for the `generateMigrationScript` command.

Parameter	Description
`--dbProvider`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`--server`	Specifies the database server name or IP address.
`--database`	Specifies the database name.
`--username`	Indicates the database account user name to connect to the database. This parameter is not required if `-useWindowsAuthentication` is used.
`--password`	Indicates the database account password to

Parameter	Description
	connect to the database. This parameter is not required if `-useWindowsAuthentication` is used.
`--useWindowsAuthentication`	Indicates that the connection should use Windows authentication.
`--additionalConnectionProperties`	Optionally, specifies any additional connection properties for the database, such as `trustServerCertificate`. For more information about additional connection properties, refer to your SQL database documentation.
`--outputDirectory`	Optionally, indicates the directory path where the migration script will be saved. If not specified, the script will be saved in the current working directory. **Note:** If the specified directory does not exist, it will be created.

Generating a connection string

The Configuration Tool CLI can generate a connection string for connecting to your ScanCentral DAST database. All non-optional parameters are required and are validated upon execution. If a parameter fails validation, a message is written to the log file and the application exits with a -1.

Understanding the generateConnectionString command

The `generateConnectionString` command includes the parameters shown in the following sample.

```
SCDAST.ConfigurationToolCLI.exe generateConnectionString --dbProvider
   <SQLServer | PostgreSQL | AzureSQLServer | AzurePostgreSQL |
   AmazonRdsSQLServer | AmazonRdsPostgreSQL> --server <string>
   --database <string> --username <string> --password <string>
   --useWindowsAuthentication --additionalConnectionProperties <string>
   --encrypt
```

The following table describes the parameters for the `generateConnectionString` command.

Parameter	Description
`--dbProvider`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`--server`	Specifies the database server name or IP address.
`--database`	Specifies the database name.
`--username`	Indicates the database account user name to connect to the database. This parameter is not required if `--useWindowsAuthentication` is used.
`--password`	Indicates the database account password to connect to the database. This parameter is not required if `--useWindowsAuthentication` is used. **Important!** Use double quotation marks if your password includes any of the following special characters: :, {, }, [,], ,, &, *, #, ?, |, -, <, >, =, !, %, @, \, `
`--useWindowsAuthentication`	Indicates that the connection should use Windows authentication.
`--additionalConnectionProperties`	Optionally, specifies any additional connection properties for the database, such as `trustServerCertificate`. For more information about additional

Parameter	Description
	connection properties, refer to your SQL database documentation.
`--encrypt`	Encrypts the results.

Understanding the Docker compose and environment files

You must use Docker compose files to pull ScanCentral DAST images from DockerHub and start the containers. The Docker compose files reference variables that are configured in environment files. Sample Docker compose files and environment files are included in the ScanCentral DAST software download package. You can edit these sample environment files with the specific settings required to properly configure your ScanCentral DAST environment.

For more information, see the following topics:

- "Configuring the TLS environment file for core components" on the next page
- "Configuring the mTLS environment file for core components" on page 112
- "Configuring the TLS environment file for the scanner service" on page 109
- "Configuring the mTLS environment file for the scanner service" on page 120

Versions available

Sample Docker compose files and their corresponding environment files are available for Linux® operating systems, including Docker compose files and environment files for Transport Layer Security (TLS) authentication and for mutual TLS (mTLS) authentication. Additionally, Docker compose files and environment files are available for PostgreSQL® and SQLExpress versions of the sensor database.

You must configure the variables in the appropriate environment files based on the type of TLS authentication you are using and the type of sensor database. The files are organized software download package into folders based on authentication type and the sensor database type.

Use the following files for TLS authentication:

- `docker-compose-tls.yml` and `environment-tls.env` - deploy all ScanCentral DAST services except the DAST scanner service with TLS.
- `docker-compose-tls-scannerservice.yml` and `environment-scannerservice-tls.env` - deploy the DAST scanner service with TLS.

Use the following files for mTLS authentication:

- `docker-compose-mtls.yml` and `environment-mtls.env` - deploy all ScanCentral DAST services except the DAST scanner service with mutual TLS.
- `docker-compose-mtls-scannerservice.yml` and `environment-scannerservice-mtls.env` - deploy the DAST scanner service with mutual TLS.

Configuring the TLS environment file for core components

This topic describes the environment file settings using TLS authentication for the core ScanCentral DAST containers. The environment file name is `environment-tls.env`.

All settings are required unless otherwise indicated.

Database/datastore settings

The following table describes the database and datastore settings.

Setting	Description
`SCDAST_DATABASE_CONNECTIONSTRING`	Specifies the string for connecting to your ScanCentral DAST database. You can use the Configuration Tool CLI to generate a connection string. See "Generating a connection string" on page 103. **Important!** OpenText recommends using an encrypted value.
`SCDAST_DATABASE_DBPROVIDER`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`DATASTORE_CORE_PASSWORD`	Specifies the customer-supplied password for the datastore container. The password is used for

Setting	Description
	communication between the sensor container and the database container. An encrypted value is not supported.

Fortify DAST sensor API settings

The following table describes the Fortify DAST sensor API setting.

Setting	Description
DAST_SCANNER_CORE_API_PORT	Indicates the port used to access the Fortify DAST sensor API . The default setting is 8089.

ScanCentral DAST API settings

The following table describes the ScanCentral DAST API settings.

Setting	Description
SCDAST_API_HOST_PORT	Specifies the scancentral-dast-api port on host machine.
SCDAST_API_CONTAINER_PORT	Specifies the scancentral-dast-api port on the container. The default setting is 443.
SCDAST_API_HOST_CERTIFICATES_DIRECTORY	Specifies the path to the certificates directory on the host machine. For example: /etc/scdast/certificates
SCDAST_API_CONTAINER_CERTIFICATES_DIRECTORY	Specifies the path to the certificates directory in the container. For example: /home/scdastuser/scdast/certificates
SCDAST_API_CERTIFICATES_PATH	Specifies the path to the certificate file. For example: /home/scdastuser/scdast/certificates/dast-api-certificate.pem

Setting	Description
SCDAST_API_CERTIFICATES_KEYPATH	(Optional) If the certificate file requires a key file, specifies the full path to the key file. If not required, remove the line or comment it out. For example: /home/scdastuser/scdast/certificates/dast-api-key.key
SCDAST_API_CERTIFICATES_PASSWORD	(Optional) If the certificate file requires a password, specifies the password. If not required, remove the line or comment it out. **Important!** OpenText recommends using an encrypted value.

ScanCentral DAST Utility Service settings

The following table describes the ScanCentral DAST Utility Service settings.

Setting	Description
SCDAST_UTILITYSERVICE_HOST_PORT	Specifies the scancentral-dast-utilityservice port on the host machine.
SCDAST_UTILITYSERVICE_CONTAINER_PORT	Specifies the scancentral-dast-utilityservice port on the container. The default setting is 443.
SCDAST_UTILITYSERVICE_HOST_CERTIFICATES_DIRECTORY	Specifies the path to the certificates directory on the host machine. For example: /etc/scdast/certificates
SCDAST_UTILITYSERVICE_CONTAINER_CERTIFICATES_DIRECTORY	Specifies the path to the certificates directory in the container. For example: /home/scdastuser/scdast/certificates
SCDAST_UTILITYSERVICE_CERTIFICATES_PATH	Specifies the path to the certificate file. For example: /home/scdastuser/scdast/certificates/dast-utilityservice-certificate.pem
SCDAST_UTILITYSERVICE_	(Optional) If the certificate file requires a key file,

Setting	Description
CERTIFICATES_KEYPATH	specifies the full path to the key file. If not required, remove the line or comment it out. For example: /home/scdastuser/scdast/certificates/dast-utilityservice-key.key
SCDAST_UTILITYSERVICE_CERTIFICATES_PASSWORD	(Optional) If the certificate file requires a password, specifies the password. If not required, remove the line or comment it out. **Important!** OpenText recommends using an encrypted value.

Optional Fortify Connect settings

The following table describes Fortify Connect settings. If your environment does not use Fortify Connect, this section can be removed or commented out.

Setting	Description
FORTIFYCONNECT_HOST_PORT	Specifies the Fortify Connect port on the host machine.
FORTIFYCONNECT_CONTAINER_PORT	Specifies the scancentral-dast-utilityservice port on the container. The default setting is 2022.
FORTIFYCONNECT_PUBLIC_KEY_CONTENTS	Specifies the base64 encoded public key. **Important!** OpenText recommends using an encrypted value.

Configuring the TLS environment file for the scanner service

This topic describes the environment file settings using TLS authentication for the scanner service (or sensor) container. The environment file name is environment-tls.env.

Datastore setting

The following table describes the required datastore setting.

Setting	Description
DATASTORE_PASSWORD	Specifies the customer-supplied password for the datastore container. The password is used for communication between the sensor container and the database container. An encrypted value is not supported.

Two-factor authentication setting

The following table describes the setting that is required for conducting scans using two-factor authentication.

Setting	Description
FORTIFY_2FA_MASTER_TOKEN	Specifies the master token for the 2FA server. For more information, see "Generating a 2FA master token" below.

Generating a 2FA master token

You must provide a master token to use as an environment variable in the environment file and in the ScanCentral DAST user interface when configuring the 2FA Server. You can generate a master token in Linux for this purpose.

Important! The master token is not stored on the host machine. Be sure to save it for use in the environment file and configuring the 2FA Server in ScanCentral DAST.

To generate a master token in Linux:

1. At the terminal prompt, enter the following commands:

   ```
   MASTER_TOKEN=$(uuidgen)
   echo "$MASTER_TOKEN"
   ```

   Linux returns a GUID similar to the one shown here.

   ```
   90fc1ea9-723f-4cc9-8a65-d231c7af73d4
   ```

2. Copy the GUID and paste it as the value for the `FORTIFY_2FA_MASTER_TOKEN` environment variable as shown in the following example:

```
# twofa settings
FORTIFY_2FA_MASTER_TOKEN={90fc1ea9-723f-4cc9-8a65-d231c7af73d4}
```

Fortify DAST sensor API settings

The following table describes the Fortify DAST sensor API setting.

Setting	Description
`DAST_SCANNER_API_PORT`	Indicates the port used to access the Fortify DAST sensor API . The default setting is `8089`.

ScanCentral DAST scanner service settings

The following table describes the ScanCentral DAST scanner service settings.

Setting	Description
`ALLOW_NON_TRUSTED_SERVER_CERTIFICATE`	Indicates whether self-signed or untrusted server certificates are allowed. The default setting is `false`.
`SCDAST_API_ROOT_URL`	Specifies the URL for the ScanCentral DAST API that was configured in the settings file. For more information, see "ScanCentral DAST API settings" on page 76.
`SCDAST_API_SERVICE_TOKEN`	Specifies the shared secret that all your DAST sensors must use to authenticate with the ScanCentral DAST API. This is the `ServiceToken` that you configured in the ScanCentral DAST settings. For more information, see "Miscellaneous ScanCentral DAST settings" on page 66. **Important!** Open Text recommends using an encrypted value.
`SCDAST_API_SCANNER_POOL_ID`	Specifies the sensor pool ID to assign to sensors

Setting	Description
	or set to `0` for the default sensor pool. The default setting is `0`.

Configuring the mTLS environment file for core components

This topic describes the environment file settings using mTLS authentication for the core ScanCentral DAST containers. The environment file name is `environment-mtls.env`.

All parameters are required unless otherwise indicated.

Database/datastore settings

The following table describes the database and datastore settings.

Setting	Description
`SCDAST_DATABASE_CONNECTIONSTRING`	Specifies the string for connecting to your ScanCentral DAST database. You can use the Configuration Tool CLI to generate a connection string. See "Generating a connection string" on page 103. **Important!** OpenText recommends using an encrypted value.
`SCDAST_DATABASE_DBPROVIDER`	Identifies the type of SQL database being used. Valid providers are: • `SQLServer` • `PostgreSQL` • `AzureSQLServer` • `AzurePostgreSQL` • `AmazonRdsSQLServer` • `AmazonRdsPostgreSQL`
`DATASTORE_CORE_PASSWORD`	Specifies the customer-supplied password for the datastore container. The password is used for communication between the sensor container and

Setting	Description
	the database container. An encrypted value is not supported.

Fortify DAST sensor API settings

The following table describes the Fortify DAST sensor API setting.

Setting	Description
DAST_SCANNER_CORE_API_PORT	Indicates the port used to access the Fortify DAST sensor API . The default setting is 8089.

ScanCentral DAST API settings

The following table describes the ScanCentral DAST API settings.

Setting	Description
SCDAST_API_HOST_PORT	Specifies the scancentral-dast-api port on host machine.
SCDAST_API_CONTAINER_PORT	Specifies the scancentral-dast-api port on the container. The default setting is 443.
SCDAST_API_HOST_CERTIFICATES_DIRECTORY	Specifies the path to the certificates directory on the host machine. For example: /etc/scdast/certificates
SCDAST_API_CONTAINER_CERTIFICATES_DIRECTORY	Specifies the path to the certificates directory in the container. For example: /home/scdastuser/scdast/certificates
SCDAST_API_CERTIFICATES_PATH	Specifies the path to the certificate file. For example: /home/scdastuser/scdast/certificates/dast-api-certificate.pem

Setting	Description
SCDAST_API_CERTIFICATES_KEYPATH	(Optional) If the certificate file requires a key file, specifies the full path to the key file. If not required, remove the line or comment it out. For example: /home/scdastuser/scdast/certificates/dast-api-key.key
SCDAST_API_CERTIFICATES_PASSWORD	(Optional) If the certificate file requires a password, specifies the password. If not required, remove the line or comment it out. **Important!** OpenText recommends using an encrypted value.

ScanCentral DAST API mTLS certificate settings

The following table describes the ScanCentral DAST API mTLS certificate settings.

Setting	Description
SCDAST_API_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_ENABLED	If set to `true` the code will use `ChainTrustValidationModeType` to determine what type of validation to use. If set to false, default certificate validation is used. The default setting is `true`.
SCDAST_API_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_ALLOWEDCERTIFICATETYPES	Specifies the allowed certificate types. Options are `All`, `Chained`, and `SelfSigned`. The default setting is `All`.
SCDAST_API_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_REVOCATIONMODETYPE	Indicates whether to check a certificate revocation list (CRL). Options are: • `NoCheck` = Do not perform a revocation check on the certificate. • `Online` = Perform a revocation check using an online CRL. • `Offline` = Perform a revocation check using a cached CRL.

Setting	Description
	The default setting is `NoCheck`.
`SCDAST_API_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_CHAINTRUSTVALIDATIONMODETYPE`	Indicates which root trust certificates to use. Options are: • `CustomRootTrust` = Use certificates in the CustomRootTrustDirectory instead of the default root trust. • `System` = Use the default (system) root trust. The default setting is `CustomRootTrust`.
`SCDAST_API_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_CUSTOMROOTTRUSTDIRECTORY`	Specifies the path to the certificates directory in the container. For example: `/home/scdastuser/scdast/certificates/ca-certificates` Any `.pfx`, `.p12`, `.pem`, `.cer`, or `.crt` file in the directory will be added to the custom root trust. This setting is required if `SCDAST_API_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_CHAINTRUSTVALIDATIONMODETYPE` is set to `CustomRootTrust`.
`SCDAST_API_CERTIFICATEFORWARDINGSETTINGS_ENABLED`	Indicates whether a proxy or load balancer is used and the client certificate is forwarded in the header. The default setting is `false`.
`SCDAST_API_CERTIFICATEFORWARDINGSETTINGS_CERTIFICATEHEADER`	Indicates the header name that will contain the client certificate. For example: `X-SSL-CERT` This setting is required if `SCDAST_API_CERTIFICATEFORWARDINGSETTINGS_ENABLED` is set to `true`.
`SCDAST_API_CERTIFICATEFORWARDINGSETTINGS_URLDECODECERTIFICATE`	Indicates whether the proxy or load balancer URL encodes the client certificate.

Setting	Description
	The default setting is `false`.

ScanCentral DAST Utility Service settings

The following table describes the ScanCentral DAST Utility Service settings.

Setting	Description
`SCDAST_UTILITYSERVICE_HOST_PORT`	Specifies the scancentral-dast-utilityservice port on the host machine.
`SCDAST_UTILITYSERVICE_CONTAINER_PORT`	Specifies the scancentral-dast-utilityservice port on the container. The default setting is `443`.
`SCDAST_UTILITYSERVICE_HOST_CERTIFICATES_DIRECTORY`	Specifies the path to the certificates directory on the host machine. For example: `/etc/scdast/certificates`
`SCDAST_UTILITYSERVICE_CONTAINER_CERTIFICATES_DIRECTORY`	Specifies the path to the certificates directory in the container. For example: `/home/scdastuser/scdast/certificates`
`SCDAST_UTILITYSERVICE_CERTIFICATES_PATH`	Specifies the path to the certificate file. For example: `/home/scdastuser/scdast/certificates/dast-utilityservice-certificate.pem`
`SCDAST_UTILITYSERVICE_CERTIFICATES_KEYPATH`	(Optional) If the certificate file requires a key file, specifies the full path to the key file. If not required, remove the line or comment it out. For example: `/home/scdastuser/scdast/certificates/dast-utilityservice-key.key`
`SCDAST_UTILITYSERVICE_CERTIFICATES_PASSWORD`	(Optional) If the certificate file requires a password, specifies the password. If not required, remove the line or comment it out. **Important!** OpenText recommends using an encrypted value.

ScanCentral DAST Utility Service mTLS certificate settings

The following table describes the ScanCentral DAST Utility Service mTLS certificate settings.

Setting	Description
`SCDAST_UTILITYSERVICE_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_ENABLED`	If set to `true` the code will use `ChainTrustValidationModeType` to determine what type of validation to use. If set to false, default certificate validation is used. The default setting is `true`.
`SCDAST_UTILITYSERVICE_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_ALLOWEDCERTIFICATETYPES`	Specifies the allowed certificate types. Options are `All`, `Chained`, and `SelfSigned`. The default setting is `All`.
`SCDAST_UTILITYSERVICE_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_REVOCATIONMODETYPE`	Indicates whether to check a certificate revocation list (CRL). Options are: • `NoCheck` = Do not perform a revocation check on the certificate. • `Online` = Perform a revocation check using an online CRL. • `Offline` = Perform a revocation check using a cached CRL. The default setting is `NoCheck`.
`SCDAST_UTILITYSERVICE_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_CHAINTRUSTVALIDATIONMODETYPE`	Indicates which root trust certificates to use. Options are: • `CustomRootTrust` = Use certificates in the CustomRootTrustDirectory instead of the default root trust. • `System` = Use the default (system) root trust. The default setting is `CustomRootTrust`.
`SCDAST_UTILITYSERVICE_ADDITIONALCERTIFICATEAUTHENTICATIONSE`	Specifies the path to the certificates directory in the container. For example:

Setting	Description
TTINGS_CUSTOMROOTTRUSTDIRECTORY	/home/scdastuser/scdast/certificates/ca-certificates Any .pfx, .p12, .pem, .cer, or .crt file in the directory will be added to the custom root trust. This setting is required if SCDAST_UTILITYSERVICE_ADDITIONALCERTIFICATEAUTHENTICATIONSETTINGS_CHAINTRUSTVALIDATIONMODETYPE is set to CustomRootTrust.
SCDAST_UTILITYSERVICE_CERTIFICATEFORWARDINGSETTINGS_ENABLED	Indicates whether a proxy or load balancer is used and the client certificate is forwarded in the header. The default setting is false.
SCDAST_UTILITYSERVICE_CERTIFICATEFORWARDINGSETTINGS_CERTIFICATEHEADER	Indicates the header name that will contain the client certificate. For example: X-SSL-CERT This setting is required if SCDAST_UTILITYSERVICE_CERTIFICATEFORWARDINGSETTINGS_ENABLED is set to true.
SCDAST_UTILITYSERVICE_CERTIFICATEFORWARDINGSETTINGS_URLDECODECERTIFICATE	Indicates whether the proxy or load balancer URL encodes the client certificate. The default setting is false.

Shared client certificate settings

The following table describes the shared client certificate settings.

Setting	Description
SCDASTAPICLIENTCERTIFICATESETTINGS_ENABLED	Indicates whether certificates in the SCDASTAPICLIENTCERTIFICATESETTINGS_CLIENTCERTIFICATESDIRECTORY directory will be sent as client certificates when

Setting	Description
	making requests to the DAST API. The default setting is `true`.
`SCDASTAPICLIENTCERTIFICATESETTINGS_CLIENTCERTIFICATESDIRECTORY`	Specifies the path to the certificates directory in the container. For example: `/home/scdastuser/scdast/certificates/api-client-certificates` Any `.pfx`, `.p12`, `.pem`, `.cer`, or `.crt` file in the directory will be sent as a client certificate when making requests to the DAST API. This setting is required if `SCDASTAPICLIENTCERTIFICATESETTINGS_ENABLED` is set to `true`.
`SCDASTUTILITYWORKERSERVICECLIENTCERTIFICATESETTINGS_ENABLED`	Indicates whether certificates in the `SCDASTUTILITYWORKERSERVICECLIENTCERTIFICATESETTINGS_CLIENTCERTIFICATESDIRECTORY` directory will be sent as client certificates when making requests to the DAST Utility Worker Service. The default setting is `true`.
`SCDASTUTILITYWORKERSERVICECLIENTCERTIFICATESETTINGS_CLIENTCERTIFICATESDIRECTORY`	Specifies the path to the certificates directory in the container. For example: `/home/scdastuser/scdast/certificates/utility-service-client-certificates` Any `.pfx`, `.p12`, `.pem`, `.cer`, or `.crt` file in the directory will be sent as a client certificate when making requests to the DAST Utility Worker Service. This setting is required if `SCDASTUTILITYWORKERSERVICECLIENTCERTIFICATESETTINGS_ENABLED` is set to `true`.

Optional Fortify Connect settings

The following table describes Fortify Connect settings. If your environment does not use Fortify Connect, this section can be removed or commented out.

Setting	Description
`FORTIFYCONNECT_HOST_PORT`	Specifies the Fortify Connect port on the host machine.
`FORTIFYCONNECT_CONTAINER_PORT`	Specifies the scancentral-dast-utilityservice port on the container. The default setting is `2022`.
`FORTIFYCONNECT_PUBLIC_KEY_CONTENTS`	Specifies the base64 encoded public key. **Important!** OpenText recommends using an encrypted value.

Configuring the mTLS environment file for the scanner service

This topic describes the environment file settings using mTLS authentication for the scanner service (or sensor) container. The environment file name is `environment-scannerservice-mtls.env`.

Datastore setting

The following table describes the required datastore setting.

Setting	Description
`DATASTORE_PASSWORD`	Specifies the customer-supplied password for the datastore container. The password is used for communication between the sensor container and the database container. An encrypted value is not supported.

Two-factor authentication setting

The following table describes the setting that is required for conducting scans using two-factor authentication.

Setting	Description
FORTIFY_2FA_MASTER_TOKEN	Specifies the master token for the 2FA server. For more information, see "Generating a 2FA master token" below.

Generating a 2FA master token

You must provide a master token to use as an environment variable in the environment file and in the ScanCentral DAST user interface when configuring the 2FA Server. You can generate a master token in Linux for this purpose.

Important! The master token is not stored on the host machine. Be sure to save it for use in the environment file and configuring the 2FA Server in ScanCentral DAST.

To generate a master token in Linux:

1. At the terminal prompt, enter the following commands:

   ```
   MASTER_TOKEN=$(uuidgen)
   echo "$MASTER_TOKEN"
   ```

   Linux returns a GUID similar to the one shown here.

   ```
   90fc1ea9-723f-4cc9-8a65-d231c7af73d4
   ```

2. Copy the GUID and paste it as the value for the FORTIFY_2FA_MASTER_TOKEN environment variable as shown in the following example:

   ```
   # twofa settings
   FORTIFY_2FA_MASTER_TOKEN={90fc1ea9-723f-4cc9-8a65-d231c7af73d4}
   ```

Fortify DAST sensor API settings

The following table describes the Fortify DAST sensor API setting.

Setting	Description
DAST_SCANNER_API_PORT	Indicates the port used to access the Fortify DAST

Setting	Description
	sensor API . The default setting is `8089`.

ScanCentral DAST scanner service settings

The following table describes the ScanCentral DAST scanner service settings.

Setting	Description
`ALLOW_NON_TRUSTED_SERVER_CERTIFICATE`	Indicates whether self-signed or untrusted server certificates are allowed. The default setting is `false`.
`SCDAST_API_ROOT_URL`	Specifies the URL for the ScanCentral DAST API that was configured in the settings file. For more information, see "ScanCentral DAST API settings" on page 76.
`SCDAST_API_SERVICE_TOKEN`	Specifies the shared secret that all your DAST sensors must use to authenticate with the ScanCentral DAST API. This is the `ServiceToken` that you configured in the ScanCentral DAST settings. For more information, see "Miscellaneous ScanCentral DAST settings" on page 66. **Important!** Open Text recommends using an encrypted value.
`SCDAST_API_SCANNER_POOL_ID`	Specifies the sensor pool ID to assign to sensors or set to `0` for the default sensor pool. The default setting is `0`.

Shared client certificate settings

The following table describes the DAST scanner service settings .

Setting	Description
`DASTAPICLIENTCERTIFICATESETTINGS_ENABLED`	Indicates whether certificates in the

Setting	Description
	DASTAPICLIENTCERTIFICATESETTINGS_CLIENTCERTIFICATESDIRECTORY directory will be sent as client certificates when making requests to the DAST API. The default setting is true.
DASTAPICLIENTCERTIFICATESETTINGS_CLIENTCERTIFICATESDIRECTORY	Specifies the path to the certificates directory in the container. For example: /home/scdastuser/scdast/client-certificates Any .pfx, .p12, .pem, .cer, or .crt file in the directory will be sent as a client certificate when making requests to the DAST API. This setting is required if DASTAPICLIENTCERTIFICATESETTINGS_ENABLED is set to true.

Using the TLS compose file for core components

The docker-compose-tls.yml and environment-tls.env files contains the various service settings required to pull images of the core ScanCentral DAST components and start the containers. You use these files on the host where you want to run these containers.

Using the compose file

Important! To use the compose file, you must first download and install Docker Compose on Linux® on the host machine. For more information, see "Setting up Docker" on page 60.

Use the following process to use the compose file.

Stage	Description
1.	Copy the following files to the host where you want to run the ScanCentral DAST core containers: • docker-compose-tls.yml

Stage	Description
	• `environment-tls.env`
2.	At the terminal prompt, type the following command and press **Enter** to create the Docker network connection: `docker network create --driver bridge wi_net`
3.	At the terminal prompt, type the following command and press **Enter**: `docker compose --env-file environment-tls.env -f docker-compose-tls.yml up -d` You should see a list of the core containers similar to the following: `Container sc-dast-main-scancentral-dast-api-1` `Container sc-dast-main-datastore-core-1` `Container sc-dast-main-scancentral-dast-fortifyconnect-1` `Container sc-dast-main-webinspectapi-core-1` `Container sc-dast-main-scancentral-dast-globalservice-1` `Container sc-dast-main-scancentral-dast-utilityservice-1`

Using the TLS compose file for the sensor

The `docker-compose-tls-scannerservice.yml` and `environment-scannerservice-tls.env` files contain the settings required to pull the sensor images and start the containers. You use these files on the host where you want to run the container.

Using the compose file

Important! To use the compose file, you must first download and install Docker Compose on Linux® on the host machine. For more information, see "Setting up Docker" on page 60.

Use the following process to use the compose file.

Stage	Description
1.	Copy the following files to the host where you want to run the Fortify DAST sensor containers: • `docker-compose-tls-scannerservice.yml` • `environment-scannerservice-tls.env`

Stage	Description
2.	At the terminal prompt, type the following command and press **Enter**: `docker compose --env-file environment-scannerservice-tls.env -f docker-compose-tls-scannerservice.yaml up -d` You should see a list of the sensor containers similar to the following: `Container sc-dast-scanner-datastore-1` `Container sc-dast-scanner-twofa-1` `Container sc-dast-scanner-wise-1` `Container sc-dast-scanner-webinspectapi-1` `Container sc-dast-scanner-dastscannerservice-1`

Using the mTLS compose file for core components

The `docker-compose-mtls.yml` and `environment-mtls.env` files contain the various service settings required to pull images of the core ScanCentral DAST components and start the containers. You use these files on the host where you want to run these containers.

Using the compose file

Important! To use the compose file, you must first download and install Docker Compose on Linux® on the host machine. For more information, see "Setting up Docker" on page 60.

Use the following process to use the compose file.

Stage	Description
1.	Copy the following files to the host where you want to run the ScanCentral DAST core containers: • `docker-compose-mtls.yml` • `environment-mtls.env`
2.	At the terminal prompt, type the following command and press **Enter** to create the Docker network connection: `docker network create --driver bridge wi_net`

Stage	Description
3.	At the terminal prompt, type the following command and press **Enter**: `docker compose --env-file environment-mtls.env -f docker-compose-mtls.yml up -d` You should see a list of the core containers similar to the following: `Container sc-dast-main-scancentral-dast-api-1` `Container sc-dast-main-datastore-core-1` `Container sc-dast-main-scancentral-dast-fortifyconnect-1` `Container sc-dast-main-webinspectapi-core-1` `Container sc-dast-main-scancentral-dast-globalservice-1` `Container sc-dast-main-scancentral-dast-utilityservice-1`

Using the mTLS compose file for the sensor

The `docker-compose-mtls-scannerservice.yml` and `environment-scannerservice-mtls.env` files contain the settings required to pull the sensor images and start the containers. You use these files on the host where you want to run the container.

Using the compose file

Important! To use the compose file, you must first download and install Docker Compose on Linux® on the host machine. For more information, see "Setting up Docker" on page 60.

Use the following process to use the compose file.

Stage	Description
1.	Copy the following files to the host where you want to run the Fortify DAST sensor containers: • `docker-compose-mtls-scannerservice.yml` • `environment-scannerservice-mtls.env`
2.	At the terminal prompt, type the following command and press **Enter**: `docker compose --env-file environment-scannerservice-mtls.env -f docker-compose-mtls-scannerservice.yaml up -d` You should see a list of the sensor containers similar to the following:

Stage	Description
	Container sc-dast-scanner-datastore-1 Container sc-dast-scanner-twofa-1 Container sc-dast-scanner-wise-1 Container sc-dast-scanner-webinspectapi-1 Container sc-dast-scanner-dastscannerservice-1

Using Fortify DAST with the sensor service

You can use a classic OpenText DAST (Fortify WebInspect) installation with the ScanCentral DAST sensor service. To do so, you must first configure and start the Fortify DAST REST API, and then install and configure the DAST sensor service.

Important information about licenses

When running a scan using ScanCentral DAST with the sensor service and an Fortify DAST installation, the license that is configured in the Fortify DAST user interface is overridden to use a LIM license. When the ScanCentral DAST scan is complete, the LIM license is released. The next time you open the Fortify DAST user interface, it will be unlicensed.

As a workaround, reactivate the installed version of Fortify DAST using the previous license in the Fortify DAST UI.

Important prerequisite

Before installing the DAST sensor service, you must install the full ASP.NET Core Runtime version 8.0.0 or later. Otherwise, the following error occurs:

```
A fatal error occurred. The required library hostfxr.dll could not be
found.
If this is a self-contained application, that library should exist in
[C:\ScannerService\].
If this is a framework-dependent application, install the runtime in
the global location [C:\Program Files\dotnet] or use the DOTNET_ROOT
environment variable to specify the runtime location or register the
runtime location in [HKLM\SOFTWARE\dotnet\Setup\InstalledVersions\
x64\InstallLocation].
```

Enabling composite settings in Fortify DAST

ScanCentral DAST uses composite settings, which consist of a JSON version of the scan settings packaged in a ZIP file with any binary files required for the scan, such as macros, client certificates, custom policies, and so forth. When using a classic Fortify DAST installation with the ScanCentral DAST sensor service, you must enable the "Use Composite Scan Settings" option in **Application Settings > General** in Fortify DAST. Otherwise, when ScanCentral DAST connects to Fortify DAST, an error will occur. For more information, see the *OpenText™ Fortify DAST User Guide*.

Configuring the Fortify DAST REST API

On the machine where Fortify DAST is installed, configure the Fortify DAST REST API as follows:

1. From the Windows Start menu, click **All Programs** > **OpenText** > **Fortify DAST Monitor**.
   The Fortify DAST Monitor icon appears in the system tray.
2. Right-click the **Fortify DAST Monitor** icon, and select **Configure DAST API**.
   The Configure DAST API dialog box appears.
3. Configure the API Server settings as described in the following table.

Setting	Value
Host	Both Fortify DAST and the Fortify DAST API must reside on the same machine. The default setting, +, is a wild card that tells the Fortify DAST REST API to intercept all request on the port identified in the Port field. If you have another service running on the same port and want to define a specific hostname just for the API service, you can change this value.
Port	Use the provided value or change it to an available port number using the up/down arrows.
Authentication	Choose **None**, **Windows**, **Basic**, or **Client Certificate** from the Authentication drop-down list. If you choose **Basic** for authentication, you must provide user name(s) and password(s). To do this: a. Click the **Edit passwords** button and select a text editor. The `wircserver.keys` file opens in the text editor. The file includes sample user name and password entries:

Setting	Value
	`` username1:password1 username2:password2 ``` b. Replace the samples with user credentials for access to your server. If additional credentials are needed, add a user name and password, separated by a colon, for each user to be authenticated. There should be only one user name and password per line. c. Save the file. If you choose **Client Certificate** for authentication, you must first generate a client certificate based on your root SSL certificate issued by a trusted certificate authority (CA), and then install it on the client machine. **Tip:** You can use a tool, such as the MakeCert utility in the Windows Software Development Kit (SDK), to create your client certificate.
Use HTTPS	Select this check box to access the server over an HTTPS connection. To run the server over HTTPS, you must create a server certificate and bind it to the API service. To quickly create a self-signed certificate to test the API over HTTPS, run the following script in an Administrator PowerShell console: ``` $rootcertID = (New-SelfSignedCertificate -DnsName "DO NOT TRUST - WIRC Test Root CA","localhost", "$($env:computername)" -CertStoreLocation "cert:\LocalMachine\My").Thumbprint $rootcert = (Get-Item -Path "cert:\LocalMachine\My\$($rootcertID)") $trustedRootStore = (Get-Item -Path "cert:\LocalMachine\Root") $trustedRootStore.open("ReadWrite") $trustedRootStore.add($rootcert) $trustedRootStore.close() netsh http add sslcert ipport=0.0.0.0:8443 certhash=$($rootcertID) appid="{160e1003-0b46-47c2-a2bc-01ea1e49b9dc}" ``` The preceding script creates a certificate for the local host and

Setting	Value
	the computer name, puts the certificate in the Personal Store and Trusted Root, and binds the certificate to port 8443. If you use a different port, specify the port you use in the script. **Important!** Use the self-signed certificate created by the preceding script for testing only. The certificate works only on your local machine and does not provide the security of a certificate from a certificate authority. For production, use a certificate that is generated by a certificate authority.
Log Level	Choose the level of log information you want to collect.

4. Do one of the following:
   - To start the Fortify DAST REST API service and test the API configuration, click **Test API**.
     The service starts, and a browser opens and navigates to the Fortify DAST REST API Swagger UI page.
   - To start the Fortify DAST REST API service without testing the API configuration, click **Start**.

Installing and configuring the DAST sensor service

Important! To install and run the DAST sensor service, you must run the service with the `appsettings.json` file from the `ScanCentral-DAST-ScannerService.zip`. Make sure you have access to this file.

On the machine where Fortify DAST is installed, install and run the DAST sensor service as follows:

1. Retrieve the `ScanCentral-DAST-ScannerService.zip` file from the OpenText DAST (Fortify WebInspect) software download package.

   Tip: The software download package is the file that you downloaded after your purchase.

2. Extract the `ScanCentral-DAST-ScannerService.zip` contents to any directory, such as the following:

   ```
   c:\ScannerService
   ```

3. In the `appsettings.json` file that was extracted from the `ScanCentral-DAST-ScannerService.zip`, edit the following settings:

- `DASTApiRootUrl` – Use the `RootUrl` setting from the `SCDASTApiSettings` in the settings file used to configure your ScanCentral DAST environment. This setting specifies the URL and port where the ScanCentral DAST API service will run. For more information, see "ScanCentral DAST API settings" on page 76.
- `ServiceToken` – Use the `ServiceToken` string from the miscellaneous settings in the settings file used to configure your ScanCentral DAST environment. This setting specifies a shared secret for all of your sensors to use to authenticate with the ScanCentral DAST API. For more information, see "Miscellaneous ScanCentral DAST settings" on page 66.

4. Save your edits to the `appsettings.json` file.
5. Place the edited `appsettings.json` file in the same directory as the existing file, replacing the existing file.

   Important! The installation directory must match the one defined in Fortify DAST under **Edit** > **Application Settings** > **Directories**.

6. Run the Command Prompt as Administrator, and then enter the following command:

   ```
   sc create ScannerWorkerService binpath= "<PathToScannerService>
      \SCDAST.ScannerWorkerService.exe" start= auto depend= "WebInspect
      API" displayname= "SC DAST Scanner Worker Service"
   ```

   The following sample uses the `c:\ScannerService` directory in the path:

   ```
   sc create ScannerWorkerService binpath= "C:\ScannerService
      \SCDAST.ScannerWorkerService.exe" start= auto depend= "WebInspect
      API" displayname= "SC DAST Scanner Worker Service"
   ```

   The ScannerWorkerService is created and automatically starts each time the computer is restarted. The `depend= "WebInspec API"` option starts the Fortify DAST API service if it has stopped. It also stops the ScannerWorkerService if the Fortify DAST API service is stopped for any reason.
7. Open Windows Services Manager (`services.msc`). For more information, refer to your Windows documentation.
8. In Windows Services Manager, configure the scanner worker service as follows:
   a. Right-click the newly created **ScannerWorkerService**.
   b. Configure the user account and password under which the service should run.

      Note: You can use credentials for any user account that has access to log in to the Windows OS.

   c. Apply the changes.

      Note: You might need to manually start the service the first time.

   The service starts and polls the Fortify DAST API for instructions.

Chapter 3: Understanding the user interface

After you configure your ScanCentral DAST environment and enable DAST in the Administration view in Application Security, you can work with the following items directly in Application Security:

- DAST scans
- Scan settings
- Sensors and sensor pools

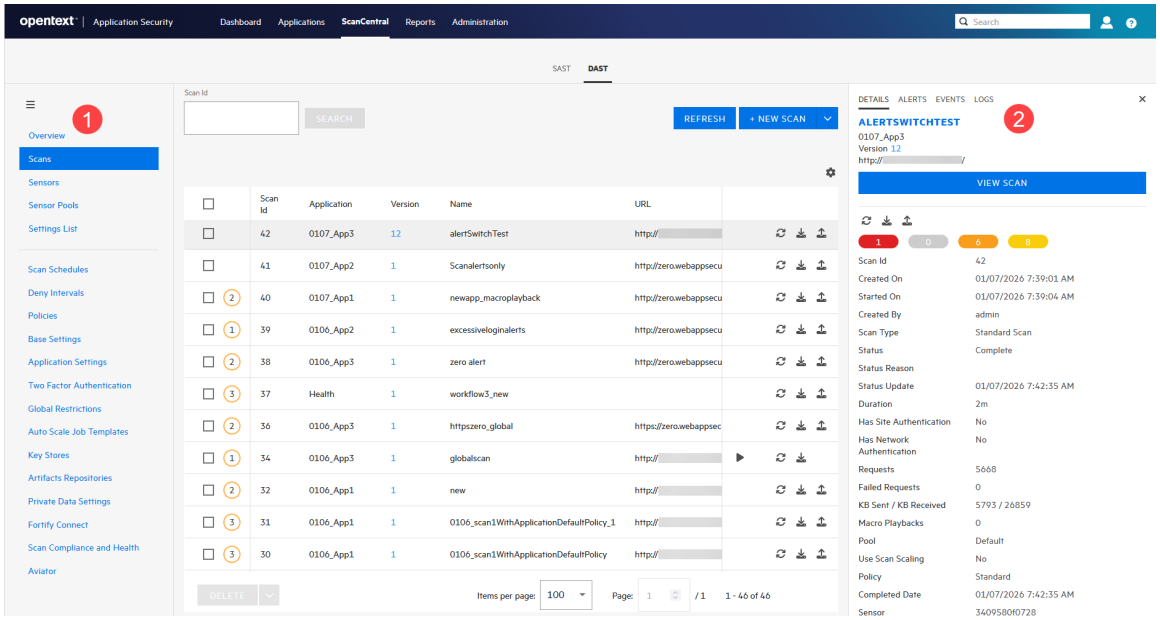
Depending on your permissions in Application Security, you may also be able to work with the following global settings:

- Application settings
- Auto Scale Job Templates
- Base settings
- Custom policies
- Deny intervals
- Fortify Connect settings
- Global restrictions and private data settings
- Key Stores and artifacts repositories
- Scan compliance and health policies
- Scan schedules
- Two-factor authentication

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools.

ScanCentral DAST user interface

The following image shows the ScanCentral DAST user interface in Application Security.



The following table describes the areas called out in the previous image.

Item	Description
1	The navigation menu enables you to navigate to the ScanCentral DAST pages (or views) that are available in Application Security.
2	The detail panel displays additional information about the item selected in the view's table.

Hiding the navigation menu

To see more of the columns of data presented in a selected view, you can hide the navigation menu.

To hide the menu:

- Click **Hide navigation** ☰.

Showing the navigation menu

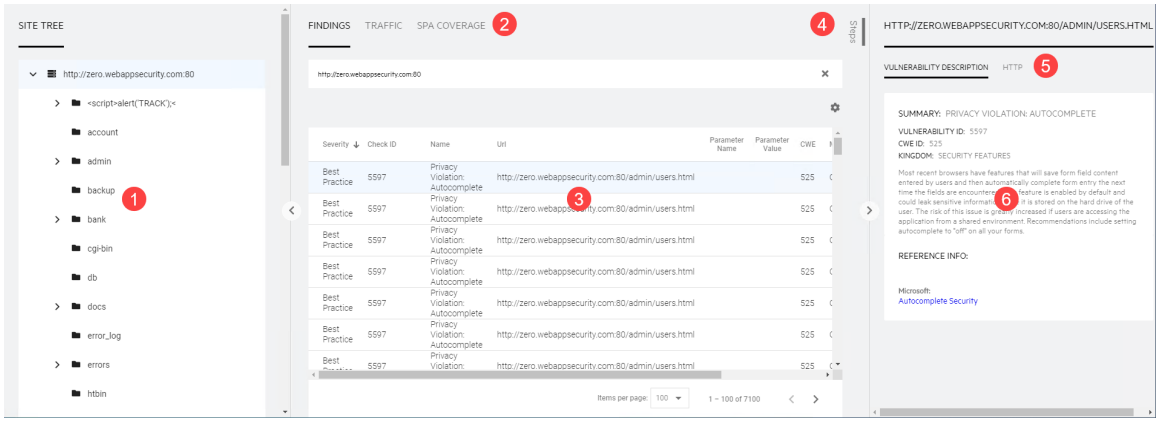
To show the menu:

- Click **Pin navigation** ☰.

  Tip: You can also hover the cursor over the icon when the navigation menu is hidden, and it will show the menu. However, if you do not click the icon and the mouse leaves the icon area, the navigation menu will automatically hide again.

Scan visualization

When you open a scan, the scan appears on a new tab in your browser. The following image shows the default view for an open scan.



The following table describes the display areas of the default view for an open scan.

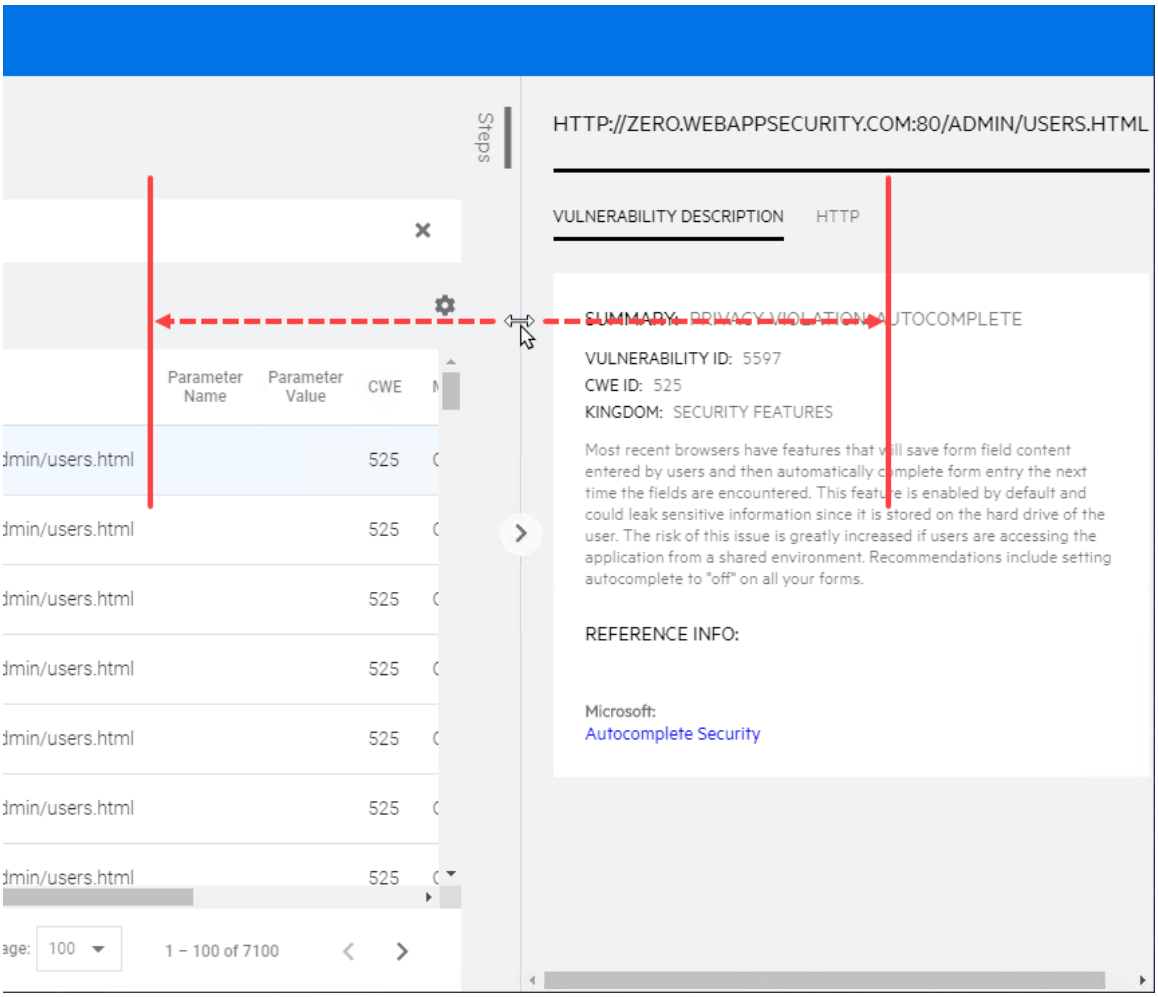
Item	Description
1	Site Tree (see "Working with the Site Tree" on page 304)
2	Findings, Traffic, and SPA Coverage tabs **Note:** The SPA Coverage tab is available only for scans that include SPA events.
3	Findings, Traffic, and SPA Coverage table views (See "Understanding the Findings table" on page 306, "Understanding the Traffic table" on page 311, and "Understanding SPA Coverage" on page 316)
4	Steps tab (See "Working with Findings" on page 308 and "Working with Traffic" on page 314)
5	Vulnerability Description, HTTP, and Parameter tabs
6	Vulnerability Description, HTTP, and Parameter detail views (See "Working with Findings" on page 308 and "Working with Traffic" on page 314)

Resizing the display areas

You can resize the Site Tree, the Findings, Traffic, and SPA Coverage view, and the Vulnerability Description, HTTP, and Parameter view.

To resize an area:

- Drag the display area border either right or left to the width you want.



Hiding and showing a display area

By default, the Site Tree and the Vulnerability Description, HTTP, and Parameter view are visible when you open a scan. You can hide the Site Tree and the Vulnerability Description, HTTP, and Parameter view.

To hide an area:

- To hide the Site Tree, click **collapse** ‹.
- To hide the Vulnerability Description, HTTP, and Parameter view, click **collapse** ›.

To show an area:

- To show the Site Tree, click **expand** ›.
- To show the Vulnerability Description, HTTP, and Parameter view, click **expand** ‹.

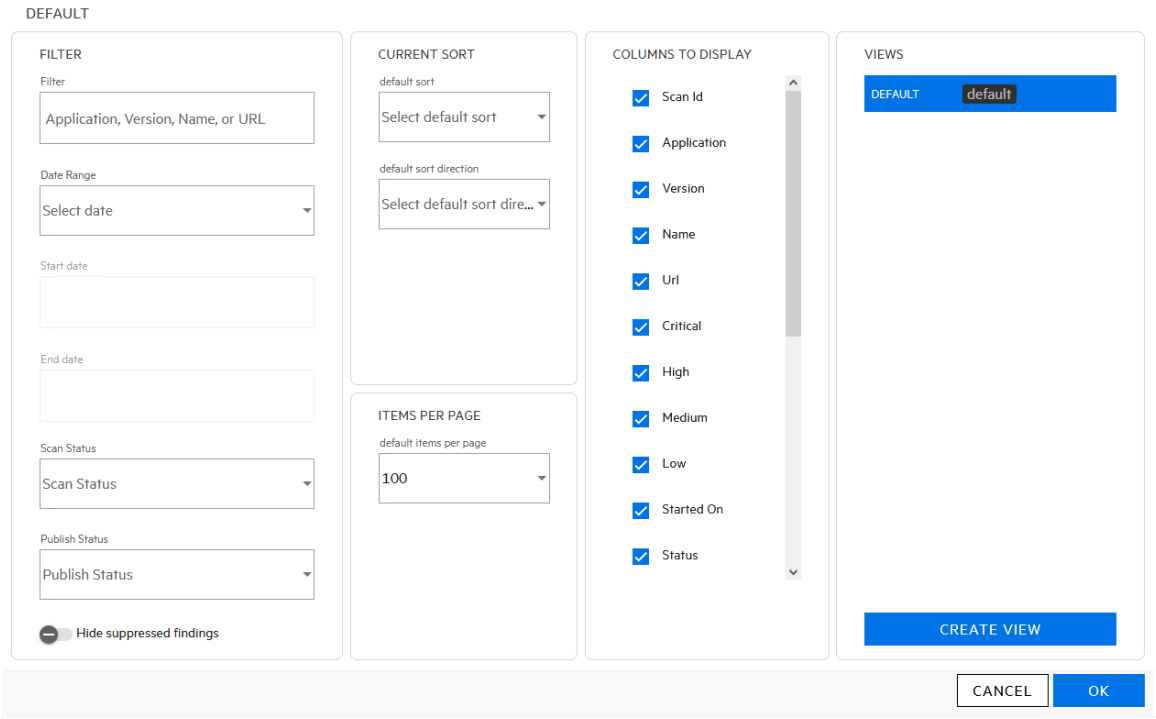
Working with tables

Much of the data available in ScanCentral DAST is presented in tables. You can customize those tables and then save the customized views. Table preferences are saved per user.

The factory default view is named DEFAULT. You can edit the default view or use the default view to create custom views.

Customizing table views

You can edit existing views or create new views in the table preferences panel.



The table preferences panel enables you to customize the following:

- Filtering (see "Understanding basic filters in tables" on page 139 and "Understanding advanced filters in tables" on page 142)
- Sorting (see "Sorting data in columns" on page 145)
- Items Per Page (see "Viewing content on multiple pages" on page 148)
- Columns to Display (see "Managing columns in tables" on the next page)

Note: Not all preference options are available for all tables. Some tables include only a subset of the preferences.

Updating or creating a view

After making changes to an existing view, you can either update the existing view or create a new view.

To update the original view with the new settings:

- In the table preferences panel, click **UPDATE *<VIEW NAME>***.

To create a new view using the new settings:

1. In the table preferences panel, click **CREATE VIEW**.
   The CREATE VIEW dialog box opens.
2. In the **View name** box, type a name for the new view.
3. (Optional) To make the new view the default view, select **Make default**.
4. Click **OK**.

Selecting a different view

To select an existing view:

1. Click **Table Preferences** ⚙.
   The table preferences panel opens.
2. In the **VIEWS** list, select a view.

   Note: If you have unsaved changes in the current view and attempt to switch views, you will be prompted that the changes will be lost.
3. Click **OK**.

Managing columns in tables

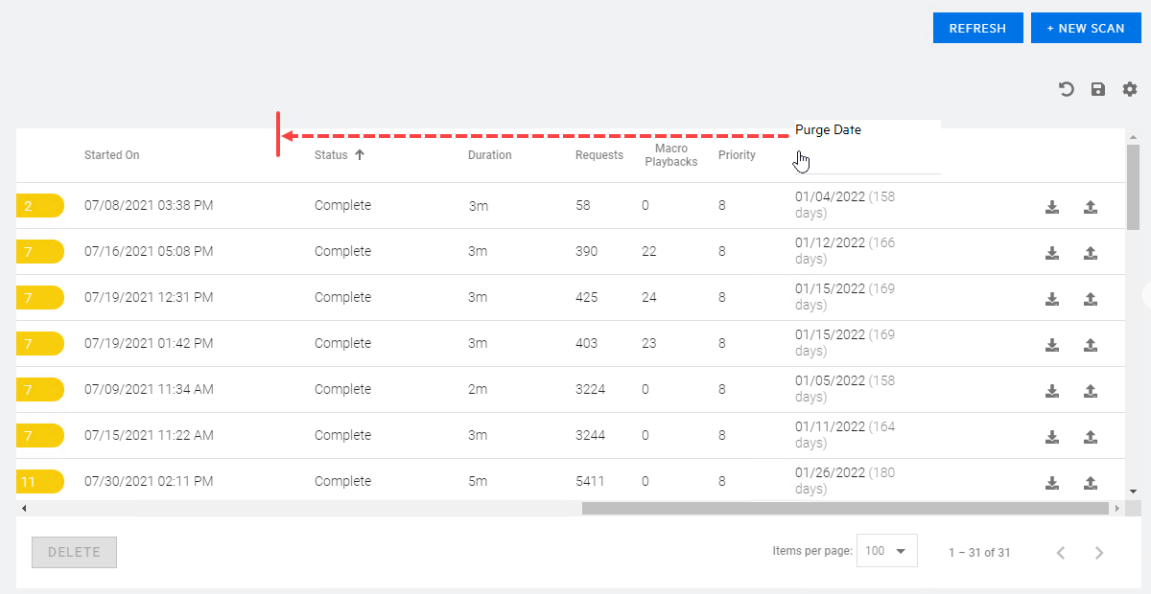
You can customize the order in which columns appear in tables, as well as change the columns to display in tables.

Rearranging the columns

You can rearrange the order in which the columns appear in the table.

To move a column:

1. Click the column heading that you want to move.
2. Drag the column right or left and drop it into its new position.



Note: You cannot move the column of check boxes or columns containing icons, such as **download** and **publish** .

Adding and removing columns

You can use the table preferences panel to select which columns of data you want visible in the table.

To add or remove displayed columns:

1. Click **Table Preferences** .
   The table preferences panel opens.
2. In the **COLUMNS TO DISPLAY** area, do the following:
   - Select the column check box to display the column.
   - Clear the column check box to hide the column.
3. Click **OK**.

When new columns are available

If you have customized a table view, such as added or removed columns, rearranged the order of columns, changed the sort order, and so forth, then when new columns of data are added to the table, you will not see them by default. Instead, the following message will appear near the top of the page:

New columns are available for the *<table_name>* table.

To view the new columns:

- Click **Table Preferences** ⚙.
  The table preferences panel opens.

To clear the message:

- Click **OK**.
  The message is cleared and will not appear again for the selected table unless new columns are added in a future update.

Understanding basic filters in tables

Basic filtering enables you to filter on certain columns of data in the Scans and Settings List tables.

You can filter data in the Scans table by application, version, name, or URL. You can also filter by scan start date, end date, date range, scan status, publish status, or a combination thereof.

You can filter data in the Settings List table by name, application, or version. You can also filter by scan start date, end date, date range, scan type, or a combination thereof.

Additionally, you can combine filtering by application, version, name, or URL with date, scan status, publish status, or scan type.

Guidelines

The following guidelines apply to basic filtering:

- You can use partial words for filtering. For example, using the filter criteria "che" includes the application named "OnlineParcheesi" and scans named "Allchecks" in the filter results.
- You cannot use wildcard characters, such as the asterisk (*), as placeholders.
- You cannot use regular expressions.

Using basic filters in tables

This topic describes how to access the basic filter user interface, specify filter criteria, and clear filters.

Accessing the basic filter feature

You can access the basic filter feature in the table preferences panel for the Scans table and the Settings List table.

To access the basic filter feature:

- In the **Scans** or **Settings List** table view, click **Table Preferences**⚙.
  The table preferences panel opens.

Specify the filter criteria in the **FILTER** area as described in "Filtering by Application, Version, Name, or URL" below and "Filtering by date, scan status, publish status, or scan type" below.

Filtering by Application, Version, Name, or URL

You can use filter criteria to filter across the application, version, name, and URL columns of data in the Scans table. For example, if you use the filter criteria "OurEstore," then all applications named "OurEstore" and all scans named "OurEstore" will be included in the filtered data. Similarly, you can filter across the name, application, and version columns in the Settings List table. This procedure illustrates filtering in the Scans table, but it also works in the Settings List table.

To filter by application, version, name, or URL:

1. In the **FILTER** area, type the filter criteria into the **Filter** box.



Note: Type only one application, one version, one name, or one URL. Do not combine filter criteria in the Filter box.

2. Click **OK**.
   The table displays the data matching the filter criteria in any of the four columns.

Tip: To combine filtering by Application, Version, Name, or URL with Date, Scan Status, or Scan Type, proceed to "Filtering by date, scan status, publish status, or scan type" below before you click **OK**.

Filtering by date, scan status, publish status, or scan type

You can filter by date range, specific date, scan status, publish status, or a combination of any filters in the Scans table. Similarly, you can filter by date range, specific date, scan type, or a combination of any filters in the Settings List table. However, when you filter on

a date in the Settings List table, you are filtering on the Modified date column. This procedure describes filtering in the Scans table and the Settings List table.

To filter by date, scan status, publish status, scan type, or a combination thereof:

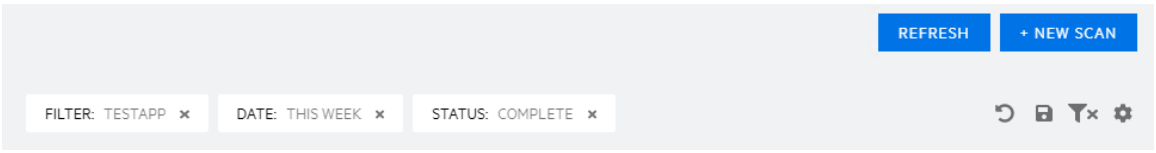
1. In the **FILTER** area, continue according to the following table.

To filter by...	Then...
A date range	Select a range from the **Date Range** list. Options are **This week**, **This month**, **Last year**, and **Custom Range**. If you select Custom Range, type dates for the range in the **Start date** and **End date** fields. **Tip:** To select dates from a calendar, click the **calendar** button.
Scan status in the Scans table	Select a scan status from the **Scan Status** list.
Publish status in the Scans table	Select a publish status from the **Publish Status** list.
Any combination of date range, publish status, and scan status in the Scans table	Select any combination of: • A range from the **Date Range** list • A scan status from the **Scan Status** list • A publish status from the **Publish Status** list
Scan type in the Settings List table	Select a scan type from the **Scan Type** list.
A date range and scan type in the Settings List table	Select a range from the **Date Range** list and a scan status from the **Scan Status** list.

2. Click **OK**.

Clearing the filter

Active filters appear as tiles at the top of the table. For basic filters, the filter value is listed in each filter tile.



To clear a filter:

- Click **Remove Filter** × on the filter tile.

To clear all filters:

- Click **Clear Filters** ▼×.

Important! Making changes outside of the table preferences panel adds **save table preferences** 🖫 to the UI. Clicking **save table preferences** 🖫 saves the changes to the current view.

Understanding advanced filters in tables

Advanced filtering enables you to construct filters using fields, operators, and conditions. The Findings and Traffic tables of a completed scan offer advanced filtering.

Important! Bear in mind that selecting a resource in the Site Tree filters data to that resource in the Findings and Traffic tables. Advanced filters are then applied to the data that is already filtered.

Understanding the operators

The following table describes the operators that are available for each type of data in advanced filtering.

Operator	Data Type			
	String	Numeric	Date/Time	Enum[1]
Equal	x	x	x	x
Not Equal	x	x	x	x
Less Than		x	x	
Less Than or Equal		x	x	
Greater Than		x	x	
Greater Than or Equal		x	x	
Between		x	x	

[1]Enumerator data consists of a key-value pair and is always presented as a list for filtering.

Operator	Data Type			
	String	Numeric	Date/Time	Enum[1]
Contains	x	x		
Starts With	x	x		
Ends With	x	x		

Understanding conditions and field filters

Field filters are treated as AND filters. For example, creating a field filter for a Severity of "High" and a field filter for a Method of "GET" filters in all records with a Severity of High AND a Method of GET.

For each field filter, you can add conditions. These conditions are treated as OR. For example, creating a field filter for a Severity of "High" and adding a condition for a Severity of "Medium" filters in all records with either a Severity of High or of Medium.

Using advanced filters in tables

This topic describes how to access the advanced filter user interface, construct filters, and clear filters.

Accessing the advance filter feature

You can access the advanced filter feature in the table preferences panel for the FINDINGS table and the TRAFFIC table.

To access the advance filter feature:

1. In the **FINDINGS** or **TRAFFIC** table of an open scan, click **Table Preferences** ⚙.
   The table preferences panel opens.
2. In the **FIELD FILTERS** area, click **ADD FILTER**.
   The ADVANCED FILTER dialog box opens.

Creating an advanced filter

You can create an advanced filter by specifying a field, an operator, and one or more values.

[1]Enumerator data consists of a key-value pair and is always presented as a list for filtering.

To create an advanced filter in the ADVANCED FILTER dialog box:

1. In the **Field** list, select a field to filter.
2. In the **Operator** box, select an operator. For more information, see the "Understanding the operators" on page 142.
3. In the box to the right of the operator, select a value from the list or type a text string.
4. Do you want to add another condition to the current filter?
   - If *yes*, click **ADD CONDITION**, and repeat steps 2 and 3.

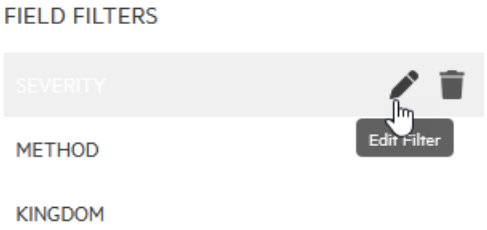
     Note: Each condition is treated as an "OR" condition. For more information, see "Understanding conditions and field filters" on the previous page.
   - If *no*, go to step 5.
5. Click **OK**.

Editing an advanced filter condition

You can edit the conditions for an advanced filter.

To edit a condition:

1. Click **Table Preferences** ⚙.
   The table preferences panel opens.
2. In the **FIELD FILTERS** area, click **Edit Filter** ✎ for the field filter you want to edit.



   The ADVANCED FILTER dialog box opens.
3. Make edits as needed.
4. Click **OK**.

Removing an advanced filter condition

You can remove a condition for an advanced filter.

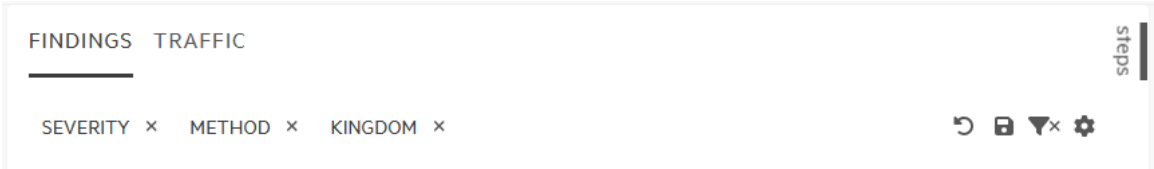
To remove a condition:

1. Click **Table Preferences** ⚙.
   The table preferences panel opens.

2. In the **FIELD FILTERS** area, click **Edit Filter** for the field filter with the condition you want to remove.
   The ADVANCED FILTER dialog box opens.
3. In the **ADVANCED FILTER** dialog box, click **Remove Condition** × next to condition to delete.
   The condition is removed.
4. Click **OK**.

Clearing filters

Active filters appear as tiles at the top of the table. For advanced filters, the field name is listed in each filter tile.



To clear a filter:

- Click **Remove Filter** × on the filter tile.

To clear all filters:

- Click **Clear Filters**.

Important! Making changes outside of the table preferences panel adds **save table preferences** to the UI. Clicking **save table preferences** saves the changes to the current view.

To delete a filter from the table preferences:

1. Click **Table Preferences**.
   The table preferences panel opens.
2. In the **FIELD FILTERS** area, click **Delete Filter** for the condition you want to delete.
   The filter is deleted.
3. Click **OK**.

Sorting data in columns

By default, columns of text in tables are listed in alphabetical order, columns of dates are in chronological order, and columns of numerical data are in numerical order. You can change the sorting directly in the table or in the table preferences panel.

Important! Making changes outside of the table preferences panel adds **save table preferences** to the UI. Clicking **save table preferences** saves the changes to the current view.

Known issue with sorting

In some columns, ascending and descending sorting sorts on a numeric value in the database, rather than on the alphabetical order of the text displayed. Therefore, sorting order may not appear as expected. For example, when sorting the sensor Status column in ascending order, one would expect to see the following alphabetical order:

- Offline
- Online

However, the sort order is based on the numeric values of 1 and 2 in the DAST database, rendering the following sort order:

- Online (represented by 1 in the database)
- Offline (represented by 2 in the database)

Sorting directly in the table

To change the sort order on any column of data:

- Click the column name.
  The arrow next to the column name indicates the new sort order.



To reverse the current sort order:

- Click the column name again.
  The arrow next to the column name indicates the reverse sort order.



To clear the sorting:

- Click the column name a third time.
  The arrow next to the column name disappears.



Sorting in the table preferences panel

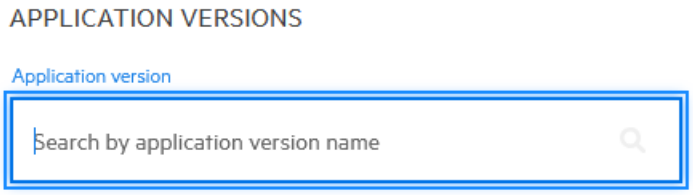
To sort table data in the table preferences panel:

1. Click **Table Preferences** ⚙.
   The table preferences panel opens.
2. In the **default sort** list of the **CURRENT SORT** area, select a column to sort.

   Note: If a column is hidden in the current view, you cannot select the column for sorting.
3. In the **default sort direction** list, do one of the following:
   - Select **asc** for ascending sort order.
   - Select **desc** for descending sort order.
4. Click **OK**.

Searching in input boxes

When search is available for an input box, a search tip appears in the box as shown below.



To search:

- Type the search criteria in the input box.
  Search results appear as you type.

Clearing data from input boxes

For any input box in which you entered search criteria or for which you selected recently used data, such as recently used options from a drop-down list box, you can quickly clear the data without manually deleting it.

To clear data from an input box:

- Click **Clear** ×.

Viewing content on multiple pages

If you have multiple pages of content, you can use the page navigation options to change the number of items displayed per page and navigate through the pages.



Changing the number of items displayed

The default number of items displayed per page is 100. You can change the number to 5, 10, 25, or 50.

To change the number of items displayed:

- Select a number from the **Items per page** drop-down list.

  Important! Making changes outside of the table preferences panel adds **save table preferences** to the UI. Clicking **save table preferences** saves the changes to the current view.

Navigating multiple pages

When the number of items you are viewing spans multiple pages, you can navigate through the pages using the page navigation icons.

To view the next page of items:

- Click **Next page** >.

To view the previous page of items:

- Click **Previous page** <.

To view a specific page:

1. In the **Page** box, do one of the following:
   - Click the up or down arrows until the desired page number appears in the box.
   - Type the desired page number in the box.
2. Press **Enter**.
   The selected page appears.

Changing the number of items displayed in the table preferences panel

To change the number of items listed per page in the table preferences panel:

1. Click **Table Preferences** ⚙.
   The table preferences panel opens.
2. In the **default items per page** list in the **ITEMS PER PAGE** area, select the number of items to view.
3. Click **OK**.

Chapter 4: Configuring a scan

Use the Settings Configuration wizard to configure an ScanCentral DAST scan of your Web application, API, and Web services to assess potential security flaws. A an ScanCentral DAST scan is an automated scan of your Web application and Web services, rather than a scan of your code. It is designed to apply attack algorithms to locate vulnerabilities, determine their severity, and provide the information you need to fix them.

This chapter describes how to configure the Basic settings that are available in the Settings Configuration wizard. For information about the Advanced settings, see "Working with Advanced scan settings" on page 219.

What is a scan?

The ScanCentral DAST sensor, which is an OpenText DAST (Fortify WebInspect) sensor, uses two basic modes for determining the security weaknesses of your Web application and Web services:

- Crawl - The process by which the sensor identifies the structure of the target website. In essence, a crawl runs until no more links on the URL can be followed.
- Audit - The actual vulnerability assessment.

A scan can combine the application crawl and audit phases into a single fluid process, or it can be a crawl-only or an audit-only scan. The scan is refined based on real-time audit findings, resulting in a comprehensive view of an entire Web application's attack surface.

Important consideration about API definition files

The Fortify DAST sensor attempts to generate the definition from the URL provided in the settings. It assumes that the API endpoint is the same URL, but without the definition file name. If your service is at the same location as your definition file, which is generally the case for GraphQL, then providing a URL will work. However, the definition may be in a different location for SOAP and gRPC.

Important information about gRPC proto files

All gRPC proto files must be self-contained. Any imports must be to internally recognized resources and not to user-generated files. The Fortify DAST sensor cannot identify file paths from imported proto files. If such files are used, the scan will fail to generate the

client and will be interrupted. If additional imports are needed, they must be combined with the primary proto file into a "master" proto file.

Known limitations of gRPC scans

Be aware of the following known limitations associated with gRPC scans:

- An Fortify DAST sensor installed on Windows 11 or a Linux version of the sensor is required for conducting scans of gRPC APIs.
- You must use a Linux version of the Fortify DAST sensor in the following scenarios:
  - Your gRPC scan requires a Socks 4/5 proxy. Using the **Any Available** sensor option may result in failure to authenticate if the scan is started on a Windows sensor.
  - Your gRPC API is running on a server with unencrypted HTTP/2 (H2C).

Preparing your system for audit

The Fortify DAST sensor is an aggressive web application analyzer that rigorously inspects your entire website for real and potential security vulnerabilities. This procedure is intrusive to varying degrees. Depending on which ScanCentral DAST policy you apply and the options you select, it can affect server and application throughput and efficiency. When using the most aggressive policies, OpenText recommends that you perform this analysis in a controlled environment while monitoring your servers.

Sensitive data

The Fortify DAST sensor captures and displays all application data sent between the application and server. It might even discover sensitive data in your application that you are not aware of. OpenText recommends that you follow one of these best practices regarding sensitive data:

- Do not use potentially sensitive data, such as real user names and passwords, while testing with the Fortify DAST sensor.
- Do not allow ScanCentral DAST scans, related artifacts, and data stores to be accessed by anyone unauthorized to access potentially sensitive data.

Network authentication credentials are not displayed in ScanCentral DAST and are encrypted when stored in settings.

Firewalls, anti-virus software, and intrusion detection systems

The Fortify DAST sensor sends attacks to servers, and then analyzes and stores the results. Web application firewalls (WAF), anti-virus software, firewalls, and intrusion

detection/prevention systems (IDS/IPS) are in place to prevent these activities. Therefore, these tools can be problematic when conducting a scan for vulnerabilities.

First, these tools can interfere with the Fortify DAST sensor's scanning of a server. An attack that the Fortify DAST sensor sends to the server can be intercepted, resulting in a failed request to the server. If the server is vulnerable to that attack, then a false negative is possible.

Second, results or attacks that are in the ScanCentral DAST product, cached on disk locally, or in the database can be identified and quarantined by these tools. When working files used by the Fortify DAST sensor or data in the database are quarantined, the sensor can produce inconsistent results. Such quarantined files and data can also cause unexpected behavior.

These types of issues are environmentally specific, though McAfee IPS is known to cause both types of problems, and any WAF will cause the first problem. OpenText has seen other issues related to these tools as well.

If such issues arise while conducting a scan, OpenText recommends that you disable WAF, anti-virus software, firewall, and IDS/IPS tools for the duration of the scan. Doing so is the only way to be sure you are getting reliable scan results.

Effects to consider

During an audit of any type, the Fortify DAST sensor submits a large number of HTTP requests, many of which have "invalid" parameters. On slower systems, the volume of requests may degrade or deny access to the system by other users. Additionally, if you are using an intrusion detection system, it will identify numerous illegal access attempts.

To conduct a thorough scan, the Fortify DAST sensor attempts to identify every page, form, file, and folder in your application. If the option to submit forms during a crawl of your site is selected, the sensor will complete and submit all forms it encounters. Although this enables the sensor to navigate seamlessly through your application, it may also produce the following consequences:

- If, when a user normally submits a form, the application creates and sends e-mails or bulletin board postings (to a product support or sales group, for example), the Fortify DAST sensor will also generate these messages as part of its probe.
- If normal form submission causes records to be added to a database, then the forms that the Fortify DAST sensor submits will create spurious records.

During the audit phase of a scan, the Fortify DAST sensor resubmits forms many times, manipulating every possible parameter to reveal problems in the applications. This greatly increases the number of messages and database records created.

Helpful hints

- For systems that write records to a back-end server (database, LDAP, and so on) based on forms submitted by clients, some ScanCentral DAST users, before auditing

their production system, backup their database, and then reinstall it after the audit is complete. If this is not feasible, you can query your servers after the audit to search for and delete records that contain one or more of the form values submitted by the Fortify DAST sensor. You can determine these values by opening the Web Form Editor.

- If your system generates e-mail messages in response to user-submitted forms, consider disabling your mail server. Alternatively, you could redirect all e-mails to a queue and then, following the audit, manually review and delete those e-mails that were generated in response to forms submitted by the Fortify DAST sensor.
- The Fortify DAST sensor can be configured to send up to 75 concurrent HTTP requests before it waits for an HTTP response to the first request. The default thread count setting is 5 for a crawl and 10 for an audit (if using separate requestors). In some environments, you may need to specify a lower number to avoid application or server failure. For more information, see "Configuring requestor settings" on page 231.
- If, for any reason, you do not want the Fortify DAST sensor to crawl and attack certain directories, you must specify those directories in the Basic Exclusions list when configuring your scan. For more information, see "Creating and managing basic exclusions" on page 199 or "Creating and managing basic exclusions in base settings" on page 411.
- By default, the Fortify DAST sensor is configured to ignore many binary files (images, documents, and so on) that are commonly found in web applications. These documents cannot be crawled or attacked, so there is no value in auditing them. Bypassing these documents greatly increases the audit speed. If proprietary documents are in use, determine the file extensions of the documents and exclude them within the sensor's default settings. For more information, see "Configuring session exclusions" on page 236. If, during a crawl, the sensor becomes extremely slow or stops, it may be because it attempted to download a binary document.
- For form submission, the Fortify DAST sensor submits data extracted from a prepackaged file. If you require specific values (such as user names and passwords), you must create a file with Fortify's Web Form Editor and identify that file to the Fortify DAST sensor. For more information, see the *OpenText™ Fortify DAST Tools Guide*.
- The Fortify DAST sensor tests for certain vulnerabilities by attempting to upload files to your server. If your server allows this, the sensor will record this susceptibility in its scan report and attempt to delete the file. Sometimes, however, the server prevents file deletion. For this reason, search for and delete files with names that start with "CreatedByHP" as a routine part of your post-scan maintenance.

Accessing scan settings configuration from Application Security

You can access the Scan Settings Configuration wizard and configure a ScanCentral DAST scan from Application Security.

Accessing from the DAST Scans list

To access the Scan Settings Configuration wizard from the ScanCentral DAST Scans list:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. On the **Scans** list, click **+ NEW SCAN**.
   The Settings Configuration wizard opens.

Accessing from the Settings List

To access the Settings Configuration wizard from the ScanCentral DAST Settings List page:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Settings List**.
3. Click **+ NEW SETTINGS**.
   The Settings Configuration wizard opens.

Restricting or allowing edits

If you have permissions to manage restricted scan settings, then you can restrict the editing of settings. If a setting is already restricted, you can allow editing.

To restrict editing:

- Click the **restrict *<setting name>*** button .

To allow editing:

- Click the **allow *<setting name>*** button .

If you do not have permissions to manage restricted scan settings, then you cannot edit any settings with the restricted button .

For more information, see "Permissions in Application Security" on page 45.

What's next?

To learn about using key store placeholders in scan settings, see "Using key stores in settings" on the next page.

To learn about using artifacts from repositories in scan settings, see "Using artifacts from a repository in settings" on page 157.

Otherwise, proceed with "Getting started" on page 159.

Using key stores in settings

You can use a key store placeholder in scan settings, base settings, or macro parameters for any field that displays **Open key store** 🔑. When the settings are downloaded or used to start a scan, the placeholder in the settings is replaced with the corresponding value from the key store entry. Using placeholder text instead of hard-coded data in settings fields allows the ScanCentral DAST administrator to change the key store entry value in one place and the value is updated in all settings where the placeholder is used. For more information about key stores, see "Understanding key stores" on page 446.

Guidelines for Key Store Usage

A scan setting field can use a single key store placeholder, a combination of text and placeholder, or multiple placeholders, as shown in the following examples:

- `${DAST_KS_KeystoreName_KeyStoreEntryName}`
- `www.${DAST_KS_KeystoreName_KeyStoreEntryName}.com`
- `${DAST_KS_KeystoreName_KeyStoreEntryName1}${DAST_KS_KeystoreName_KeyStoreEntryName2}`

Using a Key Store Placeholder

To use key store placeholder text in scan settings, base settings, or macro parameter:

1. Click **Open key store** 🔑 in the setting field.
   The KEY STORE dialog box opens.
2. In the **KEY STORE** list, select the key store whose entry you want to use.
3. In the **KEY STORE ENTRY** list, select the entry whose placeholder and value you want to use.
   The KEY STORE ENTRY SELECTION displays your placeholder text with the value masked.

   Tip: To view the stored value for the placeholder text, click **REVEAL VALUE**.
4. Click **OK**.

The placeholder text is added to the settings field.

Viewing, clearing, or replacing the key store entry value

You may view the key store entry value after placeholder text is added to the settings field. You may also remove the placeholder from the field or replace it with a different placeholder.

To view, clear, or replace the key store entry value:

1. Click **Open key store** to the right of the placeholder text in the field.
   A summary dialog box opens with the value masked.
2. Continue according to the following table.

If you want to...	Then...
View the key store entry value	Click **REVEAL VALUE**.
Remove the key store placeholder from the field	Click **CLEAR**.
Replace the key store placeholder with a different placeholder	a. Click **REPLACE**. The KEY STORE dialog box opens. b. Follow Steps 2-4 of the "Using a Key Store Placeholder" on the previous page.

Manually editing a key store placeholder in settings

You can type any text in the field before a placeholder or after a placeholder or before and after a placeholder. There are no restrictions on the text. The placeholder text will be replaced with the key store entry value.

For example, `http://www.myqa_testsite1.com`, could be expressed as `http://www.${DAST_KS_KeyStoreName_KeyStoreEntryName}.com` in the URL field.

Any entry in a field that includes the format `${DAST_KS_KeystoreName_KeyStoreEntryName}` is identified by ScanCentral DAST as a key store placeholder. If you manually edit this placeholder to include two sequential underscore characters, such as `${DAST_KS_KeystoreName__KeyStoreEntryName}`, or any other change that alters the format, it will no longer be identified by ScanCentral DAST as a key store placeholder.

If you manually type key store placeholder text, but the key store does not exist, **Key store entry may not exist** indicates that the key store placeholder text does not exist in the key store. This icon may also indicate that the key store placeholder text exists, but is not assigned to the selected application for which the settings apply.

What's next?

To learn about using artifacts from repositories in scan settings, see "Using artifacts from a repository in settings" below.

Otherwise, proceed with "Getting started" on page 159.

Using artifacts from a repository in settings

You can use an artifact from a repository for any setting in scan settings or base settings that allows you to import a file. For more information about key stores, see "Understanding artifacts repositories" on page 453.

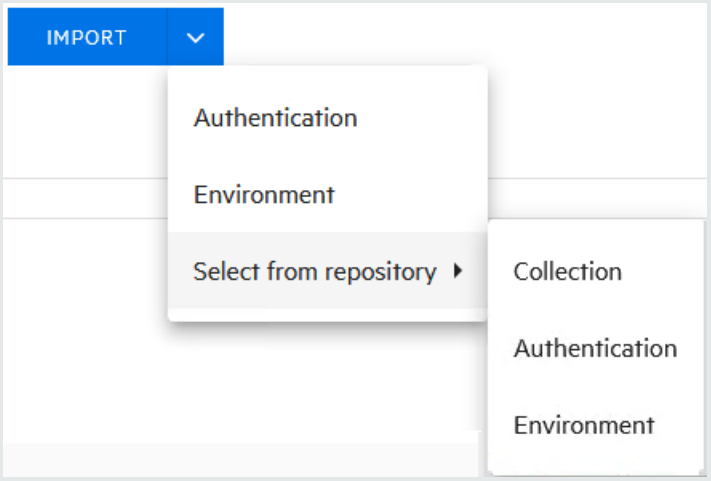
To use an artifact from a repository:

1. Click the **IMPORT** drop-down arrow, and then click **Select From Repository**.



The SELECT FILE FROM REPOSITORY dialog box opens.

Note: The **Select from repository** option may also have sub-menu items as shown in the following image.



2. From the **Repository** list, select the repository where the artifact is stored.

Tip: To see the complete URL for a repository, hover the cursor over the repository in the list.

The dialog box displays a list of artifacts that are available in the repository.

3. Navigate to the artifact that you want to use.

   Note: For tips on navigating within the repository, see "Navigating in the repository" below.

4. Select the artifact to use, and then click **OK**.

   The file name is added to the settings field and the repository logo appears to the right of the file name.



Navigating in the repository

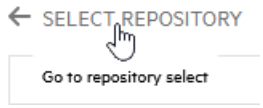
When navigating down through multiple directories in the repository, you can use the breadcrumbs at the top of the list to navigate back up to any previous directory. Click the **ellipses** ... button at the start of the breadcrumbs to return to the root directory of the repository.

Click the **two-dot ellipses** .. button at the top of the artifacts list to return to the parent directory.

In the **Go to Path** box, type the directory path to the artifact inside the repository.

Tip: Do not include the root URL for the repository in the directory path.

To return to the SELECT FILE FROM REPOSITORY dialog box, click **SELECT REPOSITORY**.



What's next?

Proceed with "Getting started" on the next page.

Getting started

To configure a ScanCentral DAST scan:

1. In the **APPLICATIONS** area, select an application from the application **Name** list.

   Tip: To search for an application, type the application name in the **Application** box.

   The APPLICATION VERSIONS area appears.
2. In the **APPLICATION VERSIONS** area, select a version from the application version **Name** list.

   Tip: To search for an application version, type the application version name in the **Application version** box.

   The GETTING STARTED area appears with a START list that provides options for creating new settings or editing existing settings. A RECENT list also appears, displaying recently-opened scan settings for the specified application and version.

3. Continue according to the following table.

If you want to...	Then...
Configure scan settings for a new scan	Select **New settings** from the **START** list.
View and edit existing scan settings from a template in Application Security	a. Select **Open from SSC** from the **START** list. A Template list appears. b. Select the existing settings from the **Template** list. **Note:** Settings that must be converted are not available for selection and their entry in the list is appended with the text " (needs conversion)." You cannot select any settings that need to be converted. For more information, see "Converting settings" on page 352.
View and edit existing scan settings from your local machine **Note:** If you import Fortify DAST settings, you will not be able to edit any settings that are not displayed in the Settings Configuration wizard. However, the settings will be used during the scan. Any settings that you change in the wizard override the values in the settings you upload.	a. Select **Open file** from the **START** list. An OPEN button appears. b. Click **OPEN** and use the standard Windows Open dialog box to locate and open the settings file.
View and edit scan settings from base settings For more information, see "Working with base settings" on page 373.	a. Select **Base Settings** from the **START** list. A Base Settings list appears. b. Select the existing settings from the **Base Settings** list.

If you want to...	Then...
	Note: Base settings that must be converted are not available for selection and their entry in the list is appended with the text " (needs conversion)." You cannot select any base settings that need to be converted. For more information, see "Converting base settings" on page 375.
View and edit recently-opened scan settings for the specified application and version	Select the settings from the **RECENT** list.

4. Click **NEXT**.

What's next?

Do one of the following:

- To configure a standard scan, proceed with "Configuring a standard scan" below.
- To configure a workflow-driven scan, proceed with "Configuring a workflow-driven scan" on page 164.
- To configure an API scan, proceed with "Configuring an API scan" on page 167.

Configuring a standard scan

A standard scan performs an automated analysis, beginning from the start URL.

To configure a standard scan:

1. On the Target page, click **STANDARD SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).
   - **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.

3. Type the complete URL or IP address in the **Url** field.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, the sensor will not scan WWW.MYCOMPANY.COM or any other variation unless you specify alternatives in the **Allowed Hosts** setting. For more information, see "Adding and managing allowed hosts" on page 194.

   An invalid URL or IP address will result in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.

   Important! If the URL resolves to an IP address that is not in the valid range for scanning, then a warning appears. If you start the scan with an IP address that is not in the valid range, then the scan will stop and a reason will be provided.

   Scans by IP address will not follow links that use fully qualified URLs (as opposed to relative paths).

   Note: The sensor supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). You must enclose IPV6 addresses in brackets.

4. (Optional) To limit the scope of the scan to a specified area, select **Restrict to folder**, and from the list, select one of the following options:
   - **Directory only** – The sensor crawls and/or audits only the URL that you specify. For example, if you select this option and specify the URL www.mycompany/one/two/, the sensor will assess only the "two" directory.
   - **Directory and subdirectories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is higher in the directory tree.
   - **Directory and parent directories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is lower in the directory tree.
5. (Optional) To submit the completed scan for triage in Application Security, select **Submit for triage**.

   Note: Submitting for triage enables you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, the selected policy is displayed above the Policy list box. You can select a different policy than the default selection or you can configure multiple policies for better coverage or for additional focus on a specific type of vulnerability. For example, if you want to run a scan using the Standard policy, but want additional focus on SQL Injection, you can select the Standard policy and the SQL Injection policy for the scan. The sensor aggregates all selected policies during the scan.

   Note: The **Standard** policy is the default policy for standard and workflow-driven scan settings in the Settings Configuration wizard. The **API** policy is the default

policy for API scan settings in the Settings Configuration wizard. You can, however, choose different policies if needed.

Continue according to the following table.

To...	Then...
Select one or more policies	a. Click in the **Policy** list box. A list of policies appears. **Tip:** Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter. b. Select a policy from the list. The policy is added to the list of selected policies. c. Repeat steps a and b for each policy you want to select.
Remove a policy from the list of selected policies	• Click **remove** × for the selected policy. The policy is cleared from the list of selected policies.

Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 519. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

7. Do one of the following:
   - To use a standard user agent, select it from the User Agent **Profile** list.

     Note: Default uses the user agent that is defined in Fortify DAST.

   - To use a custom user agent, select **Custom** from the User Agent **Profile** list, and then type the user-agent string in the **User-Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (*<system and browser information>*) *<platform>* (*<platform details>*) *<extensions>*

What's next?

Do one of the following:

- To configure proxy settings for the scan, proceed with "Configuring proxy settings" on page 173.
- To configure authentication for the scan, click **NEXT** and proceed with "Configuring authentication for standard and workflow-driven scans" on page 175.

Configuring a workflow-driven scan

A workflow-driven scan audits only those URLs included in a macro that you previously recorded. It does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, all of them will be included in the same scan.

Types of macros supported

You can use `.webmacro` files, HTTP archive (`.har`) files, or Burp Proxy captures.

Important! If you use a login macro in conjunction with a workflow macro or startup macro or both, all macros must be of the same type: all `.webmacro` files, all `.har` files, or all Burp Proxy captures. You cannot use different types of macros in the same scan. Likewise, `.webmacro` login and workflow files must have been created using the same version of Web Macro Recorder. You cannot use a login file that was recorded in the Event-based Web Macro Recorder and a workflow file that was recorded in the Session-based Web Macro Recorder.

Configuring a workflow-driven scan

To configure a workflow-driven scan:

1. On the Target page, click **WORKFLOW-DRIVEN SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).
   - **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.
3. Continue according to the following table.

To...	Then...
Record a workflow macro	Click **Open Workflow Macro Recorder 26.4**. **Tip:** If you have not already downloaded and installed the Macro Recorder tool, the Open Workflow Macro Recorder 26.4 link will not open the tool. You must first download the tool and install it on your local machine.
Add a macro to the scan settings	a. Click **MANAGE**. b. Type a name for the macro in the **Name** field. c. Click **IMPORT** and browse to locate the workflow to add to the scan settings. d. Click **OK**. e. Repeat steps a through d to add another macro to the scan settings.
Remove a macro from the list of macros	a. Select the macro in the macro list. b. Click **REMOVE**.

Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

You can use a key store placeholder for any field that displays **Open keystore**. For more information, see "Using key stores in settings" on page 155.

4. (Optional) To submit the completed scan for triage in Application Security, select **Submit for triage**.

   Note: Submitting for triage enables you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

5. Under **Audit Depth (Policy)**, the selected policy is displayed above the Policy list box. You can select a different policy than the default selection or you can configure multiple policies for better coverage or for additional focus on a specific type of vulnerability. For example, if you want to run a scan using the Standard policy, but want additional focus on SQL Injection, you can select the Standard policy and the SQL Injection policy for the scan. The sensor aggregates all selected policies during the scan.

   Note: The **Standard** policy is the default policy for standard and workflow-driven scan settings in the Settings Configuration wizard. The **API** policy is the default policy for API scan settings in the Settings Configuration wizard. You can,

however, choose different policies if needed.

Continue according to the following table.

To...	Then...
Select one or more policies	a. Click in the **Policy** list box. A list of policies appears. **Tip:** Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter. b. Select a policy from the list. The policy is added to the list of selected policies. c. Repeat steps a and b for each policy you want to select.
Remove a policy from the list of selected policies	• Click **remove** × for the selected policy. The policy is cleared from the list of selected policies.

Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 519. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

6. Do one of the following:
   - To use a standard user agent, select it from the User Agent **Profile** list.

     Note: Default uses the user agent that is defined in Fortify DAST.

   - To use a custom user agent, select **Custom** from the User Agent **Profile** list, and then type the user-agent string in the **User-Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/*<version>* (*<system and browser information>*) *<platform>* (*<platform details>*) *<extensions>*

What's next?

Do one of the following:

- To configure proxy settings for the scan, proceed with "Configuring proxy settings" on page 173.
- To configure authentication for the scan, click **NEXT** and proceed with "Configuring authentication for standard and workflow-driven scans" on page 175.

Configuring an API scan

For Open API, OData, and Postman scans, the sensor creates a macro from the REST API definition, and then performs an automated analysis. For GraphQL, gRPC, and SOAP scans, a more traditional scanning method is used.

Important! The ScanCentral DAST Utility Service container must be up and running to configure and run a Postman scan. Also, if the Postman scan requires a proxy, you must configure the proxy settings before you validate the Postman collection file(s). For more information, see "Configuring proxy settings" on page 173.

To configure an API scan:

1. On the **Target** page, click **API SCAN**.
2. In the **API Type** list, select the API type to be scanned. The options are:
   - **GraphQL**
   - **GRPC**
   - **OData**
   - **Open API** (also known as Swagger)
   - **Postman**
   - **SOAP**

   Important! If you are configuring a Postman scan while using a classic Fortify DAST installation with the ScanCentral DAST sensor service, you must install prerequisite software on the sensor machine. For more information about this and other aspects of using Postman collection files, including configuring dynamic authentication using dynamic tokens, see "Scanning with a Postman

collection" on page 502.

3. Continue according to the following table.

For this API type...	Do this...
GraphQL **GRPC** **OData** **Open API**	To use a file: a. In the **API Definition Source Type** list, select **File**. b. Click **IMPORT** and import the definition file. **Tip:** Alternatively, you can paste in the full path to a definition file that is saved on your local machine. **Important!** Open API definition files must specify the host, scheme, and service path. Otherwise, undesirable results may occur. To use a URL: a. In the **API Definition Source Type** list, select **URL**. b. Provide the URL to the API definition file, as shown in the following examples: `http://172.16.81.36/v1` `http://myapi/protos/client.proto` `http://myapi/graphql/`
Postman	a. Do one of the following: ◦ To import a workflow collection, select **IMPORT** and then import the Postman collection file. ◦ To import an authentication collection, select **Authentication** from the **IMPORT** drop-down list, and then import the Postman collection file. ◦ To import an environment file, select **Environment** from the **IMPORT** drop-down list, and then import the Postman environment file. The file is added to the list of collection files. Repeat this Step to import additional files. **Important!** You can import only one authentication collection and one environment file.

For this API type...	Do this...
	b. Click **VALIDATE** to validate the collection file(s). **Note:** At least one workflow collection must be imported before you can validate the files. The **VALIDATE** button is not available if only authentication and environment collections have been imported. **Tip:** To cancel the validation process, click **Cancel validation** ×. Upon successful validation, the POSTMAN VALIDATION dialog box opens, displaying a list of sessions contained in the collection file(s). If authentication sessions are identified, they are preselected as **Auth** sessions. All other sessions are preselected as **Audit** sessions. Additionally, the Postman Authentication Results area displays the type of authentication detected as **None**, **Static**, or **Dynamic**. **Note:** **Auth** sessions will be used for authentication for the scan. **Audit** sessions will be audited in the scan. c. (Optional) Select the **Auth** or **Audit** check box for a session to change its type as needed. d. (Optional) Make changes to the **Postman Authentication Results** as follows: ◦ For **Static** authentication, enter a token in the **Custom Header Token** box. ◦ For **Dynamic** authentication, do the following: • Select the **Regex (Custom)** option to the right of the **Response Token Name** box, and then enter a custom regular expression in the **Response Token Name** box. • Select the **Regex (Custom)** option to the right of the **Request Token Name** box, and then enter a custom regular expression in the **Request Token Name** box. • Clear the **Use Auto Detect** option to the right of the **Logout Condition** box, and then enter a new logout condition string in the **Logout Condition** box.

For this API type...	Do this...
	e. Did you make changes to the Postman Authentication Results? ◦ If yes, click **VALIDATE** to validate the new authentication settings, and then click **OK**. **Note:** Clicking **VALIDATE** regenerates all sessions for the postman collection. It does not retain any previous changes to **Auth** or **Audit** sessions even if the collection and sessions are the same. **Tip:** To cancel the validation process, click **Cancel validation** ×. ◦ If no, click **OK**. **Note:** After validation, an **EDIT** button is available. This button opens the POSTMAN VALIDATION dialog box for editing the sessions contained in the collection file(s) as described previously in this procedure.
SOAP	To use a file: a. In the **API Definition Source Type** list, select **File**. b. In the **API Definition Version Type** list, select a version to allow filtering of operations by the specific version. Options are as follows: ◦ **Legacy** – filters against the lowest supported version. ◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available. ◦ **Newest** – the default setting, filters against the latest version. c. Click **IMPORT** and import the definition file. **Tip:** Alternatively, you can paste in the full path to a definition file that is saved on your local machine. To use a URL: a. In the **API Definition Source Type** list, select **URL**.

For this API type...	Do this...
	b. In the **API Definition Version Type** list, select a version to allow filtering of operations by the specific version. Options are as follows: ◦ **Legacy** – filters against the lowest supported version. ◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available. ◦ **Newest** – the default setting, filters against the latest version. c. Provide the URL to the API definition file, as shown in the following example: `http://172.16.81.36/web-services/infoService?wsdl`

4. If you imported a definition file, the **API location is different from API definition location** option is selected. Specify the following:
   a. In the **API Scheme Type** list, select a type. Options are **HTTP**, **HTTPS**, and **HTTP/HTTPS**.
   b. In the **API Host** box, type the URL or hostname.
   c. In the **API Service Path** box, type the directory path for the API service.

Note: The GraphQL service location is always the same as the definition location. For SOAP, if the query string "?wsdl" value is removed, then the SOAP service location may or may not be the same as the definition location. The gRPC service location is always different from the definition location.

Note: If the service path is not defined for an Open API scan, then the sensor will use the basePath that is defined in the Open API definition contents. For Open API scans, select **API location is different from API definition location** unless your service is explicitly run at the same location as the docs folder for Open API. Optionally, you may choose to define a service path if it differs from the basePath.

5. (Optional) To submit the completed scan for triage in Application Security, select **Submit for triage**.

Note: Submitting for triage enables you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, the selected policy is displayed above the Policy list box. You can select a different policy than the default selection or you can configure multiple policies for better coverage or for additional focus on a specific type of vulnerability. For example, if you want to run a scan using the Standard policy, but want additional focus on SQL Injection, you can select the Standard policy and the SQL Injection policy for the scan. The sensor aggregates all selected policies during the scan.

   Note: The **Standard** policy is the default policy for standard and workflow-driven scan settings in the Settings Configuration wizard. The **API** policy is the default policy for API scan settings in the Settings Configuration wizard. You can, however, choose different policies if needed.

   Continue according to the following table.

To...	Then...
Select one or more policies	a. Click in the **Policy** list box. A list of policies appears. **Tip:** Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter. b. Select a policy from the list. The policy is added to the list of selected policies. c. Repeat steps a and b for each policy you want to select.
Remove a policy from the list of selected policies	• Click **remove** × for the selected policy. The policy is cleared from the list of selected policies.

   Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 519. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

7. Do one of the following:
   - To use a standard user agent, select it from the User Agent **Profile** list.

     Note: Default uses the user agent that is defined in Fortify DAST.

   - To use a custom user agent, select **Custom** from the User Agent **Profile** list, and then type the user-agent string in the **User-Agent** box.

Tip: User-agent strings generally use the following format:

<browser>/<version> (*<system and browser information>*) *<platform>* (*<platform details>*) *<extensions>*

What's next?

Do one of the following:

- To configure proxy settings for the scan, proceed with "Configuring proxy settings" below.
- To configure authentication for the scan, click **NEXT** and proceed with "Configuring authentication for API scans" on page 181.

Configuring proxy settings

Important! If a Fortify Connect client is configured for the application and is running in **Remote** mode, then you cannot configure proxy settings for the scan. The scan will use the Fortify Connect client proxy and any proxy that is configured on the machine running the client.

If the Fortify Connect client is running in **Local** mode, then you can configure proxy settings for the scan.

For more information about these modes, see "Working with Fortify Connect for private application scanning" on page 317.

To configure proxy settings:

1. On the Target page, click **PROXY SETTINGS**.
   The PROXY CONFIGURATION dialog box opens.
2. Select the **Use Proxy Server** option.
   The settings become available for you to configure.
3. Configure the settings according to the following table.

To...	Then...
Use the Web Proxy Autodiscovery Protocol (WPAD) to locate and use a proxy autoconfig file to configure the web proxy settings	Select **Auto detect proxy settings**.
Import your proxy server information	Select **Use Firefox proxy settings**.

To...	Then...
from Firefox	**Note:** Using browser proxy settings does not guarantee that you can access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used.
Load proxy settings from a Proxy Automatic Configuration (PAC) file	a. Select **Configure proxy settings using a PAC file**. b. In the **URL** box, type the URL location for the PAC file.
Access the Internet through a proxy server	a. Select **Explicitly configure proxy** settings. b. In the **Server** box, enter the URL or IP address of your proxy server. c. In the **Port** box, enter the port number (for example, 8080). d. From the **Type** list, select the protocol type for handling TCP traffic through the proxy server. The options are: **Standard**, **SOCKS4**, or **SOCKS5**. **Important!** Socks4 proxy servers do not support authentication. When using a Socks proxy server that requires authentication, you must use a Socks5 proxy. e. If authentication is required, select a type from the **Authentication** list. The options are: **None**, **Basic**, **NTLM**, **Digest**, **Automatic**, **Kerberos**, or **Negotiate**. **Note:** For sensors running on

To...	Then...
	the Linux OS, ADFS_CBT will be used if Negotiate is selected. f. If your proxy server requires authentication, enter the qualifying user name in the **User Name** field and the qualifying password in the **Password** field. g. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass** field. Use semicolons to separate entries.

4. Click **OK**.
   The proxy settings are saved and the PROXY CONFIGURATION dialog box closes.

What's next?

To configure authentication for the scan, click **NEXT** and proceed with "Configuring authentication for standard and workflow-driven scans" below or "Configuring authentication for API scans" on page 181.

Configuring authentication for standard and workflow-driven scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Configuring site authentication

You can use a recorded login macro containing one or more usernames and passwords that allow you to log in to the target site. The macro must also contain a "logout condition," which indicates when an inadvertent logout has occurred so that the sensor can rerun the macro to log in again.

To configure site authentication:

1. Select **Site Authentication**.
2. Do one of the following:
   - To import an existing login macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays **Open keystore** 🔑. For more information, see "Using key stores in settings" on page 155.
   - To record a login macro, click **Open Macro Recorder 26.4**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 26.4 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder tool" on the next page.
   - To have Aviator automatically create a login macro, proceed with "Using Aviator for login macro creation" below.

     Tip: The Aviator service must be configured and enabled for the Autogen UI to appear. For more information, see "Working with Aviator auto-generated macros" on page 475.

Using Aviator for login macro creation

To use Aviator for automatic login macro creation, do the following:

1. Select the **Aviator Autogen Macro** tab.
2. In the **Username** box, type a user name.
3. In the **Password** box, type the corresponding password.
4. Optionally, to use TOTP, slide the **Use TOTP** option to enabled and continue according to the following table:

To...	Then...
Use a QR code image	a. Select the **Upload Image** tab. b. Upload or drag and drop the QR code image into the upload image area. A message indicates whether the secret is successfully extracted. After which, you can either replace or remove the uploaded image.

To...	Then...
Manually enter the secret	a. Select the **Enter Text** tab. b. In the **TOTP Secret** box, enter the secret.

Important! You may continue configuring the scan settings and save the configuration. However, when an Aviator auto-gen macro is pending, scan settings in the Getting Started section of the Settings configuration wizard become temporarily read-only. The settings remain visible but are disabled with a "pending macro validation" message. After macro generation completes, the settings become fully editable and selectable.

Validating the login macro

You can have Fortify DAST test the login macro at the start of the scan to ensure that the log in is successful. If the macro is invalid and fails to log in to the application, the scan stops and an error message is written in the scan log file. For more information and troubleshooting tips, see "Testing login macros" on page 498.

To validate the login macro:

- Select **Enable macro validation**.

Downloading the Macro Recorder tool

The Scan Settings Configuration wizard enables you to download the Event-based Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is available for both Microsoft Windows® and Mac® operating systems. You cannot use the Event-based Web Macro Recorder on Linux® operating systems.

To download the Macro Recorder tool:

1. Do one of the following:
   - On the **Workflow-Driven Scan** tab on the **Target** page of the Scan Settings Configuration wizard, click **Download Macro Recorder 26.4**.
   - Under **Site Authentication** on the **Authentication** page of the Scan Settings Configuration wizard, click **Download Macro Recorder 26.4**.

   The DOWNLOAD MACRO RECORDER dialog box opens.
2. Do one of the following:
   - To download the Microsoft Windows® version, select **Macro Recorder Windows (x64) Setup**.

The `MacroRecorderWindowsX64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.

- To download the Mac® version, select **Macro Recorder MacOS (arm64) Setup**.

  The `MacroRecorderMacOSArm64Setup.dmg` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the DMG file.

  Tip: For instructions on installing and launching the Mac® version, refer to the *OpenText™ Fortify DAST Tools Guide*.

Using a client certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

To use a client certificate:

1. Select **Use Client Certificate**.
2. Click **IMPORT**.

   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.

   The certificate file is added to the Client certificate box.
4. If the certificate requires a password, do the following:
   a. Select **Requires password**.
   b. Enter the password in the **Client certificate password** box.
5. Optionally, click **VALIDATE** to perform basic validation of the certificate.

   Note: Basic validation only confirms that the file is a certificate, verifies the password if applicable, and checks for a private key. If the certificate is not valid, the scan will fail upon startup.

Configuring network authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Network Authentication**.
2. Select an **Authentication Type**. Options are as follows:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Digest**
   - **Kerberos**
   - **NT LAN Manager (NTLM)**
   - **OAuth 2.0 Bearer**
3. For all authentication methods except OAuth 2.0 Bearer, do the following:
   a. Type the authentication user name in the **Username** box.
   b. Type the authentication password in the **Password** box.
4. For the OAuth 2.0 Bearer method, continue with "Configuring OAuth 2.0 bearer credentials" below.

Caution! The sensor crawls all servers granted access by this password (if the sites/servers are included in the Allowed Hosts setting). To avoid potential damage to your administrative systems, do not use credentials that have administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional.

Configuring OAuth 2.0 bearer credentials

Open authorization (OAuth) 2.0 is an open-standard authorization protocol that shares authorization tokens between services or applications to prove the identity of a user. You can configure the following types of OAuth 2.0 authentication flows:

- **Client Credentials Grant** – The client uses its client credentials, such as client ID and client secret, when requesting access to the protected resources.
- **Password Credentials Grant** – The client obtains the resource owner's credentials, such as user name and password, usually by way of an interactive form.

If you configure OAuth 2.0 authentication, then the sensor will use the retrieved token for the entire scan. The token will be refreshed if it expires.

After selecting **OAuth 2.0 Bearer** as network authentication type in scan settings, to configure OAuth 2.0 bearer credentials:

1. In the **Access Token URL** box, type the URL that is used to generate tokens, such as `https://<yourDomain>/oauth2/token`.

2. In the **OAuth Flow Type** list, select a flow. Options are **Client Credentials Grant** and **Password Credentials Grant**.
3. Optionally, if your service supports different scopes (or permissions) for the OAuth flow, specify the scope to use in the **Scope** box.
4. Provide information that will be included in the authorization request header according to the following table.

To configure...	Then...
A Client Credentials Grant flow	In the **Client ID** box, enter the application (client) ID. In the **Client Secret** box, enter the client secret that you generated for your application in the OAuth provider's registration portal.
A Password Credentials Grant flow	In the **User Name** box, enter the user name. In the **Password** box, enter the password.

5. Optionally, to specify additional parameters:
   a. Select **Use Additional Parameters**.
   b. Click **add oauth parameter** +.
   c. In the **parameter name** box, enter a parameter name.
   d. In the **parameter value** box, enter a parameter value.
   e. To add another parameter name-value set, return to Step 5b. Otherwise, go to Step 6.

   Important! The `grant_type` and `scope` parameter names are reserved and cannot be used in the additional parameters list.

   If the OAuth Flow Type is Client Credentials Grant, then `client_credentials`, `client_id`, and `client_secret` cannot be used in the additional parameters list.

   If the OAuth Flow Type is Password Credentials Grant, then `username` and `password` cannot be used in the additional parameters list.
6. By default, the sensor uses Status Code 403 for the logout signature. Optionally, if you use a custom status code, in the **Logout Signature** box, enter the status code or a regular expression to indicate the logout signature. Use the following syntax:

   `[STATUSCODE]<Number>`
7. Optionally, click **Test** to validate access to the server and receipt of a bearer token.

   To see the response of the validation request, click **SEE RESPONSE**.

What's next?

To configure details for the scan, click **NEXT** and proceed with "Configuring scan details" on page 188.

Configuring authentication for API scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Options for configuring authentication include the following:

- "Using a client certificate" below
- "Configuring network authentication" below
- "Using custom headers" on page 186
- "Configuring SOAP settings" on page 186

Using a client certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

Note: Client certificates do not apply to OData or Open API definition types.

To use a client certificate:

1. Select **Use API Client Certificate**.
2. Click **IMPORT**.
   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.
   The certificate file is added to the Client certificate box.
4. Enter the password in the **Client certificate password** box.

Configuring network authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Use API Network Authentication**.
2. Select an **Authentication Type**. The API Type determines the available authentication types. The complete list of authentication types is:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Bearer**
   - **Custom**
   - **Digest**
   - **Kerberos**
   - **NT LAN Manager (NTLM)**
   - **OAuth 2.0 Bearer**
3. Continue according to the following table.

For this authentication type...	Do this...
ADFS CBT **Automatic** **Basic** **Digest** **Kerberos** **NTLM**	a. Type the authentication user name in the **Username** box. b. Type the authentication password in the **Password** box.
Bearer	Optionally, type the JSON token, generally from a response to a login form, in the **Token Value** box. When using Bearer, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a token value" on the next page. **Note:** Not available for SOAP web service scans.
Custom	a. Type the token name in the **Scheme** box. b. Optionally, type the token value in the **Parameter** box.

For this authentication type...	Do this...
	When using Custom, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a token value" below. **Note:** Not available for SOAP web service scans.
OAuth 2.0 Bearer	Continue with "Configuring OAuth 2.0 bearer credentials" on the next page.

Fetching a token value

You can use a custom regular expression to fetch the token value from a login or workflow macro. If a match to the regular expression occurs in the response, then the value is fetched and used as a bearer token. If the regular expression contains parentheses, then the value inside the parentheses will be extracted and used as a bearer token. Only the first value inside parentheses will be used.

Note: Fetching a token value does not apply to OData or Open API definition types.

To fetch a token value:

1. Select **Use Fetch Token**.
2. Do one of the following:
   - To import an existing macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays **Open keystore** 🔑. For more information, see "Using key stores in settings" on page 155.

   - To record a macro, click **Open Macro Recorder 26.4**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 26.4 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder tool" on page 185.
3. Type a regular expression for pattern matching in the **Search Pattern** box.

4. Do one of the following:
   - To have each scan thread run its own fetch macro playback and apply the bearer token value to the thread, select the **Isolate state** check box.
   - To have only one fetch macro playback run for all scan threads and the single shared bearer token value apply to all threads, clear the **Isolate state** check box.

Configuring OAuth 2.0 bearer credentials

Open authorization (OAuth) 2.0 is an open-standard authorization protocol that shares authorization tokens between services or applications to prove the identity of a user. You can configure the following types of OAuth 2.0 authentication flows:

- **Client Credentials Grant** – The client uses its client credentials, such as client ID and client secret, when requesting access to the protected resources.
- **Password Credentials Grant** – The client obtains the resource owner's credentials, such as user name and password, usually by way of an interactive form.

If you configure OAuth 2.0 authentication, then the sensor will use the retrieved token for the entire scan. The token will be refreshed if it expires.

After selecting **OAuth 2.0 Bearer** as network authentication type in scan settings, to configure OAuth 2.0 bearer credentials:

1. In the **Access Token URL** box, type the URL that is used to generate tokens, such as `https://<yourDomain>/oauth2/token`.
2. In the **OAuth Flow Type** list, select a flow. Options are **Client Credentials Grant** and **Password Credentials Grant**.
3. Optionally, if your service supports different scopes (or permissions) for the OAuth flow, specify the scope to use in the **Scope** box.
4. Provide information that will be included in the authorization request header according to the following table.

To configure...	Then...
A Client Credentials Grant flow	In the **Client ID** box, enter the application (client) ID. In the **Client Secret** box, enter the client secret that you generated for your application in the OAuth provider's registration portal.
A Password Credentials Grant flow	In the **Username** box, enter the user name. In the **Password** box, enter the password.

5. Optionally, to specify additional parameters:
   a. Select **Use Additional Parameters**.
   b. Click **add oauth parameter** +.
   c. In the **parameter name** box, enter a parameter name.
   d. In the **parameter value** box, enter a parameter value.
   e. To add another parameter name-value set, return to step b. Otherwise, go to Step 6.

   Important! The `grant_type` and `scope` parameter names are reserved and cannot be used in the additional parameters list.

   If the OAuth Flow Type is Client Credentials Grant, then `client_credentials`, `client_id`, and `client_secret` cannot be used in the additional parameters list.

   If the OAuth Flow Type is Password Credentials Grant, then `username` and `password` cannot be used in the additional parameters list.
6. By default, the sensor uses Status Code 403 for the logout signature. Optionally, if you use a custom status code, in the **Logout Signature** box, enter the status code or a regular expression to indicate the logout signature. Use the following syntax:
   `[STATUSCODE]<Number>`
7. Optionally, click **Test** to validate access to the server and receipt of a bearer token.
   To see the response of the validation request, click **SEE RESPONSE**.

Downloading the Macro Recorder tool

You can download the Event-based Web Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is a Microsoft Windows®-based application. You cannot use the Event-based Web Macro Recorder on Linux operating systems.

To download the Macro Recorder tool:

- Under **Site Authentication**, do one of the following:
  - To download the Microsoft Windows® version, select **Macro Recorder Windows (x64) Setup**.
    The `MacroRecorderWindowsX64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

    Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.
  - To download the Mac® version, select **Macro Recorder MacOS (arm64) Setup**.

The `MacroRecorderMacOSArm64Setup.dmg` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the DMG file.

Tip: For instructions on installing and launching the Mac® version, refer to the *OpenText™ Fortify DAST Tools Guide*.

Using custom headers

You can configure multiple custom headers.

Important! OpenText recommends that you do not configure more than one custom header using the same HTTP header name.

To add a custom header:

1. Select **Use Custom Headers**.
2. Click **add custom header** +.
3. In the **header name** box, type the custom HTTP header name. For example, `X-MyCustomAuth`.

   Important! The header must be unique and cannot be `Authorization`.
4. In the **header scheme** box, type the header value prefix name. For example, `CustomToken`.
5. In the **header value** box, type the custom header value.
6. Click **confirm** ✔.

   The custom header is added to the list.

To edit a custom header:

- Click **edit** for the custom header you want to edit.

To delete a custom header:

- Click **delete** × for the custom header you want to delete.

Configuring SOAP settings

You can configure message-based authentication for SOAP scans.

To configure SOAP authentication settings:

1. Select **Use SOAP Configuration**.
2. Select that authentication method to use from the **SOAP Method** list. Options are **Username Token** and **Certificate Pair**.
3. Continue according to the following table.

For this authentication method...	Do this...
Username Token	a. In the **Username** box, type the user name whose credentials are used to access the SOAP service. b. In the **Password** box, type the password for the user name. c. In the **Username Token Type** list, select the type of token. Options are **Text** and **Hash**. d. In the **Timestamp** list, select an option for when the Username Token was created and when it expires. Options are **Created**, **Full**, and **None**. e. If nonce is enabled for the token, select **Includes nonce**. **Important!** Nonce is required for hash tokens because it helps the server to recalculate the hash and compare it to the data the client sent.
Certificate Pair	a. Click **IMPORT** to the right of the **Client Certificate** box. A standard Windows file selection dialog box opens. b. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Client Certificate box. c. In the **Client Certificate Password** box, type the password. d. Click **IMPORT** to the right of the **Server Certificate** box. A standard Windows file selection dialog box opens. e. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Server Certificate box. f. If the server certificate requires a password, select **Requires password** and type the password in the **Server Certificate Password** box.

4. Optionally, to identify the Web Services Addressing (WS-Addressing) schema version used by the SOAP service, select **Use WS Addressing** and continue as follows:
   a. In the **Schema Version** list, select the version. Options are **NONE**, **WSA0408**, and **WSA0508**.
   b. In the **WSA: To** box, enter the URL override for the Web service host.

   Note: SOAP services may be exposed by way of a load balancer or reverse proxy. This configuration may prevent the sensor from getting the correct

information for the internal Web service host name. The "WSA: To" URL override provides the correct address into WS Addressing.

The URL override uses the following format:

`https://<host_name><service_path>/<port_name>`

What's next?

To configure details for the scan, click **NEXT** and proceed with "Configuring scan details" below.

Configuring scan details

You can configure the following settings on the Details page:

- API Content and filters (API scans only. For more information, see "Configuring API content and filters" below.)
- Allowed hosts (For more information, see "Adding and managing allowed hosts" on page 194.)
- Scan priority (For more information, see "Configuring scan priority" on page 195.)
- Data retention (For more information, see "Configuring data retention" on page 198.)
- Single-page application (SPA) support (Standard and Workflow-driven scans only. For more information, see "Scanning single-page applications" on page 198.)
- Traffic Monitor (For more information, see "Enabling traffic monitor" on page 199.)
- Exclusions (For more information, see "Creating and managing basic exclusions" on page 199.)
- Redundant page detection (Standard and Workflow-driven scans only. For more information, see "Configuring redundant page detection" on page 204.)

What's next?

After you configure the scan details, click **NEXT** and proceed with "Reviewing scan settings" on page 205.

Configuring API content and filters

When configuring API scans, you can use the Content and Filters page to configure the preferred content type, as well as operations and parameter names and types to include or exclude during the scan.

Specifying the preferred content type

The preferred content type setting specifies the preferred content type of the request payload. If the preferred content type is in the list of supported content types for an operation, then the generated request payload will be of that type. Otherwise, the first content type listed in an operation will be used. By default, the preferred content type is application/json.

To change the preferred type:

- Type the preferred content type in the **Preferred Content Type** box.

Defining specific operations to include

The Include feature defines an allow list of operation IDs that should be included in the output.

To define a specific operation to include:

1. Select **Specific Operations**.
2. Select **Include**.
3. Click **add operation** +.
4. In the **Operation to add** box, type the operation ID.
5. Click **confirm** ✓.
   The operation ID is added to the allow list.

Defining specific operations to exclude

The Exclude feature defines a deny list of operation IDs that should be excluded from the output.

To define a specific operation to exclude:

1. Select **Specific Operations**.
2. Select **Exclude**.
3. Click **add operation** +.
4. In the **Operation to add** box, type the operation ID.
5. Click **confirm** ✓.
   The operation ID is added to the deny list.

Editing specific operations

To edit a specific operation in the allow or deny list:

1. Do one of the following:
   - To edit an operation in the allow list, select **Include**.
   - To edit an operation in the deny list, select **Exclude**.
2. Click the **edit** for the operation ID you want to edit.

Removing specific operations

To remove a specific operation from the allow or deny list:

1. Do one of the following:
   - To remove an operation from the allow list, select **Include**.
   - To remove an operation from the deny list, select **Exclude**.
2. Select the check box for each operation ID you want to remove.
3. Click **REMOVE**.

Defining parameter rules

Parameter rules define a default value to use for a parameter when the parameter name and type are encountered. You can also specify operations to determine whether a specific parameter rule should or should not apply to those operations.

Important! If you configure a parameter rule and then change the API definition type for which the parameter rule type becomes invalid, the invalid parameter rule type will be changed to **Any**. The invalid parameter rule will be highlighted in the Parameter Rules list, and a warning message will be displayed below the list.

To add a parameter rule:

1. Select **Parameter Rules**.
2. Click **Add**.
   The PARAMETER RULE dialog box appears.
3. In the **Parameter Rule Name** box, type a name for the rule.
4. In the **Parameter Rule Type** list, select a type. Available options depend on the API type and may include the following:
   - **Any**
   - **Boolean**
   - **Date**

- **File**
- **Guid**
- **Number**
- **String**

For more information on the Parameter Rule Types and their equivalents based on API type, see "Understanding parameter type matches" on page 193.

5. Continue according to the following table:

For this Rule Type...	Do this...
Any	In the **Value** box, type any value.
Boolean	In the **Boolean Value** list, select **true** or **false**.
Date	To enter any string value as the date: • Type the string in the **Date** box. **Note:** You may enter a duration, time span, formatted date, or formatted time in the **Date** box. To select a date/time format and use a calendar and clock to generate a formatted string: a. Click **GENERATE DATE**. The GENERATE DATE STRING dialog box opens. b. From the **Date Type** list, select a format. Options are **Date and time**, **Date**, and **Time**. c. In the **Date** box, enter a date using the preferred format defined in your Application Security. **Tip:** To select a date from the calendar, click the **Calendar** button. d. In the **Time** box, enter a time using the preferred format defined in your Application Security **Tip:** To select a time from a list, click the **Clock** button. e. Click **OK**.
File	a. Click **IMPORT** and browse to locate the file to add to the scan settings.

For this Rule Type...	Do this...
	b. Click **Open**.
Guid	In the **Value** box, enter a GUID.
Number	In the **Number Value** box, enter a numerical value.
String	In the **Value** box, type any value.

6. For Open API scans, in the **Parameter Rule Location** list, select a location where the parameter is found in the request. Options are:
   - **Any**
   - **Body**
   - **Header**
   - **Path**
   - **Query**
7. Optionally, select **Inject Parameter** to include the defined parameter in the request.

   Important! The **Inject Parameter** option does not work with schema-based APIs, such as SOAP, gRPC, and Postman. Those API types do not accept forced parameters. For GraphQL, **Inject Parameter** only works with the query operation if the property is in the query schema.
8. Optionally, to specify operations to which this parameter rule should or should not apply, select **Specific Operations** and perform steps 2-5 of "Defining specific operations to include" on page 189 or "Defining specific operations to exclude" on page 189.
9. Click **OK**.

   The rule is added to the Parameter Rules list.

Editing a parameter rule

To edit a rule in the Parameter Rules list:

- Select the check box for the rule to edit, and then click **EDIT**.

  The PARAMETER RULE dialog box appears. For more information about using this dialog box, see "Defining parameter rules" on page 190.

Removing a parameter rule

To remove a rule from the Parameter Rules list:

- Select the check box for the rule to remove, and then click **REMOVE**.

Understanding parameter type matches

The following table describes the parameter rule type equivalents by API type.

ScanCentral DAST Parameter Rule Type	Equivalent				
	Open API (Swagger)	OData	GraphQL	gRPC	SOAP
Any	All	All	All	All	All
Boolean	boolean	Edm.Boolean	boolean	bool	boolean
Date	date (OpenAPI 2.0) string (OpenAPI 3.0)[1]	Edm.Date Edm.DateTime Edm.DateTimeOffset Edm.Duration Edm.Time Edm.TimeOfDay	N/A	N/A	date
File	file (OpenAPI 2.0)[2]	Edm.Binary	N/A	bytes	N/A
GUID	N/A	Edm.Guid	N/A	N/A	N/A
Number	number integer	Edm.Byte Edm.Decimal Edm.Double Edm.Int16 Edm.Int32 Edm.Int64 Edm.SByte Edm.Single	int float	double enum fixed32 fixed64 float int32 int64 sfixed32 sfixed64 sint32 sint64 uint32 uint64	base64Binary byte decimal double float hexBinary hexint int integer long signedInt short unsignedByte unsignedInt unsignedLong unsignedShort
String	string	Edm.GeographyCollection Edm.GeographyLineString Edm.GeographyMultiLineString Edm.GeographyMultiPoint Edm.GeographyMultiPolygon Edm.GeographyPoint	id string	string	string

[1] OpenAPI 3.0 implementation is qualified by date string format.

[2] OpenAPI 3.0 implementation is qualified by binary or byte string formats.

ScanCentral DAST Parameter Rule Type	Equivalent				
	Open API (Swagger)	OData	GraphQL	gRPC	SOAP
		Edm.GeographyPolygon Edm.GeometryCollection Edm.GeometryLineString Edm.GeometryMultiLineString Edm.GeometryMultiPoint Edm.GeometryMultiPolygon Edm.GeometryPoint Edm.GeometryPolygon Edm.String			

Adding and managing allowed hosts

Use the **Allowed Hosts** setting to add and manage domains to crawl and audit. If your Web application uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the scan.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify www.myco.com as the scan target and you enter "myco" as an allowed host. As the sensor scans the target site, if it encounters a link to any URL containing "myco," it will pursue that link and scan that site's server, repeating the process until all linked sites are scanned. For this hypothetical example, the sensor would scan the following domains:

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

Adding allowed hosts

To add allowed hosts:

1. Click **add allowed host** +.
2. Type a URL in the **Host name** box.

Important! When you specify the URL, do not include the protocol designator (such as http:// or https://).

3. (Optional) To use a regular expression to represent a URL, select **Use Regular Expression**.
4. Do one of the following:
   - To save the allowed host to the list, click **confirm** ✔.
     The URL is added to the allowed hosts list. To add another allowed host, return to Step 1.
   - To clear the field and start over, click **discard** ✕ and return to Step 1.

Editing or removing allowed hosts

To edit an allowed host:

1. In the **Allowed Hosts** list, click **edit** for the host you want to edit.
2. Edit the host as described in "Adding allowed hosts" on the previous page.

To remove an allowed host:

- In the **Allowed Hosts** list, click **delete** ✕ for the host you want to delete.

Configuring scan priority

Scans are run using a priority ranking from 0 to 10, where 0 is the lowest priority and 10 is the highest. Before starting a scan, the Global Service determines if there is a higher-priority scan that needs to be started. If there is, the lower-priority scan will remain in the queue. Additionally, a lower-priority scan that is running will be paused for a higher-priority scan if no other sensor is available.

If Advanced Scan Prioritization is enabled, the Global Service may move scans to other sensors, depending on scan priority and other settings. For more information about Advanced Scan Prioritization, see "Understanding advanced scan prioritization" on the next page.

Note: Applications are configured with a default priority level in the application settings. For more information, see "Understanding the Application Settings view" on page 419.

Changing the priority

To select a priority other than the default setting for the scan:

- Select a priority from 0 to 10 in the **Priority** list.

Note: If you set a priority that differs from the Application Settings, the lower of the two settings will be used.

Tip: You cannot disable scan priority. However, you can set all applications and scans to the same priority to accomplish something similar.

Understanding advanced scan prioritization

Advanced scan prioritization allows the Global Service to move a scan to a different sensor, depending on the scan priority and other settings as described in the following paragraphs.

Priority and sensor pools

For prioritization, scans are grouped by the sensor pool to which the scan belongs. Grouping scans by pool ensures that a higher-priority scan in sensor pool 1 will not pause a lower priority scan in sensor pool 2.

Priority and scan status

Scans with the following statuses are processed first from the highest to lowest scan priority and then from the oldest to newest:

- Queued
- Resume Scan Queued
- Resume Scan Queued Scan Priority
- License Unavailable
- Paused Scan Priority

The following table provides examples using five scans with various statuses, priorities, and creation times.

Scan Status	Priority	Created On Date/Time	When Started or Resumed
Paused Scan Priority	0	9/26/2025 08:00 AM	Fifth
Resume Scan Queued	5	9/26/2025 08:15 AM	Second
Resume Scan Queued Scan Priority	5	9/26/2025 09:00 AM	Third
Queued	5	9/26/2025 11:26 AM	Fourth
Queued	10	9/26/2025 12:01 PM	First

Priority and sensors

When configuring a scan, you can select a specific sensor in the Run Scan or Schedule Scan dialog boxes. You can also select the **Use this sensor only** option. The following table describes how these options affect advanced scan prioritization.

Selected Sensor Options	What Happens
A specific sensor is selected with the **Use this sensor only** option	If the sensor is available, then the scan starts on the sensor. If the sensor is not available and there is a lower-priority scan that is running on that sensor, then the lower-priority scan is paused and the higher-priority scan is started on the sensor.
A specific sensor is selected *without* the **Use this sensor only** option	If the sensor is available, then the scan starts on the sensor. If the sensor is not available, the Global Service attempts to find any other available sensor in the sensor pool. If an available sensor is found, the scan starts on that sensor. If no sensor is available, the Global Service checks whether a lower-priority scan is running. If a lower-priority scan is running, then the lower-priority scan is paused and the higher-priority scan is started on that sensor.
Any Available sensor is selected	If a sensor is available in the sensor pool, then the scan is started on the sensor. If no sensor is available in the sensor pool, the Global Service checks whether a lower-priority scan is running. If a lower-priority scan is running, then the lower-priority scan is paused and the higher-priority scan is started on that sensor.

When advanced scan prioritization is disabled

If the **Disable Advanced Scan Prioritization** option was selected in the ScanCentral DAST Configuration Tool, then when a lower-priority scan is paused for a higher-priority scan to run, the lower-priority scan resumes only on the sensor on which it was originally running, regardless to whether another sensor is available in the sensor pool. Partial scan results are uploaded to the ScanCentral DAST database, but the paused scan remains on the sensor. If the scan is resumed, but the scan no longer exists on the sensor for any reason, the Global Service downloads and imports the partial results prior to resuming the scan.

For more information, see "Configuring scan priority" on page 195.

Configuring data retention

If data retention is enabled for the application being scanned, then a default number of days for scan retention is configured in the application settings. In such cases, the default number of days for scan retention is displayed in the Details page. For more information, see "Working with application settings" on page 418.

To set a number of days other than the default setting for the scan:

- Enter the number of days in the **Data Retention** box.

Note: If you set a number of days that differs from the Application Settings, the lower of the two settings will be used.

Scanning single-page applications

This topic describes single-page application (SPA) support for crawling and auditing the Document Object Model (DOM) of an application.

The challenge of single-page applications

Developers use JavaScript frameworks such as Angular, Ext JS, and Ember.js to build SPAs. These frameworks make it easier for developers to build applications, but more difficult for security testers to scan those applications for security vulnerabilities.

Traditional sites use simple back-end server rendering, which involves constructing the complete HTML web page on the server side. SPAs and other Web 2.0 sites use front-end DOM rendering, or a mix of front-end and back-end DOM rendering. With SPAs, if the user selects a menu item, the entire page can be erased and recreated with new content. However, the event of selecting the menu item does not generate a request for a new page from the server. The content update occurs without reloading the page from the server.

With traditional vulnerability testing, the event that triggered the new content might destroy other events that were previously collected on the SPA for audit. Through its SPA support, the dynamic sensor offers a solution to the challenge of vulnerability testing on SPAs.

Configuring SPA support

When SPA support is enabled, the DOM script engine finds JavaScript includes, frame and iframe includes, CSS file includes, and AJAX calls during the crawl, and then audits all traffic generated by those events.

To configure SPA support:

- Under **Single-Page Applications** on the Details page, select one of the following options:

- **Automatic** - If the sensor detects a SPA framework, it automatically switches to SPA-support mode.
- **Disabled** - Indicates that SPA frameworks are not used in the target application.
- **Enabled** - Indicates that SPA frameworks are used in the target application.

  Caution! Enable SPA support for single-page applications only. Enabling SPA support to scan a non-SPA website results in a slow scan.

Enabling traffic monitor

The site tree of a scan normally displays only the hierarchical structure of the website or web service, plus those sessions in which a vulnerability was discovered. If traffic monitor is enabled, then the Traffic Viewer tool and the Traffic table in the scan results allow you to view every HTTP request sent by the sensor and the associated HTTP response received from the web server.

Note: The Traffic Viewer tool is not included with ScanCentral DAST. However, if you have Fortify DAST installed locally, you can use the tool that is included with your local installation.

Option must be enabled

To see all traffic in the Traffic Viewer tool or in the Traffic table in the scan results, you must enable Traffic Monitor logging in the scan settings.

Note: The Traffic table is always available in the scan results in ScanCentral DAST. However, enabling Traffic Monitor logging includes all of the scan traffic.

Enabling traffic monitor logging

To enable traffic monitor logging:

- Under **Traffic Analysis** on the Details page, select **Enable Traffic Monitor**.

Creating and managing basic exclusions

You can exclude URLs and sessions—based on criteria in their requests or responses—from being crawled and audited. Excluding URLs means that the sensor will not examine the specified URL or host for links to other resources. Excluding sessions means that sensor will not process the sessions that meet the exclusion criteria.

To exclude these items from your scan, you must create a list of Basic Exclusions. Each exclusion in the list identifies one or more targets in which the criteria for exclusion is found.

Note: You can add multiple targets to each entry in the Basic Exclusions list.

Creating exclusions

To create one or more exclusions:

1. Under **Basic Exclusions** on the Details page, click **CREATE**.
   The MANAGE EXCLUSIONS dialog box opens.
2. Type a name for the exclusion in the **Name** box.
3. From the **Target** list, select one of the following target types to configure for exclusion:
   - **Extension** - Excludes file extensions that match the exclusion criteria
   - **Host** - Excludes hosts that match the exclusion criteria
   - **Post parameter** - Excludes sessions with a POST request parameter that matches the exclusion criteria
   - **Query parameter** - Excludes sessions with a query parameter in the URL that matches the exclusion criteria
   - **Request** – Excludes sessions with a request that matches the exclusion criteria
   - **Response** – Excludes sessions with a response that matches the exclusion criteria
   - **Response header** - Excludes sessions with a response header that matches the exclusion criteria
   - **Status code** - Excludes sessions with a response status code that match the exclusion criteria
   - **URL** – Excludes URLs that match the exclusion criteria
4. Type a name for the target in the **Name** box.
5. Select one of the following types of exclusion for the target from the **Type** list:
   - **Matches Regex** – Matches the regular expression you specify in the **String** box
   - **Matches Regex extension** – Matches the regular expression extension you specify in the **String** box
   - **Matches** - Matches the specified criteria in the **String** box
   - **Contains** – Contains the text string you specify in the **String** box
6. Type the string to match in the **String** box.
   For examples of Target, Type, and String settings, see "Exclusion examples" on the next page.
7. Click **add** +.
   The exclusion is added to the exclusion list.
8. Optionally, to create another exclusion, return to Step 3. Otherwise, go to Step 9.
9. When the list of exclusions is complete, click **OK**.

Exclusion examples

The following table provides examples of exclusions.

To...	Create the following exclusion...
Ensure that you never send requests to any resource at Microsoft.com	URL contains `Microsoft.com`
Exclude the following directories: `http://www.test.com/W3SVC55/` `http://www.test.com/W3SVC5/` `http://www.test.com/W3SVC550/`	URL matches regex `/W3SVC[0-9]*/`
Ensure that you never process session responses with 404 Not Found	Response contains `Not Found`

For more information about creating exclusions, see "Understanding and creating inclusive exclusions" below.

Editing or removing exclusions

To edit or remove an entry in the **Basic Exclusions** list:

1. Select an entry from the **Basic Exclusions** list.
2. Do one of the following:
   - To edit the exclusion settings, click **MANAGE**.

     The MANAGE EXCLUSIONS dialog box opens. For more information about using this dialog box, see "Creating exclusions" on the previous page.
   - To remove the host from the allowed hosts list, click **REMOVE**.

Understanding and creating inclusive exclusions

When a site contains many pages that are essentially redundant, it makes sense to scan only a selection of such pages and exclude the rest. To accomplish this, we need to specify what to include by excluding everything else. Such exclusions are called "inclusive exclusions."

You can create regular expressions that exclude everything including the sessions you want to scan, and then add the inclusion regular expression within the negative look ahead construct.

Understanding inclusive exclusion regular expressions

Suppose you have the following URLs:

```
http://site.tld/sub/sub1
http://site.tld/sub/sub2
http://site.tld/sub/sub3
http://site.tld/sub/sub4
http://site.tld/sub/sub5
...
http://site.tld/sub/sub9999
```

And you want to include `sub1` in the scan but not `sub2` through `sub9999`.

A regular expression to match and exclude everything is:

```
\/sub/sub[0-9]+
```

Adding the negative look ahead to include `sub1` results in this regular expression:

```
\/sub/sub(?!1)[0-9]+
```

This regular expression matches and excludes everything in the previous list of URLs that does not include `sub1`.

Important! If the regular expression includes the host name, then it must also include the port as shown here:

```
site\.tld:80/sub/sub[0-9]+
```

```
site\.tld:80/sub/sub(?!1)[0-9]+
```

The following paragraphs provide additional examples of various inclusive exclusions.

Example one

Suppose you want to scan only the contents of folders where the folder name starts with the combination "N13" and omit the others in the following list:

```
http://10.0.6.124:22000/cssbundle/1666793387/bundles/service.css
http://10.0.6.124:22000/cssbundle/N1375383199/bundles/service.css
http://10.0.6.124:22000/jsbundle/1337374041/bundles/catalogs.js
http://10.0.6.124:22000/jsbundle/1337374041/bundles/general.js
http://10.0.6.124:22000/jsbundle/335652056/bundles/search.js
http://10.0.6.124:22000/jsbundle/N1222120407/bundles/
http://10.0.6.124:22000/jsbundle/N1408948977/bundles/
http://10.0.6.124:22000/jsbundle/N1982198842/bundles/
http://10.0.6.124:22000/jsbundle/N273479010/bundles/
```

A regular expression to match and exclude all folder names that begin with letter "N" is:

```
 \/N[\d]+\/
```

Adding the negative look ahead to include `(?!13)` results in this regular expression:

```
\/N(?!13)[\d]+\/
```

Using this regular expression as a session exclusion causes Fortify DAST to omit all of the paths except for those where the folder name starts with the combination "N13":

```
http://10.0.6.124:22000/cssbundle/N1375383199/bundles/service.css
```

Note: The number "13" is arbitrary. You could easily replace the "13" character set in the regular expression with your desired character set.

Example two

Suppose you want to omit most of My Awesome Store's catalog while still permitting URLs that include keywords "awesome" or "core" in the following list:

```
http://my.awesome.store.com/dotcom/14k-gold-plated-ring/cat.jump
http://my.awesome.store.com/dotcom/2-panel-jewelry-box/prod.jump
http://my.awesome.store.com/dotcom/core-short-sleeve-top/prod.jump
http://my.awesome.store.com/dotcom/core-graphic-tee/prod.jump
http://my.awesome.store.com/dotcom/core-pro-striped-shorts/prod.jump
http://my.awesome.store.com/dotcom/awesome-brand-pro-striped-shorts/prod.jump
http://my.awesome.store.com/dotcom/core-pro-striped-shorts/prod.jump
http://my.awesome.store.com/dotcom/shoes/sandals-flip-flops/low-mid-
heel/cat.jump
http://my.awesome.store.com/dotcom/shoes/sandals-flip-flops/wedge-
sandals/cat.jump
http://my.awesome.store.com/dotcom/shoes/sandals-flip-flops/flat-
sandals/cat.jump
http://my.awesome.store.com/dotcom/shows/all-mens-shoes/slippers/cat.jump
http://my.awesome.store.com/dotcom/men/shorts/bermuda-core-beige/prod.jump
http://my.awesome.store.com/dotcom/men/shorts/pleated-core-beige/prod.jump
http://my.awesome.store.com/dotcom/men/shorts/bermuda-awesome-brand-
beige/prod.jump
http://my.awesome.store.com/dotcom/core-proportioned-pants/prod.jump
http://my.awesome.store.com/dotcom/awesome-brand-slender-jean---plus/prod.jump
http://my.awesome.store.com/dotcom/awesome-brand/half-zip-jacket/prod.jump
http://my.awesome.store.com/dotcom/toys/categories/costumes-dress-
up/boys/cat.jump
http://my.awesome.store.com/dotcom/shoes/kids-shoes/boys-shoes/cat.jump
http://my.awesome.store.com/dotcom/toys/gender/boys/cat.jump
http://my.awesome.store.com/dotcom/shoes/boots/ankle-boots-booties/cat.jump
http://my.awesome.store.com/dotcom/shoes/all-womens-shoes/view-all/cat.jump
http://my.awesome.store.com/dotcom/women/awesome-brand/tops-sweaters/cat.jump
http://my.awesome.store.com/dotcom/men/wallets-accessories/backpacks-
```

```
bags/cat.jump
http://my.awesome.store.com/dotcom/women/wear-to-work/skirts/cat.jump
```

A regular expression to include "awesome" or "core" keywords is:

```
\/dotcom\/((?!awesome|core)[\w-%\/])+(?:cat|prod)\.jump
```

Configuring redundant page detection

Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, the sensor would never be able to finish the scan. The **Perform redundant page detection** option compares page structure to determine the level of similarity, allowing the sensor to identify and exclude processing of redundant resources.

Important! Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan.

To configure redundant page detection:

1. Select the **Perform redundant page detection** check box.
2. Configure settings as described in the following table.

Setting	Description
Page Similarity Threshold (%)	Indicates how similar two pages must be to be considered redundant. Enter a percentage from 1 to 100, where 100 is an exact match. The default setting is 95 percent.
Tag attributes to include	Identifies the tag attributes to include in the page structure. Typically, tag attributes and their values are dropped when determining structure. Identifying tag attributes in this list adds those attributes and their values in the page structure. By default, `id` and `class` tag attributes are included. To add tag attributes: a. Type the attribute name in the **Tag item** box. Do not include tag brackets (`<` and `>`). b. Click **ADD**. The tag attribute is added to the **Tag attributes to include** list. **Tip:** Certain sites may be primarily composed of one type of tag, such as `<div>`. Including these attributes creates a more

Setting	Description
	rigid page match. Excluding these attributes creates a less strict match.

Enabling SAST correlation

SAST correlation correlates the static and dynamic findings for your web application in Application Security. Correlation enables you to see the static findings that were also found in a dynamic scan. It can help you to prioritize which issues to fix and help verify that those issues are not false positives.

To enable SAST correlation:

- Select **Enable SAST Correlation**.

Reviewing scan settings

You can review the settings you configured for the scan on the Review page.

After you review the settings, do one of the following:

- If the settings are correct, type a name for the settings in the **Name** box.
- If changes are needed, click the page name in the navigation pane, and then make corrections.

  Tip: The names of pages that contain missing information or errors are displayed in red text in the navigation pane.

When the settings are correct, do one of the following:

- Save the settings to Application Security (For instructions, see "Saving the settings to Application Security" on the next page.)
- Schedule a scan (For instructions, see "Scheduling a scan" on the next page.)
- Run a scan (For instructions, see "Running a scan" on page 207.)
- Use the settings in the API (For instructions, see "Using the scan settings in the DAST API" on page 208.)

Saving the settings to Application Security

You can save the settings as a template to Application Security. The settings are stored in XML format along with a JSON object with setting overrides.

To save as a template:

- Click **SAVE**.
  The file is saved to Application Security.

Scheduling a scan

You can use the settings for a scheduled scan to be run later.

To schedule a scan:

1. Click **SCHEDULE**.
   The SCAN SCHEDULE dialog box opens.
2. Type a name for the scheduled scan in the **Name** box.
3. Enter a date for the scan to run in the **Start Date** box.

   Tip: To select a date from the calendar, click the **calendar** button.
4. Enter a time for the scan to start in the **Start Time** box.

   Note: The schedule uses the time zone from your browser.
5. To schedule a recurring scan, in the **Pattern** section specify how often to run the scan according to the following table.

To run...	Then...
Daily	a. Select **DAILY**. b. Select a recurrence in the **Occur every ___ day** box.
Weekly	a. Select **WEEKLY**. b. Select a recurrence in the **Occur every ___ week** box. c. Select the days to run each week.
Monthly	a. Select **MONTHLY**. b. Select a recurrence in the **Occur every ___ month** box. c. Do one of the following: ◦ Select **Occur on day** and enter a date in the box.

To run...	Then...
	◦ Select **Occur on the**, and then select an interval from the **Interval** list and a day from the **Day** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.
Yearly	a. Select **YEARLY**. b. Do one of the following: ◦ Select **Occur on**, and then select a month from the **Month** list and enter a date in the **Day** box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list, a day from the **Day** list, and a month from the **Month** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.

6. Under **Range**, do one of the following:
   - To leave the recurrence open ended, select **Never ends**.
   - To set an end date, select **Ends by**, and then enter an end date in the **End Date** box or enter the number of occurrences after which to end in the **occurrence** box.

     Note: Entering data into the **End Date** box automatically updates the **occurrence** box, and conversely.
7. Select a dynamic sensor from the **Sensor** list.

   The list of sensors comes from the Application Security sensor pools. **Any Available** is the default.
8. (Optional) If you select a sensor that is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
9. Click **OK**.

   The scan schedule is added to the ScanCentral DAST database.

Running a scan

You can use the settings to run a scan immediately. To run a scan:

1. Click **RUN**.

   The RUN SCAN dialog box opens.

Note: The name you gave to the settings appears in the **Name** field. You can type a different name in the field if needed.

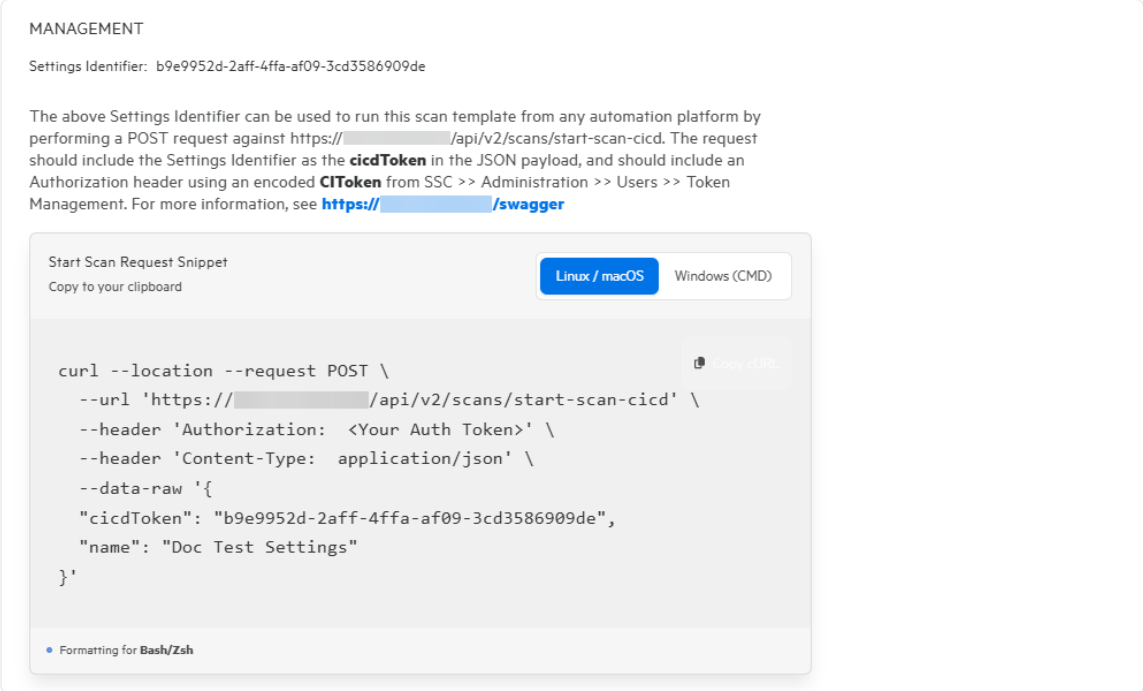
2. Select a ScanCentral DAST sensor from the **Sensor** list.

   The list of sensors comes from the Application Security sensor pools. **Any Available** is the default.
3. (Optional) If you select a sensor, but it is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
4. Click **RUN**.

   The scan is queued to run.

Using the scan settings in the DAST API

You can use the scan settings to conduct a scan from the DAST API.



After saving the settings, the GUID in the **Settings Identifier** field provides a unique identifier for the settings. You can select a cURL sample for Linux, macOS, or Windows, and then copy the sample that includes the GUID to use in the API.

Note: This GUID is also known as the CICD Identifier.

If you copy the settings before saving, a placeholder is used for the settings ID. You must manually update the sample with the settings ID.

To copy the cURL sample:

1. Do one of the following:
   - For a Linux or macOS compatible cURL sample, click **Linux / macOS**.
   - For a Windows compatible cURL sample, click **Windows (CMD)**.
2. Click **copy to clipboard** .

Accessing the DAST API Swagger UI

Complete documentation—including detailed schema, parameter information, sample code, and functionality for testing endpoints—is included in the DAST API Swagger UI.

To access this information:

- In your browser, navigate to the DAST API URL using the following format:
  `http://<ScanCentral_DAST_API_URL>:<Port>/swagger/index.html`

Using the Swagger UI

To use the Swagger UI:

1. On the Swagger UI page, click an endpoint category.
2. Click the endpoint method to use.

   Detailed schema, parameter information, sample code, and functionality for testing the endpoint appear.
3. (Optionally) To view a previous version of the DAST API, select the version from the **Select a definition** list.

   Important! The latest version of the DAST API includes newer functionality than older versions. For this reason, OpenText recommends that you use the most recent version of the DAST API.

Conducting an automated scan with FAST

Functional Application Security Testing (FAST) is a lightweight proxy that integrates with Fortify ScanCentral DAST. FAST provides a way to capture traffic from functional test scripts, such as those of Selenium, Cucumber, Curl, Postman, Unified Functional Test (UFT), and others. FAST turns the captured traffic into a workflow macro and sends it to ScanCentral DAST, which uses the macro and an existing scan settings identifier to conduct a scan.

Automation overview

The automation scenario involves three stages:

1. Start the FAST proxy using a CLI command (or commands).
2. Run functional tests though the FAST proxy.
3. Stop the FAST proxy using a CLI command.

FAST versions available

FAST is available in two versions:

- Windows MSI installer (For more information, see "Using the FAST Windows version" below.)
- Linux Docker image (For more information, see "Using the FAST Linux version" on page 213.)

Using the FAST Windows version

The following paragraphs describe how to install and use the Windows version of FAST.

Installation recommendation

Important! Do not install the FAST proxy on the same machine as Fortify DAST or an Fortify DAST sensor being used with Fortify WebInspect Enterprise.

OpenText recommends that you install the FAST proxy on the machine that runs your functional tests, and then control the FAST proxy using the command line interface (CLI). This installation method allows you to integrate FAST CLI scripts into your functional testing automation pipeline.

Before you begin

You will need to following items to conduct an automated scan with FAST:

- The `WIRCServerSetup64-ProxyOnly.msi` installer
- An authentication token from Application Security
- A settings identifier, or GUID, for scan settings in ScanCentral DAST
- The ScanCentral DAST API URL

Process overview

The following table describes the process for conducting an automated scan with FAST.

Stage	Description
1.	Download and install the `WIRCServerSetup64-ProxyOnly.msi`. For more information, see "Downloading the FAST installer" on the next page.
2.	Obtain an authentication token of type **CIToken** from Application Security. For more information, see the *OpenText™ Application Security User Guide*. **Tip:** This token is passed as the value for the `CIToken` in the FAST command.
3.	Obtain a settings identifier from a scan settings file in ScanCentral DAST. For more information, see "Understanding the scan settings detail panel" on page 350. **Tip:** This token is passed as the value for the `CICDToken` in the FAST command.
4.	On the machine where you installed the FAST proxy, open the command prompt and start the FAST proxy. **Tip:** The default installation directory for the FAST proxy is `C:\Program Files\Micro Focus WIRC Server\Fast.exe`. The following is an example of the command to start the proxy: `Fast.exe -p <ListeningPort> -u http://<host|ip>:<port>/api/ -CIToken <Base64_encoded_token> -CICDToken <Guid>` You should see a response similar to the following: `0.0.0.0:<ListeningPort>` `Listening` For descriptions of these and other FAST command options, see "Understanding the FAST options for Windows" on the next page.
5.	Run the traffic from your functional tests through the FAST proxy IP address and port specified in the start command. **Note:** If your functional tests run on the same machine where you installed the FAST proxy, then you can use `127.0.0.1` for proxy address.
6.	After traffic has been captured, stop the FAST proxy. The following is an example of the command to stop the proxy:

Stage	Description
	`Fast.exe -p <ListeningPort> -s`
7.	The ScanCentral DAST instance specified in the `<DAST_API_HOST|IP>/api/` option automatically runs the scan with workflow overrides applied to the settings.

Downloading the FAST installer

The FAST installer, named `WIRCServerSetup64-ProxyOnly.msi`, is included in the ScanCentral DAST download package. It is packaged in a ZIP file named `Dynamic_Addons.zip`.

Understanding the FAST options for Windows

The following table describes the FAST options used in the Windows command.

Option	Description
`-h`	Displays the help.
`-p`	Specifies the listening port for the FAST proxy. Example: `-p <port>`
`-n`	Identifies the scan name that will appear in ScanCentral DAST. For example: `-n <FAST_scan_name>`
`-u`	Specifies the ScanCentral DAST URL. Example: `-u https://<DAST_API_HOST|IP>:<port>/api/`
`-c`	Optionally, exports the FAST proxy root CA certificate. If your `https` application performs certificate validation, you can use this option alone to install the certificate on your client application to avoid an untrusted certificate error. Example:

Option	Description
	`-c c:\fast_proxy_ca.crt`
`-f`	Optionally when starting the proxy, specifies a regular expression for the allowed hosts for proxy capture. Example: `-f ".*\.<hostname>\.com"`
`-ps`	Optionally when starting the proxy, configures an external proxy server when the target application does not have direct access from the machine where the FAST proxy is installed. Example: `-ps <host|ip>:<port>`
`-s`	Stops listening. Example: `-s -p <port>`
`-q`	Runs the FAST proxy in quiet mode. This mode does not display messages.
`-k`	Keeps local traffic files after capture.
`-CICDToken`	Specifies the Guid for the scan settings in ScanCentral DAST.
`-CIToken`	Specifies the Base64-encoded authentication token from Application Security.

Using the FAST Linux version

The following paragraphs describe how to configure and use the Linux Docker image version of FAST.

Options for accessing your functional tests

To create a macro from your functional tests, the FAST proxy must have access to those tests. Consider the following options for accessing your functional tests with the Linux Docker image version of FAST:

1. Run Docker on the machine that runs your functional tests.
2. Run the FAST proxy on a remote Docker host by using a run command similar to the following:

```
docker -H=your-remote-docker:2375 run
```

3. Use remote Docker by way of the Docker REST API.

For Docker documentation, see https://docs.docker.com/.

For options 2 and 3, the functional tests can be on any machine with network access to the Docker host where FAST is running.

Regardless of the option you choose, the Docker host where FAST is running must have network access to the DAST API to upload the macro.

Process overview

The following table describes the process of configuring and using the Linux version of FAST.

Stage	Description
1.	Prepare a Linux VM machine with Red Hat Enterprise Linux 8 distribution for x86-64 or Ubuntu 22.04, 20.04, 18.04, LTS x64. This machine will be the host for the FAST image.
2.	Install the appropriate Docker Engine for your host machine. **Important!** Follow Docker recommendations for the Docker engine version to use for Red Hat Universal Base Image (UBI) 8.x x86_64 or Ubuntu 22.04 LTS x86_64 host operating systems.
3.	Pull the FAST Docker image. For more information, see "Pulling the FAST image" on the next page.
4.	Obtain an authentication token of type **CIToken** from Application Security. For more information, see the *OpenText™ Application Security User Guide*. **Tip:** This token is passed as the value for the `CIToken` in the FAST command.
5.	Obtain a settings identifier from a scan settings file in ScanCentral DAST. For more information, see "Understanding the scan settings detail panel" on page 350. **Tip:** This token is passed as the value for the `CICDToken` in the

Stage	Description
	FAST command.
6.	Run the FAST Docker container. For more information, see "Running the FAST container" below.
7.	Run the traffic from your functional tests through the FAST proxy IP address and port specified in the run command.
8.	After traffic has been captured, stop the FAST proxy. For more information, see "Stopping the container" on the next page.
9.	The ScanCentral DAST instance specified in the *<DAST_API_HOST|IP>*/api/ option automatically runs the scan with workflow overrides applied to the settings.

Pulling the FAST image

After installing the Docker Engine on your host machine and starting the Docker service, you can pull an image of Fortify FAST from the Fortify Docker repository.

To pull the current version of the Fortify FAST UBI image:

- At the terminal prompt on the Red Hat host machine, enter the following command:

```
docker pull fortifydocker/fortify-fast:26.4ubi.9
```

To pull the current version of the Fortify FAST Ubuntu image:

- At the terminal prompt on the Ubuntu host machine, enter the following command:

```
docker pull fortifydocker/fortify-fast:26.4.ubuntu.2204
```

Running the FAST container

After you have pulled the image, you can run a container to capture traffic from your functional test scripts.

To run the Fortify FAST UBI container:

- At the terminal prompt, enter the following commands:

```
CONTAINER_NAME="fortify-fast"
IMAGE_NAME="fortifydocker/fortify-fast:26.4ubi.9"
mkdir -p "$HOME/.fast/certs"
docker run --name $CONTAINER_NAME \
```

```
    -p <port>:<port> \
    -v "$HOME/.fast/certs:/etc/fast/certs" \
    --rm \
    $IMAGE_NAME \
    -p <port> \
    -u http://<host|ip>:<port>/api/ \
    -CIToken <Base64_encoded_token> \
    -CICDToken <Guid>
```

To run the Fortify FAST Ubuntu container:

- At the terminal prompt, enter the following commands:

```
CONTAINER_NAME="fortify-fast"
IMAGE_NAME="fortifydocker/fortify-fast:26.4.ubuntu.2204"
mkdir -p "$HOME/.fast/certs"
docker run --name $CONTAINER_NAME \
    -p <port>:<port> \
    -v "$HOME/.fast/certs:/etc/fast/certs" \
    --rm \
    $IMAGE_NAME \
    -p <port> \
    -u http://<host|ip>:<port>/api/ \
    -CIToken <Base64_encoded_token> \
    -CICDToken <Guid>
```

You should see a response similar to the following:

```
0.0.0.0:<ListeningPort>
Listening
```

For descriptions of these run command options, see "Understanding the run command options" on the next page.

Stopping the container

After you have captured the traffic, you can stop the container and upload the results to ScanCentral DAST.

To stop the container:

- At the terminal prompt, enter the following command:

```
docker exec $CONTAINER_NAME fast -p <port> -s
```

Understanding the run command options

The following table describes the options used in the run command.

Option	Description
`--name`	Specifies the name of your Fortify FAST container. Any string is valid. In the sample code, the name is taken from the `CONTAINER_NAME="fortify-fast"` command.
`-p <port>:<port>`	Publishes the container's main TCP ingress port to the host. For example: `-p 8087:8087`
`-v "$HOME/.fast/certs:/etc/fast/certs" \`	Adds a volume for a Fortify FAST auto-generated certificates directory. This directory safeguards the certificates in case the Fortify FAST container needs to be removed or upgraded.
`--rm`	Automatically removes the container when it exits.
`$IMAGE_NAME \` `-p <port>`	Specifies the listening port for the FAST proxy. For example: `-p 8087`
`-u http://<host|ip>:<port>/api/`	Specifies the ScanCentral DAST URL. For example: `-u https://dast-web-api:64814/api/`
`-CICDToken`	Specifies the Guid for the scan settings in ScanCentral DAST.
`-CIToken`	Specifies the Base64-encoded authentication token from Application

Option	Description
	Security.
`-s`	Stops listening.

Chapter 5: Working with Advanced scan settings

Some scan settings are not visible in the Basic view of the Scan Settings Configuration or Base Settings Configuration wizards. You can see these additional settings in the Advanced view in the wizards.

Note: The Advanced view includes the settings that are found in the Basic view. This design enables you to configure all scan settings in the Advanced view without switching between views. Descriptions of the Basic view settings, however, are not included in this chapter. For information about the Basic view settings, see "Configuring a scan" on page 150 or "Working with base settings" on page 373.

Accessing the Advanced settings view

You can access the Advanced view while configuring scan settings or base settings.

To access the Advanced view:

- In the SCAN SETTINGS CONFIGURATION or BASE SETTINGS CONFIGURATION wizard, click **ADVANCED**.

  The Advanced view appears.

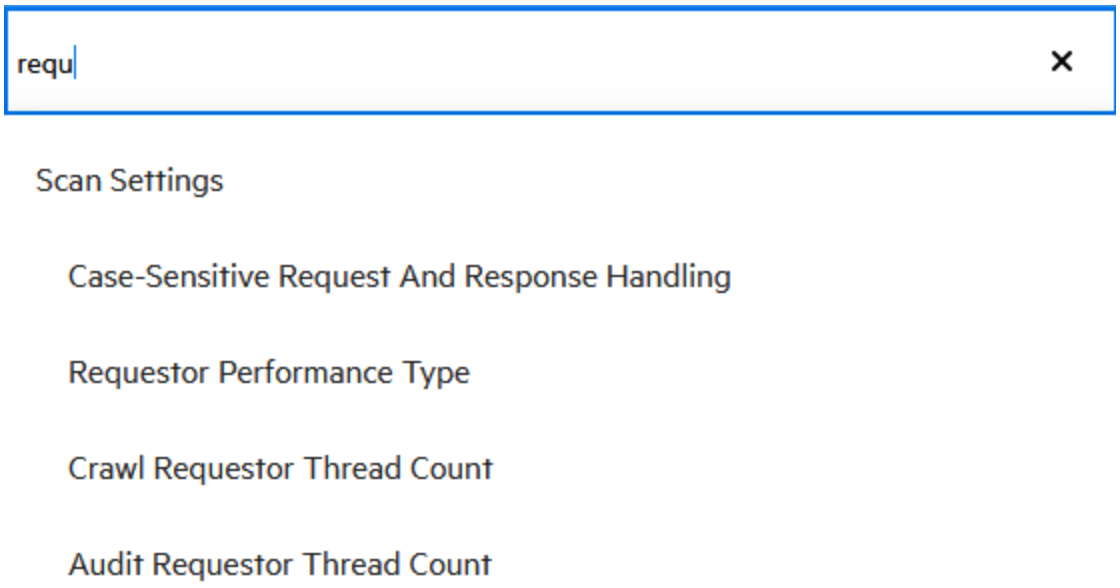
Searching for a setting

If you are not sure where to find a setting in the wizards, you can search for the setting in the Advanced view.

To search for a setting:

1. In the **Search settings** box, type the setting name.

   As you type, settings that match the letters typed are displayed in a list.



2. Select a setting from the list.

Important! The search is a search of the UI that is currently being displayed based on the currently configured settings. For example, if authentication is disabled, and you search for macro settings, the macro settings will not be found because the current settings do not include authentication.

Using advanced settings in the API

The `application-version-scan-settings/advanced` API endpoint under `ApplicationVersionScanSettings` includes the same advanced settings that are described in this document. This topic provides useful information to assist you in finding and using advanced settings in the ScanCentral DAST API. For more information about accessing and using the API, see "Using the scan settings in the DAST API" on page 208.

Facts about using advanced settings in the API

Keep the following facts in mind when using advanced settings in the API:

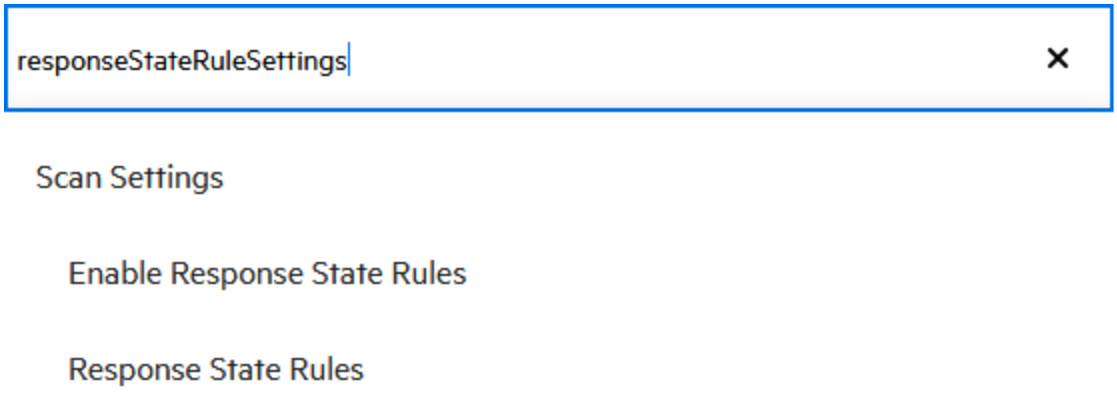
- If a value for any advanced setting is deleted in the API, the sensor will use the default setting during the scan.
- The maximum value allowed for a numeric value is 2147483647. This is a limitation of .Net. If a setting is larger than this value, you will receive the .NET error code 435 before the value is processed by ScanCentral DAST. Most of the value ranges for the advanced settings are much smaller than this value. However, this might be useful information while troubleshooting error codes.

Searching for settings to use in the API

If you routinely configure scan settings using the ScanCentral DAST API, you can use the setting name or property from the API to search for the settings in the ScanCentral DAST UI. For a description of the setting, you can then locate the setting name from the UI in this document.

To search for a setting name:

1. In the Swagger UI, copy a property from the `application-version-scan-settings/advanced` API endpoint. For example, `responseStateRuleSettings` or `autoDetectFileNotFoundPageSettings`.
2. In the **Search settings** box in the ScanCentral DAST UI, paste the setting name. Settings that match the letters typed are displayed in a list.



3. Select a setting from the list.

Important! The search is a search of the UI that is currently being displayed based on the currently configured settings. For example, if authentication is disabled, and you search for macro settings, the macro settings will not be found because the current settings do not include authentication.

Getting default advanced setting values

Many of the default values in the `application-version-scan-settings/advanced` API endpoint come from Swagger and might not be valid for use in ScanCentral DAST. For assistance in configuring settings, you can use the `utilities/default-advanced-scan-settings` API endpoint under `Utilities` to retrieve default advanced scan settings values that are valid for use in ScanCentral DAST.

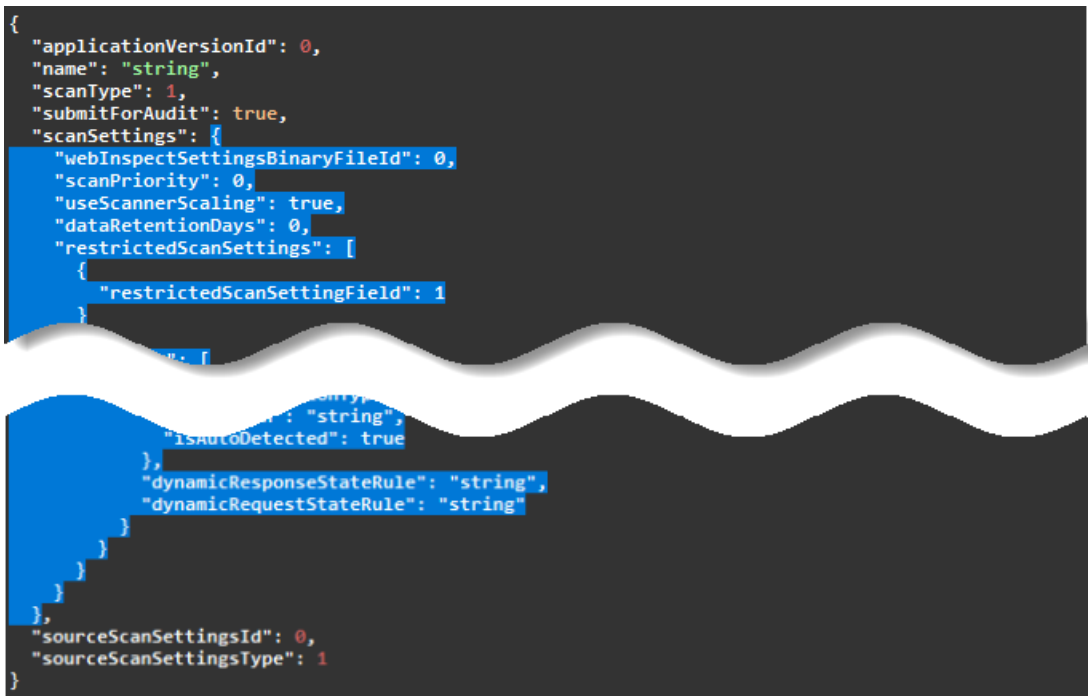
To retrieve default values:

1. In the Swagger UI, locate `utilities/default-advanced-scan-settings` API endpoint under `Utilities`.
2. Click **Execute**.

Default settings are returned in the Response body.

3. In the **Example Value** view of the Response body, select all lines of code and then click the copy button in the Swagger UI.
4. Select the entire "`scanSettings`" portion of code in `application-version-scan-settings/advanced` endpoint.

Important! Be sure to include the opening brace after "`scanSettings`" and the closing brace before "`sourceScanSettingsId`" as shown in the following image.



5. Paste the code copied from the `default-advanced-scan-settings`.

Configuring method settings

The method settings enable you to configure the crawl and audit mode and other details.

Configuring the Crawl and Audit Mode

The crawl and audit mode advanced setting is available only if the scan mode is set to **Crawl and Audit**.

Tip: If you selected **Crawl Only** or **Audit Only** on the Target page in the Basic view of the Scan Settings Configuration or Base Settings Configuration wizard, you can change it in the advanced settings to enable the crawl and audit mode advanced setting.

To change the crawl and audit mode advanced setting:

- In the **CRAWL AND AUDIT MODE** area, select a Scan Strategy Type as described in the following table.

Type	Description
Simultaneously	As the sensor maps the site's hierarchical data structure, it audits each resource (page) as it is discovered, rather than crawling the entire site and then conducting an audit. This option is most useful for extremely large sites where the content could change before the crawl can be completed. **Note:** This is the default setting.
Sequentially	The sensor crawls the entire site, mapping the site's hierarchical data structure, and then conducts a sequential audit, beginning at the site's root.

Configuring the crawl and audit details

To change the crawl and audit details:

- In the **CRAWL AND AUDIT DETAILS** area, choose from the options described in the following table.

Option	Description
Include search probes (send search attacks)	If you select this option, the sensor will send requests for files and directories that might or might not exist on the server, even if those files are not found by crawling the site. **Note:** This option is selected by default only when the Scan Mode is set to **Crawl and Audit**. The option is not selected by default when the Scan Mode is set to **Crawl Only** or **Audit Only**.
Crawl links on File Not Found responses	If you select this option, the sensor will look for and crawl links on responses that are marked as “file not found.” **Note:** This option is selected by default when the Scan Mode is set to **Crawl Only** or **Crawl and Audit**. The option is not available when the Scan Mode is set to **Audit Only**.

Configuring general settings

The general settings enable you to configure scan and crawl details.

Configuring Scan Details

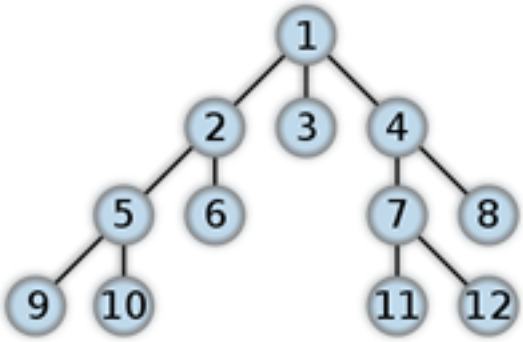
Configure the Scan Details options as described in the following table.

Option	Description
Enable path truncation	Path truncation attacks are requests for known directories without file names. This may cause directory listings to be displayed. The sensor truncates paths, looking for directory listings or unusual errors within each truncation. **Example:** If a link consists of http://www.site.com/folder1/folder2/file.asp, then truncating the path to look for http://www.site.com/folder1/folder2/ and http://www.site.com/folder1/ may cause the server to reveal directory contents or may cause unhandled exceptions.
Case-sensitive request and response handling	Select this option if the server at the target site is case-sensitive to URLs.
Recalculate correlation data	This option is used only for comparing scans. The setting should be changed only upon the advice of Customer Support personnel.
Compress response data	If you select this option, the sensor saves disk space by storing each HTTP response in a compressed format in the database.
Enable traffic monitor logging	The site tree of a scan normally displays only the hierarchical structure of the website or web service, plus those sessions in which a vulnerability was discovered. If traffic monitor is enabled, then the Traffic Viewer tool and the Traffic table in the scan results allow you to view every HTTP request sent by the sensor and the associated HTTP response received from the web server. For more information, see "Enabling traffic monitor" on page 199.
Encrypt traffic	All sessions are normally recorded in the traffic monitor file as

Option	Description
monitor file	clear text. If you are concerned about storing sensitive information such as passwords on your computer, you can encrypt the file. Encrypted files cannot be compressed. Selecting this option will significantly increase the size of exported scans containing log files. **Note:** The **Encrypt traffic monitor file** option is available after turning on **Enable traffic monitor logging**. **Note:** The Traffic Viewer tool does not support the encryption of traffic files. The **Encrypt traffic monitor file** option is reserved for use under special circumstances with legacy traffic files only.
Maximum crawl-audit recursion depth	When an attack reveals a vulnerability, the sensor crawls that session and follows any link that may be revealed. If that crawl and audit reveals a link to yet another resource, the depth level is incremented and the discovered resource is crawled and audited. This process can be repeated until no other links are found. However, to avoid the possibility of entering an endless loop, you may limit the number of recursions. The default value is 2. The maximum recursion level is 1,000.

Configuring Crawl Details

By default, the sensor uses breadth-first crawling, which begins at the root node and explores all the neighboring nodes (one level down). Then for each of those nearest nodes, it explores their unexplored neighbor nodes, and so on, until all resources are identified. The following illustration depicts the order in which linked pages are accessed using a breadth-first crawl. Node 1 has links to nodes 2, 3, and 4. Node 2 has links to nodes 5 and 6.



You cannot change this crawling method in the user interface. However, you can configure the Crawl Details options described in the following table.

Option	Description
Enable keyword search audit	A keyword search, as its name implies, uses an attack engine that examines server responses and searches for certain text strings that typically indicate a vulnerability. Normally, this engine is not used during a crawl-only scan, but you can enable it by selecting this option.
Perform redundant page detection	Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, the sensor would never be able to finish the scan. This option compares page structure to determine the level of similarity, allowing the sensor to identify and exclude processing of redundant resources. **Important!** Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan. You can configure the following settings for redundant page detection:

Option	Description
	• **Page Similarity Threshold** – indicates how similar two pages must be to be considered redundant. Enter a percentage from 1 to 100, where 100 is an exact match. The default setting is 95 percent. • **TAG ATTRIBUTES TO INCLUDE** - identifies the tag attributes to include in the page structure. Typically, tag attributes and their values are dropped when determining structure. Identifying tag attributes adds those attributes and their values in the page structure. Select the tag attributes to include in the page structure. To edit a tag attribute or add an attribute to the table, see "Configuring tag attributes" on page 229. **Tip:** Certain sites may be primarily composed of one type of tag, such as `<div>`. Including these attributes creates a more rigid page match. Excluding these attributes creates a less strict match.
Limit maximum single URL hits to	Sometimes, the configuration of a site will cause a crawl to loop endlessly through the same URL. Use this setting to limit the number of times a single URL will be crawled. The default value is 5.
Include parameters in hit count	If you select **Limit maximum single URL hits to** (above), a counter is incremented each time the same URL is encountered. However, if you also select **Include parameters in hit count**, then when parameters are appended to the URL specified in the HTTP request, the crawler will crawl that resource up to the single URL limit. Any differing set of parameters is treated as unique and has a separate count. For example, if this option is selected, then "page.aspx?a=1" and "page.apsx?b=1" will both be counted as unique resources (meaning that the crawler has found two pages). If this option is not selected, then "page1.aspx?a=1" and "page.aspx?b=1" will be treated as the same resource (meaning that the crawler has found the same page twice). **Note:** This setting applies to both GET and POST parameters.

Option	Description
Limit maximum directory hit count to	This option defines the maximum number of sub-directories and pages to be traversed within each directory during the crawl. This setting reduces the scope of the crawl and might be useful in reducing scan times for some sites, such as those consisting of a content management system (CMS). The default setting is 200.
Minimum folder depth	If you select **Limit maximum directory hit count to** (above), this setting defines the folder depth at which the maximum directory hit count will begin to apply. The default setting is 1.
Limit maximum link traversal sequence to	This option restricts the number of hyperlinks that can be sequentially accessed as the sensor crawls the site. For example, if five resources are linked as follows • Page A contains a hyperlink to Page B • Page B contains a hyperlink to Page C • Page C contains a hyperlink to Page D • Page D contains a hyperlink to Page E and if this option is set to "3," then Page E will not be crawled. The default value is 15.
Limit maximum crawl folder depth to	This option limits the number of directories that may be included in a single request. The default value is 15. For example, if the URL is http://www.mysite.com/Dir1/Dir2/Dir3/Dir4/Dir5/Dir6/Dir7 and this option is set to "4," then the contents of directories 5, 6, and 7 will not be crawled.
Limit maximum crawl count to	This feature restricts the number of HTTP requests sent by the crawler and should be used only if you experience problems completing a scan of a large site.
Limit maximum web form submission to	Normally, when the sensor encounters a form that contains controls having multiple options (such as a list box), it extracts the first option value from the list and submits the form; it then extracts the second option value and resubmits the form, repeating this process until all option values in the list have been submitted. This ensures that all possible links will be followed.

Option	Description
	There are occasions, however, when submitting the complete list of values would be counterproductive. For example, if a list box named "State" contains one value for each of the 50 states in the United States, there is probably no need to submit 50 instances of the form. Use this setting to limit the total number of submissions that the sensor will perform. The default value is 3.
Suppress repeated path segments	Many sites have text that resembles relative paths that become unusable URLs after the sensor parses them and appends them to the URL being crawled. These occurrences can result in a runaway scan if paths are continuously appended, such as `/foo/bar/foo/bar/`. This setting helps reduce such occurrences and is enabled by default. With the setting **enabled**, the options are: **1** – Detect a single sub-folder repeated anywhere in the URL and reject the URL if there is a match. For example, `/foo/baz/bar/foo/` will match because "`/foo/`" is repeated. The repeat does not have to occur adjacently. **2** – Detect two (or more) pairs of adjacent sub-folders and reject the URL if there is a match. For example, `/foo/bar/baz/foo/bar/` will match because "`/foo/bar/`" is repeated. **3** – Detect two (or more) sets of three adjacent sub-folders and reject the URL if there is a match. **4** – Detect two (or more) sets of four adjacent sub-folders and reject the URL if there is a match. **5** – Detect two (or more) sets of five adjacent sub-folders and reject the URL if there is a match. If the setting is **disabled**, repeating sub-folders are not detected and no URLs are rejected due to matches.

Configuring tag attributes

You can add tag attributes that are not included by default in the tag attributes to include table in the ADVANCED scan settings view. Additionally, you can edit the default tag attributes.

Adding tag attributes

To add a tag attribute:

1. Click **add tag attribute**+.
   A row is added to the table.
2. In the **Attribute tag name** box, enter that tag name to include in the page structure.
3. Click **confirm** ✔.
   The tag attribute is added to the table.

Editing existing tag attributes

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting a tag attribute

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring JavaScript settings

The JavaScript settings enable you to configure how the JavaScript analyzer works during the scan. The JavaScript analyzer allows the sensor to crawl links defined by JavaScript, and to create and audit any documents rendered by JavaScript.

Configure the JavaScript settings as described in the following table.

Option	Description
Crawl links found from script execution	If you select this option, the crawler will follow dynamic links, such as links generated during JavaScript execution.

Option	Description
Log JavaScript errors	The sensor logs JavaScript parsing errors from the script parsing engine.
Enable JS framework UI exclusions	With this option selected, the sensor JavaScript parser ignores common JQuery and Ext JS user interface components, such as a calendar control or a ribbon bar. These items are then excluded from JavaScript execution during the scan.
Enable site-wide event reduction	When this option is selected, the crawler and JavaScript engine recognize common functional areas that appear among different parts of the website, such as common menus or page footers. This eliminates the need to find within HTML content the dynamic links and forms that have already been crawled, resulting in quicker scans. This option is enabled by default and should not normally be disabled.
Capture web socket events	WebSocket is an asynchronous protocol, which means that not every request requires a response. Most of the time when a request does not receive a response, WebSocket ends with a timeout that affects both scan time and the ability to discover new attack surface. To prevent adversely affecting scan quality, this option is disabled by default.
Max Script Events Per Page	Certain scripts endlessly execute the same events. You can limit the number of events allowed on a single page to a value between 1 and 9999. The default value is 1000.
SPA Support	SPA support applies to single-page applications. When enabled, the DOM script engine finds JavaScript includes, frame and iframe includes, CSS file includes, and AJAX calls during the crawl, and then audits all traffic generated by those events. For more information, see "Scanning single-page applications" on page 198.

Configuring requestor settings

The requestor is the software module that handles HTTP requests and responses. The Requestor settings enable you to configure shared or separate requestors, as well as the maximum number of threads per requestor. You can also configure a maximum response size, number of request attempts, request timeout, and connectivity.

Using a shared requestor

With this option, the crawler and the auditor use a common requestor when scanning a site, and each thread uses the same state, which is also shared by both modules. This option is suitable for use when maintaining state is not a significant consideration.

To use a shared requestor:

1. In the **REQUESTOR PERFORMANCE** area, select **Shared** from the **Requestor Performance Type** drop-down list.
2. In the **Requestor thread count** box, enter the maximum number of threads (up to 75).

Using separate requestors

With this option, the crawler and auditor use separate requestors. Also, the auditor's requestor associates a state with each thread, rather than having all threads use the same state. This method results in significantly faster scans.

When performing crawl and audit, you can specify the maximum number of threads that can be created for each requestor. The **Crawl Requestor Thread Count** can be configured to send up to 25 concurrent HTTP requests before waiting for an HTTP response to the first request; the default setting is 5.

The **Audit Requestor Thread Count** can be set to a maximum of 50; the default setting is 10. Increasing the thread counts may increase the speed of a scan, but might also exhaust your system resources as well as those of the server you are scanning.

To use separate requestors:

1. In the **REQUESTOR PERFORMANCE** area, select **Separate** from the **Requestor Performance Type** drop-down list.
2. In the **Crawl Requestor Thread Count** box, enter the maximum number of threads (up to 25).
3. In the **Audit Requestor Thread Count** box, enter the maximum number of threads (up to 50).

Configuring Requestor Settings

Configure the Requestor Settings options as described in the following table.

Option	Description
Limit maximum response size	Select this option to limit the size of accepted server responses, and then specify the maximum size (in kilobytes). The default is

Option	Description
(kilobytes)	1024000 kilobytes. **Note:** Flash files (.swf) and JavaScript "include" files are not subject to this limitation.
Request retry count (attempts)	Specifies how many times the sensor will resubmit an HTTP request after receiving a "failed" response (which is defined as any socket error or request timeout). The value must be greater than zero.
Request timeout (seconds)	Specifies how long the sensor will wait for an HTTP response from the server. If this threshold is exceeded, the sensor resubmits the request until reaching the retry count. If it then receives no response, the sensor logs the timeout and issues the first HTTP request in the next attack series. The default value is 20 seconds. **Note:** The first time a timeout occurs, the sensor will extend the timeout period to confirm that the server is unresponsive. If the server responds within the extended Request timeout period, then the extended period becomes the new Request timeout for the current scan.
HTTP/2 support	Select to turn on HTTP/2 support.

Configuring Connectivity Settings

There may be occasions during a scan when a web server fails or becomes too busy to respond in a timely manner. You can instruct the sensor to terminate a scan by specifying a threshold for the number of timeouts.

To stop the scan at connectivity loss:

1. Select **Stop scan if loss of connectivity detected**.
2. Configure the connectivity settings as described in the following table.

To...	Then...
Limit the number of consecutive retry failures for a single host...	a. Select **Consecutive 'single host' retry failures to stop scan**. b. In the **Consecutive 'single host' retry failures** box, enter the number of permitted failures from one specific server.

To...	Then...
	The default value is 75.
Limit the number of consecutive retry failures for any host...	a. Select **Consecutive 'any host' retry failures to stop scan**. b. In the **Consecutive 'any host' retry failures** box, enter the total number of consecutive timeouts permitted from all hosts. The default value is 150.
Limit the number of nonconsecutive retry failures for a single host...	a. Select **Nonconsecutive 'single host' retry failures to stop scan**. b. In the **Nonconsecutive 'single host' retry failures** box, enter the total number of nonconsecutive timeouts permitted from a single host. The default value is "unlimited."
Limit the number of nonconsecutive retry failures for any host...	a. Select **Nonconsecutive 'any host' retry failures to stop scan**. b. In the **Nonconsecutive 'any host' retry failures** box, enter the total number of nonconsecutive timeouts permitted from all hosts. The default value is 350.
Stop the scan if the target server does not respond to the first request...	Select **If first request fails, stop scan**.
Stop the scan if a specific response code is received...	If the HTTP response code that you want to use exists in the **RESPONSE CODES TO STOP SCAN IF RECEIVED** table, select the check box for the code. To edit an existing response code or change a single code in the table to a range of codes, see "Configuring response codes" below.

Configuring response codes

You can add response codes that are not included by default in the RESPONSE CODES TO STOP SCAN IF RECEIVED table in the ADVANCED scan settings view. Additionally, you can edit the default codes and add ranges of response codes.

Adding response codes

To add an HTTP response code or to create a range of codes:

1. Click **add operation** +.
   A row is added to the table.
2. Do one of the following:
   - To add one response code, enter the code in the **Start Response Code** box and the **End Response Code** box.
   - To specify a range of codes, enter the first code of the range in the **Start Response Code** box and the last code of the range in the **End Response Code** box.

     Note: A range that includes a subcode must be formatted as *<RangeCode>.<SubCode>*, such as `401.40104` found in the response `HTTP/1.1 401 SubCode=40104: Invalid authorization token audience.`

     Tip: When creating a range of codes, clicking **discard** — in the top right of the table discards the new range. Clicking **cancel** × to the right of new entry discards the new range.
3. Click **confirm** ✔.
   The code or range of codes is added to the table.

Editing existing response codes

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting a response code

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring session exclusions

The session exclusions settings enable you to configure exclusions for file extensions, hosts, URLs, request and response criteria, and MIME-types.

For information about exclusions for request and response criteria, see "Creating and managing basic exclusions" on page 199 and "Creating and managing basic exclusions in base settings" on page 411.

Session exclusions for scan settings, crawl settings, and audit Settings

The session exclusions configured for Scan Settings apply to both the crawl and audit phases of a scan. To specify exclusions for only the crawl or only the audit, use the Crawl Settings Session Exclusions or the Audit Settings Session Exclusions. You configure session exclusions in Crawl Settings and Audit Settings the same way as for Scan Settings. You cannot, however, edit any exclusions in Crawl Settings or Audit Settings that are configured in the Scan Settings.

Rejecting versus excluding

When configuring session exclusions for file extensions, hosts, and URLs, you can reject the session, exclude the session, or reject and exclude the session. Reject and Exclude are enabled by default. The following table describes how the sensor handles rejecting and excluding each session type.

Session Exclusion	Reject	Exclude
File extension exclusion	The sensor will not request files of the type you specify. **Note:** By default, most image, drawing, media, audio, video, and compressed file types are rejected.	The sensor will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.
Host or URL exclusion	The sensor will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any	During a crawl, the sensor will not examine the specified host or URL for links to other resources. During the audit portion of the

Session Exclusion	Reject	Exclude
	URL that deals with logging off the site, because you don't want to log out of the application before the scan is completed.	scan, the sensor will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, such as to check for broken links on URLs that you don't want to process, select the **Exclude** option, but do not select **Reject**.

Adding a file extension exclusion

To add an exclusion for file extensions:

1. Click **add operation**+ at the top of the EXCLUDED OR REJECTED FILE EXTENSIONS table.

   A row is added to the table.
2. In the **File Extension** box, type the extension to exclude.

   Important! The file extension cannot contain the following special characters:

   `- , # % & $ * : < > ? / \ -`

   It can contain a period (.) character only at the beginning of the extension, such as `.jpg`, although the period will not be visible in the table after saving. The file extension cannot contain multiple period (.) characters.
3. To not request files with this extension, select **reject**.
4. To request files with this extension but not attack them, select **exclude**.
5. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Adding a host exclusion

To add an exclusion for a host:

1. Click **add operation**+ at the top of the EXCLUDED OR REJECTED HOSTS table.
2. In the **Host** box, enter the fully qualified host name or a regular expression designed to match the targeted host to exclude.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. To not send any HTTP requests to the host, select **reject**.
4. To not examine the host for links to other resources, select **exclude**.
5. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Adding a URL exclusion

To add an exclusion for a URL:

1. Click **add operation**+ at the top of the EXCLUDED OR REJECTED URLS table.
2. In the **File Extension** box, enter the URL or a regular expression designed to match the targeted URL to exclude.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. To not send any HTTP requests to the URL, select **reject**.
4. To not examine the URL for links to other resources, select **exclude**.
5. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Adding a MIME-type exclusion

To add an exclusion for a MIME-type:

1. Click **add operation**+ at the top of the EXCLUDED MIME TYPES table.
2. In the **MIME Type** box, enter a MIME type.
3. Click **confirm** ✔.

Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

The session exclusion is added to the table.

Editing existing session exclusions

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

The edits are saved.

Deleting a session exclusion

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring HTTP parameters used for state

You can configure HTTP parameters used for state in the HTTP Parsing settings.

Understanding HTTP parameters used for state

If your application uses URL rewriting or post data techniques to maintain state within a website, then you must identify which parameters are used. For example, a PHP4 script can create a constant of the session ID named SID, which is available inside a session. By appending this to the end of a URL, the session ID becomes available to the next page. The actual URL might look something like the following:

```
.../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01
```

Because session IDs change with each connection, an HTTP request containing this URL would create an error when you tried to replay it. However, if you identify the parameter (`PHPSESSID` in this example), then the sensor will replace its assigned value with the new session ID obtained from the server each time the connection is made.

Similarly, some state management techniques use post data to pass information. For example, the HTTP message content may include `userid=slbhkelvbkl73dhj`. In this case, "`userid`" is the parameter you would identify.

Note: You need to identify parameters only when the application uses URL rewriting or posted data to manage state. It is not necessary when using cookies.

The sensor can identify potential parameters if they occur as posted data or if they exist within the query string of a URL. However, if your application embeds session data in the URL as extended path information, you must provide a regular expression to identify it. In the following example, "`1234567`" is the session information:

```
http://www.onlinestore.com/bikes/(1234567)/index.html
```

The regular expression for identifying the parameter would be: `/\([\w\d]+\)/`

Adding HTTP parameters used for state

To add an HTTP parameter that is used for state:

1. Under **HTTP PARAMETERS USED FOR STATE**, click **CREATE**.
   The MANAGE STATE HTTP PARAMETER dialog box appears.
2. In the **Expression Type** list, select the type parameter being created. Options are **Plain Text**, **Regular Expression**, and **Sub-parameter Text**.
3. In the **HTTP Parameter** box, enter plain text or a regular expression for the parameter.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
4. In the **Look for parameters in** list, select one or more places in the HTTP response to look for the parameter. Options are **HTTP query data**, **HTTP post data**, and **HTTP custom data**.
5. Click **OK**.
   The parameter is added to the table.

Editing an existing HTTP parameter

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

To edit the HTTP parameter expression type:

1. Select the check box for the rule to edit, and click **EDIT**.
   The MANAGE STATE HTTP PARAMETER dialog box appears.
2. In the **Expression Type** list, select the type parameter being created.
3. Click **OK**.

Deleting an HTTP parameter

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Enabling CSRF

If the site you are scanning includes cross-site request forgery (CSRF) tokens, you can enable CSRF in the HTTP PARSING section in the ADVANCED scan settings view.

Understanding CSRF

CSRF is a malicious exploit of a website where unauthorized commands are transmitted from a user's browser that the website trusts. CSRF exploits piggyback on the trust that a site has in a user's browser; using the fact that the user has already been authenticated by the site and the chain of trust is still open.

Example:

A user visits a bank, is authenticated, and a cookie is placed on the user's machine. After the user completes the banking transaction, he or she switches to another browser tab and continues a conversation on an enthusiast website devoted to the user's hobby. On the site, someone has posted a message that includes an HTML image element. The HTML image element includes a request to the user's bank to extract all of the cash from the account and deposit it into another account. Because the user has a cookie on his or her device that has not expired yet, the transaction is honored and all of the money in the account is withdrawn.

CSRF exploits often involve sites that rely on trust in a user's identity, often maintained through the use of a cookie. The user's browser is then tricked into sending HTTP requests to the target site in hopes that a trust between the user's browser and the target site still exists.

Using CRSF tokens

To stop cross-site request forgeries from occurring, common practice is to set up the server to generate requests that include a randomly generated parameter with a common name such as "`CSRFToken`". The token may be generated once per session or a new one generated for each request. If you use CSRF tokens in your code and enable CSRF in the ADVANCED scan settings view, the sensor will take this into consideration when crawling your site. Each time the sensor launches an attack, it will request the form again to acquire a new CSRF token. This adds significantly to the time it takes for the sensor to complete a scan, so do not enable CSRF if you are not using CSRF tokens on your site.

Enabling CSRF

To enable CSRF awareness for the scan:

- Select **Enable CSRF**.

Configuring URL expressions for determining state

If your application determines state from certain components in the URL path, you can configure plain text or Regular Expressions to identify those components in the HTTP PARSING section in the ADVANCED scan settings view.

Enabling URL expressions for determining state

To enable URL expressions:

- Under **URL PATH STATE**, select **Determine State From Path URL**.
  The expressions listed in the table will be used to determine state from the URL path.

Adding a URL expression

To add a URL expression:

1. Under **URL PATH STATE**, click **add operation** +.
   A row is added to the table.
2. In the **URL Expression** box, enter plain text or a regular expression for the expression to match.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.

3. Optionally, in the **Comments** box, enter a description for the expression.
4. Click **OK**.
   The expression is added to the table.

Editing existing URL expressions

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** .

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting a URL expression

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring response state rules

If your application maintains client state with bearer tokens, you can configure a rule that will identify the bearer token from the response and add it to the next request automatically. You can configure response state rules in the HTTP PARSING section in the ADVANCED scan settings view.

Note: The **Auto Response State Rules** option is enabled by default and provides several predefined rules for automatic detection of bearer tokens. You can enhance the automatic detection of bearer tokens by enabling response state rules and adding a rule as described in the following procedure.

Enabling response state rules

To enable response state rules:

- Under **RESPONSE STATE RULES**, select **Enable Response State Rules**.
  You can now create a response state rule or edit existing rules.

Adding a response state rule

To add a response state rule:

1. Under **RESPONSE STATE RULES**, click **CREATE**.
   The MANAGE RESPONSE STATE RULE dialog box appears.
2. In the **Rule Name** box, type a unique name for the rule.
3. Above the **SEARCH IN RESPONSE REGEX** table, click **add operation** +.
   A row is added to the table.
4. Do one of the following:
   - To use a predefined regular expression, place your cursor in the **Regex** box and select a regular expression statement from the list. You can then edit the selected statement.
   - To create a regular expression, in the **Regex** box enter a regular expression pattern for the text that will contain the token. For example:
     `"Token"\s*:\s*"([-a-zA-Z0-9._~+/]+?=*)"`

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
5. Click **confirm** ✔.
6. Above the **REPLACE IN REQUEST REGEX** table, click **add operation** +.
   A row is added to the table.
7. Do one of the following:
   - To use a predefined regular expression, place your cursor in the **Regex** box and select a regular expression statement from the list. You can then edit the selected statement.
   - To create a regular expression, in the **Regex** box enter a regular expression pattern for the text that will contain the token. For example:
     `"BearerToken"\s*:\s*"([-a-zA-Z0-9._~+/]+?=*)"`

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
8. Click **confirm** ✔.
9. Click **OK**.
   The rule is added as a row to the **RESPONSE STATE RULES** table.

Important! To avoid regular expressions that could drain your system resources and affect scan performance, do not use the following text strings when constructing your regular expressions:

- Any character with infinite numbers `".*"` or `".+"`
- Positive lookahead `"(?=…)"`

- Negative lookahead `"(?!...)"`
- Positive lookbehind `"(?<=…)"`
- Negative lookbehind `"(?<!...)"`

Editing an existing rule

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** .

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

To edit the regular expression patterns of a rule:

1. Select the check box for the rule to edit, and click **EDIT**.
   The MANAGE RESPONSE STATE RULE dialog box appears.
2. Edit the values as described in "Adding a response state rule" on the previous page.
3. Click **OK**.

Deleting a rule

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring HTTP parameters used for navigation

You can configure HTTP parameters used for navigation in the HTTP PARSING section in the ADVANCED scan settings view.

Understanding HTTP parameters used for navigation

Some sites contain only one directly accessible resource, and then rely on query strings to deliver the requested information, as in the following examples:

Example 1 - `http://www.anysite.com?Master.asp?Page=1`

Example 2 - `http://www.anysite.com?Master.asp?Page=2;`

Example 3 - `http://www.anysite.com?Master.asp?Page=13;Subpage=4`

Ordinarily, the sensor would assume that these three requests refer to identical resources and would conduct a vulnerability scan on only one of them. Therefore, if your target website employs this type of architecture, you must identify the specific resource parameters that are used.

Examples 1 and 2 contain one resource parameter: "Page." Example 3 contains two parameters: "Page" and "Subpage.

Adding HTTP parameters used for navigation

To add an HTTP parameter that is used for navigation:

1. Under **HTTP PARAMETERS USED FOR NAVIGATION**, click **add operation** +.
   A row is added to the table.
2. In the **Parameter** box, enter plain text for the parameter name.

   Tip: When adding a parameter, clicking **discard** — in the top right of the table discards the new row. Clicking **cancel** × to the right of new entry discards the new row.
3. Click **confirm** ✔.
   The code or range of codes is added to the table.

Editing an existing HTTP parameter

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting an HTTP parameter

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring advanced HTTP parsing

You can configure the character set used by your website and how to handle query parameters without values in the HTTP PARSING section in the ADVANCED scan settings view.

Specifying the default encoding

Most webpages contain information that tells the browser which character set to use. This is accomplished by using the Content-Type response header (or a META tag with an HTTP-EQUIV attribute) in the HEAD section of the HTML document.

For pages that do not announce their character set, you can specify which language family (and implied character set) the sensor should use.

To specify the character set to use:

- Under **ADVANCED HTTP PARSING**, select the appropriate character set from the **Default Encoding** list.

Handling query parameters without values

You can define how the sensor interprets query parameters without values. For example:

```
http://somehost?param
```

If the **Treat query parameter value as parameter name when only value is present** check box is selected, the sensor will interpret “param” to be a parameter named “param” with an empty value.

If the **Treat query parameter value as parameter name when only value is present** check box is not selected, the sensor will interpret “param” to be a nameless parameter with the value “param”.

This setting can influence the way the sensor calculates the hit count. (For more information, see the **Limit maximum single URL hits to** setting in "Configuring general settings" on page 224). This setting is useful for scenarios in which a URL contains an

anti-caching parameter. These often take the form of a numeric counter or timestamp. For example, the following parameters are numeric counters:

- `http://somehost?1234567`
- `http://somehost?1234568`

In such cases, the value is changing for each request. If the value is treated as the parameter name, and the **Include parameters in hit count** setting in General Settings is selected, the crawl count may inflate artificially, thus increasing the scan time. In these cases, clearing the **Treat query parameter value as parameter name when only value is present** check box will prevent these counters from contributing to the hit count and produce a more reasonable scan time.

Configuring custom parameters

Custom parameters are used to accommodate sites that use URL rewriting techniques and/or Representation State Transfer (REST) web services technologies. You can write rules for these custom parameters, or you can import rules from a common configuration file written in Web Application Description Language (WADL).

About URL rewriting

Many dynamic sites use URL rewriting because static URLs are easier for users to remember and are easier for search engines to index the site. For example, an HTTP request such as

`http://www.pets.com/ShowProduct/7`

is sent to the server's rewrite module, which converts the URL to the following:

`http://www.pets.com/ShowProduct.php?product_id=7`

In this example, the URL causes the server to execute the PHP script "ShowProduct" and display the information for product number `7`.

When the sensor scans a page, it must be able to determine which elements are variables so that its attack agents can thoroughly check for vulnerabilities. To enable this, you must define rules that identify these elements. You can do so using a proprietary ScanCentral DAST syntax.

Examples:

HTML: User 1 details
Rule: /someDetails/{username}/

HTML: User 1 details
Rule: /TwoParameters/Details/{username}/{parameter2}

HTML: User 1 details
Rule: /{parameter2}/PreFixParameter/Details/{username}

About RESTful services

A RESTful web service (also called a RESTful web API) is a simple web service implemented using HTTP and the principles of REST. It has gained widespread acceptance across the web as a simpler alternative to web services based on SOAP and Web Services Description Language (WSDL).

The following request adds a name to a file using an HTTP query string:

```
GET /adduser?name=Robert HTTP/1.1
```

This same function could be achieved by using the following method with a web service:

```
POST /users HTTP/1.1 Host: myserver
 Content-Type: application/xml
 <?xml version="1.0"?>
 <user>
   <name>Robert</name>
 </user>
```

Note that the parameter names and values have been moved from the request URI and now appear as XML tags in the request body.

In the case of both URL rewriting and RESTful web services, you must create rules that instruct Fortify WebInspect how to create the appropriate requests.

Creating a custom parameter rule

To create a custom parameter rule:

1. Under **CUSTOM PARAMETERS**, click **add operation**+.
   A row is added to the table.
2. In the **Expression** box, enter rule. See "Path matrix parameters" on page 251 for guidelines and examples.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.

   Tip: When adding a parameter, clicking **discard**− in the top right of the table discards the new row. Clicking **cancel**× to the right of new entry discards the new row.
3. Click **confirm**✓.
   The rule is added to the table. The **Enabled** check box is selected by default.

Disabling and enabling a rule

To disable or enable a parameter rule:

1. Click **edit** for the row to disable or enable.
2. Do one of the following:
   - To enable the rule, select **Enabled**.
   - To disable the rule, clear the **Enabled** check box.
3. Click **confirm**.

Editing an existing rule

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm**.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting an existing rule

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Enabling automatic seeding of rules that were not used during scan

The most reliable rules for custom parameters are those deduced from a WADL file or created by developers of the website. If a rule is not invoked during a scan (because the rule doesn't match any URL), then the sensor can programmatically assume that a valid portion of the site has not been attacked. Therefore, if you select this option, the sensor will create sessions to exercise these unused rules in an effort to expand the attack surface.

Double-encoding URL parameters

Double-encoding is an attack technique that encodes user request parameters twice in hexadecimal format in an attempt to bypass security controls or cause unexpected behavior from the application. For example, a cross-site scripting (XSS) attack might normally appear as:

```
<script>alert('FOO')</script>
```

This malicious code could be inserted into a vulnerable application, resulting in an alert window with the message “FOO.” However, the web application can have a filter that prohibits characters such as < (less than) > (greater than) and / (forward slash), since they are used to perform web application attacks. The attacker could attempt to circumvent this safeguard by using a "double encoding" technique to exploit the client’s session. The encoding process for this JavaScript is:

Char	Hex encode	Encoded % Sign	Double encoded result
<	%3C	%25	%253C
/	%2F	%25	%252F
>	%3E	%25	%253E

Finally, the malicious code, double-encoded, is:

```
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
```

If you select this option, the sensor will create double-encoded URL parameters (instead of single-encoded parameters) and submit them as part of the attack sequence. This is recommended when the web server uses, for example, Apache mod-rewrite plus PHP or Java URL Rewrite Filter 3.2.0.

Path matrix parameters

There are three ways rules can be created in the system. Rules may be:

- Entered manually
- Generated from a WADL file specified by the user or received through Fortify DAST Agent
- Imported from a flat file containing a list of rules

When entering rules manually, you specify the path segments of a URL that should be treated as parameters.

The rules use special characters to designate parts of the actual URL that contain parameters. If a URL matches a rule, the sensor parses the parameters and attacks them. Notable components of a rule are:

- Path (`gp/c/{book_name}/`)
- Query (anything that follows "`?`")
- Fragment (anything that follows "`#`")

Definition of path segment

A path segment starts with '`/`' characters and is terminated either by another '`/`' character or by end of line. To illustrate, path "`/a`" has one segment whereas path "`/a/`" has two segments (the first containing the string "`a`" and the second being empty. Note that paths "`/a`" and "`/a/`" are not equal. When attempting to determine if a URL matches a rule, empty segments are considered.

Special elements for rules

A rule may contain the special elements described in the following table.

Element	Description
*	Asterisk. May appear in production defined below; presence in non-path productions means that this part of the URL will not participate in matching (or, in other words, will match anything).
{ }	Group; a named parameter that may appear within the path of the rule. The content has no special meaning and is used during reporting as the name of the attacked parameter. The character set allowed within the delimiting brackets that designate a group `{ }` is defined in RFC 3986 as `*pchar`: `pchar = unreserved / pct-encoded / sub-delims / ":" / "@"` `pct-encoded = "%" HEXDIG HEXDIG` `unreserved = ALPHA DIGIT - . _ ~` `reserved = gen-delims / sub-delims` `gen-delims = : / ? # [ ] @"` `sub-delims = ! $ & ' ( ) * + , ; =` A group's content cannot include the "open bracket" and "close bracket" characters, unless escaped as pct-encoded element.

The rules for placing `*` out of path are described below. Within a path segment, any amount of `*` and `{}` groups can be placed, provided they're interleaved with plain text. For example:

Valid rule: `/gp/c/*={param}`
Invalid rule: `/gp/c/*{}`

Rules with segments having `**`, `*{}`, `{}*` or `{}{}` entries are invalid.

For a rule to match a URL, all components of the rule should match corresponding components of the crawled URL. Path comparison is done segment-wise, with `*` and `{}` groups matching any number of characters (including zero characters), plain text elements matching corresponding plain text elements of the path segment of the URL. So, for example:

`/gp/c/{book_name}` is a match for these URLs:

- `http://www.amazon.com:8080/gp/c/Moby_Dick`
- `http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&price=0`
- `https://www.amazon.com/gp/c/Hobbit`

But it is not a match for any of these:

- `http://www.amazon.com /gp/c/Moby_Dick/` (no match because of trailing slash)
- `http://www.amazon.com/gp/c/Sex_and_the_City/Horror` (no match because it has a different number of segments)

The sensor will treat elements of path segments matched by `{…}` groups in the rule URL as parameters, similar to those found in a query. Moreover, query parameters of crawled URLs matched by rule will be attacked along with parameters within the URL's path. In the following example of a matched URL, the sensor would conduct attacks on the format and price parameters and on the third segment of the path (Singularity_Sky):

`http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&:price=0`

Asterisk placeholder

The "`*`" placeholder may appear in the following productions and subproductions of the URL:

- Path – cannot be matched as a whole, since `*` in path matches a single segment or less.
  - Path segments – as in `/gp/*/{param}`, which will match URLs with schema HTTP, hostname www.amazon.com, path containing three segments (first is exactly "gp", second is any segment, and the third segment will be treated as parameter and won't participate in matching).
  - Part of path segment – as in `/gp/ref=*`, which will match URLs with path containing two segments (first is exactly "gp", second containing any string with prefix "ref=").
- Query – as in `/gp/c/{param}?*`, which matches any URL with path of three segments (first segment is "gp", second segment is "c" and third segment being a parameter, so it won't participate in matching); this URL also MUST contain a query string of arbitrary structure. Note the difference between rules `/gp/c/{param}` and `/gp/c/{param}?*`. The first rule will match URL http://www.amazon.com/gp/c/Three_Little_Blind_Mice, while the second will not.

  - Key-value pair of query – as in `/gp/c/{param}?format=*` which will match URL only if query string has exactly one key-value pair, with key name being “format.”
  - Key-value pair of query – as in `/gp/c/{param}?*=pdf` which will match URL only if query string has exactly one key-value pair, with value being “pdf.”
- Fragment – as in case `/gp/c/{param}#*` which matches any URL with fragment part being present

Benefit of using placeholders

The main benefit of using placeholders is that it enables you to create rules that combine matrix parameters and URL path-based parameters within single rule. For relevant URL

```
http://www.amazon.com/gp/color;foreground=green;background=black/something?for
mat=dvi
```

the following rule will allow attacks on all parameters

```
gp/*/{param}
```

with the matrix parameter segment being ignored by `*` placeholder within second segment of the path, but recognized by the sensor and attacked properly.

Multiple rules matching a URL

In the case of multiple rules matching a given URL, there are two options:

- Stop iterating over the rules once a match is found and so use only the first rule.
- Iterate over all of the rules and collect all custom parameters that match.

For instance, for the following URL

```
http://mySite.com/store/books/Areopagitica/32/1
```

the following rules both match

- `*/books/{booktitle}/32/{paragraph}`
- `store/*/Areopagitica/{page}/{paragraph}`

The sensor will try to collect parameters from both rules to ensure the greatest attack coverage, so all three segments (“Areopagitica”, “32” and “1” in the example above) will be attacked.

Configuring filters

Use the filters settings to add search-and-replace rules for HTTP requests and responses. This feature is used most often to avoid the disclosure of sensitive data such as credit card numbers, employee names, or social security numbers. It is a means of disguising information that you do not want to be viewed by persons who use ScanCentral DAST or those who have access to the raw data or generated reports.

Adding an HTTP request filter

To add an HTTP request filter:

1. Under **FILTER HTTP REQUEST CONTENT**, click **CREATE**.
   The HTTP CONTENT FILTER dialog box appears.
2. Continue with "Configuring HTTP content filter settings" below.

Adding an HTTP response filter

To add an HTTP response filter:

1. Under **FILTER HTTP REQUEST CONTENT**, click **CREATE**.
   The HTTP CONTENT FILTER dialog box appears.
2. Continue with "Configuring HTTP content filter settings" below.

Configuring HTTP content filter settings

To configure the settings for the HTTP request or response filter:

1. On the HTTP CONTENT FILTER dialog, in the **Search for text** box, type (or paste) the string you want to locate (or enter a regular expression that describes the string).

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.

2. In the **Search for text In** box, select the section of the request or response you want to search for the filter pattern. The options are:
   - **All** – Search the entire request or response.
   - **Headers** – Search each header individually. Some headers, such as Set-Cookie and HTTP Version headers, are not searched.

     Note: To ensure that all headers are searched, select Prefix.

   - **Post Data** – For requests only, search all of the HTTP message body data.
   - **Body** – Search all of the HTTP message body data.
   - **Prefix** – Simultaneously search everything that is in the request or status line, all headers, and the empty line prior to the body.
3. For case-sensitive searches, select the **Case sensitive match** check box.
4. Click **OK**.
   The filter is added as a row in the FILTER HTTP REQUEST CONTENT or FILTER HTTP RESPONSE CONTENT table.

Editing an existing filter

To edit an existing HTTP request or response filter:

1. Select the check box for the filter to edit, and click **EDIT**.
   The HTTP CONTENT FILTER dialog box appears.
2. Edit the values as described in "Configuring HTTP content filter settings" on the previous page.
3. Click **OK**.

Enabling or disabling an existing filter

When you create a filter, it is enabled by default. You can edit the filter to disable it. Disabled filters are not used during a scan. Afterward, you can edit the filter to enable it once again. The filter table indicates whether a filter is enabled or disabled.

To disable or enable an existing HTTP request or response filter:

1. Select the check box for the filter to disable or enable, and click **EDIT**.
   The HTTP CONTENT FILTER dialog box appears.
2. Do one of the following:
   - To disable the filter, slide the **Enabled** toggle to **Disabled**.
   - To enable the filter, slide the **Disabled** toggle to **Enabled**.
3. Click **OK**.

Deleting a filter

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring custom cookies and headers

You can configure settings for standard header parameters as well as settings to append custom cookies and custom headers.

Configuring standard header parameters

The options for configuring standard headers are described in the following table.

Option	Description
Include 'referer' in HTTP request headers	Select this check box to include referer headers in HTTP requests from the sensor. The Referer request-header field allows the client to specify, for the server's benefit, the address (URI) of the resource from which the Request-URI was obtained.
Include 'host' in HTTP request headers	Select this check box to include host headers with HTTP requests from the sensor. The Host request-header field specifies the Internet host and port number of the resource being requested, as obtained from the original URI given by the user or referring resource (generally an HTTP URL).

Appending custom cookies

You can specify data that will be sent with the Cookie header in HTTP requests sent by the sensor to the server when conducting a vulnerability scan.

The default custom cookie used to flag the scan traffic is:

```
CustomCookie=WebInspect;path=/
```

Tip: The equal sign (=) is the delimiter between the name `CustomCookie` and the value `WebInspect`. The `path=/` specifies that the cookie applies to all requests. The custom cookie named `WebInspect` has special processing. Other custom cookies with different names are treated as standard cookies.

Adding a custom cookie

To add a custom cookie:

1. Under APPEND CUSTOM COOKIES, click **add operation** +.
   A row is added to the table.
2. In the **Custom Cookie** box, enter the cookie using the format *<name>=<value>*.

   For example, if you enter

   ```
   CustomCookie=ScanEngine
   ```

then each HTTP-Request will contain the following header:
`Cookie: CustomCookie=ScanEngine`

Tip: If you create a custom cookie and specify the `path=/xyz`, then the custom cookie would only appear in requests starting with "`/xyz`".

3. Click **confirm** ✔.

Appending custom headers

Use this section to add, edit, or delete headers that will be included with each audit the sensor performs. For example, you could add a header such as "Alert: You are being attacked by Consultant ABC" that would be included with every request sent to your company's server when the sensor is auditing that site. You can add multiple custom headers.

The default custom headers are described in the following table.

Header	Description
Accept: */*	Any encoding or file type is acceptable to the crawler.
Pragma: no-cache	This forces a fresh response; cached or proxied data is not acceptable.
Accept-Encoding: gzip, deflate	The client requests that the server uses one of the specified encoding methods.

Adding a custom header

To add a custom header:

1. Under APPEND CUSTOM HEADERS, click **add operation** +.
   A row is added to the table.
2. In the **Custom Header** box, enter the header using the format *<name>: <value>*.
3. Click **OK**.

Editing an existing custom cookie or custom header

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

Tip: Clicking **cancel** ↺ in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

The edits are saved.

Deleting a custom cookie or custom header

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring multi-user site authentication

Applications that allow only a single active login session per user prevent multi-threaded scanning. With multiple logins, the threads invalidate each other's state, resulting in slow scan times.

A solution to this problem is to convert the recorded credentials in a login macro to parameters and use multiple login accounts with the same application privileges. You can use the Multi-User Login option in the AUTHENTICATION section in the ADVANCED scan settings view to parameterize the username and password in a login macro, and define multiple username and password pairs to use in a scan. You can also parameterize the phone number, email, and email password if two-factor authentication is required.

This approach allows the scan to run across multiple threads. Each thread has a different login session, resulting in faster scan times.

Before you begin

You must use a parameterized login macro to configure a multi-user login scan. For more information, see the "Working with Parameters" topic in the Event-based Web Macro Recorder chapter of the *OpenText™ Fortify DAST Tools Guide*.

Known limitations

The following known limitations apply to the multi-user login feature:

- When using this feature, the Fortify DAST sensor does not detect several login-related Securebase checks.
- This feature currently supports only shared requestor threads. Using default scan settings with separate crawl and audit threads is not supported. For more information,

see "Configuring requestor settings" on page 231.

- The scan does not distribute the work equally among the multiple users logged in. For example, one configured user might use up to 75% of the scan activities while all other users are allocated to the remaining 25% of scan activities.

Enabling multi-user login

To enable multi-user login for the scan:

- In the AUTHENTICATION section in the ADVANCED scan settings view, select **Use Multi-User Login**.
  An area for user login credentials appears. Continue with "Adding user login credentials" below.

Adding user login credentials

To add user login credentials:

1. Click **CREATE**.
   The MULTI USER LOGIN CREDENTIALS dialog box opens.
2. Enter credentials for one user according to the following table.

For this credential box...	Enter this...
Username	Username
Password	Corresponding password for the username
Phone Number	Corresponding phone number for the username (to receive SMS responses)
Email	Corresponding email address for the username (to receive email responses)
Email Password	Password for the email address (to receive email responses)

Note: Phone Number, Email, and Email Passwords are used for two-factor authentication. For more information, see "Working with two-factor authentication" on page 425.

3. Click **OK**.
   The user credentials are added to the login credentials table.

Repeat this procedure to add additional user login credentials.

Editing user login credentials

To edit a row in the table:

1. Select the check box for credentials you want to edit.
   Click **EDIT**.
   The MULTI USER LOGIN CREDENTIALS dialog box opens.
2. Edit the credentials for the user as described in "Adding user login credentials" on the previous page.
3. Click **OK**.
   The user credentials in the login credentials table are updated.

Deleting user login credentials

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring file-not-found settings

You can use HTTP response codes and custom signatures to determine whether a file is not found. You can also allow the sensor to automatically detect files not found.

Using HTTP response codes to determine FNF

You can use HTTP response codes to specify response codes that should never be treated as a file-not-found response and response codes that should always be treated as a file-not-found response.

To use HTTP response codes:

- Slide the **Determine File Not Found (FNF) using HTTP response codes** option to enabled.
  The sensor uses the default response codes. You can also add response codes as described in "Adding a response code for never FNF" on the next page and "Adding a response code for always FNF" on the next page.

Adding a response code for never FNF

To add a response code or range of codes that should never be treated as FNF:

1. Under **FORCED VALID RESPONSE CODES (NEVER A FNF)**, click **add operation** +.
   A row is added to the table.
2. Do one of the following:
   - To add a single response code, enter the code in the **Start Response Code** box and the **End Response Code** box.
   - To add a range of response codes, enter the starting code in the **Start Response Code** box and enter the ending code in the **End Response Code** box.
3. Click **confirm** ✔.

Adding a response code for always FNF

To add a response code or range of codes that should always be treated as FNF:

1. Under **FORCED FNF RESPONSE CODES (ALWAYS A FNF)**, click **add operation** +.
   A row is added to the table.
2. Do one of the following:
   - To add a single response code, enter the code in the **Start Response Code** box and the **End Response Code** box.
   - To add a range of response codes, enter the starting code in the **Start Response Code** box and enter the ending code in the **End Response Code** box.
3. Click **confirm** ✔.

Editing a response code

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Using custom 404 page notifications

If your company has configured a different page to display when a 404 error occurs, you can use custom signatures to determine whether a file is not found.

To use custom signatures:

1. Slide the **Determine FNF from custom supplied signature** option to enabled.
   The sensor uses the default custom signatures.
2. Optionally, you can add a custom signature as follows:
   a. Click **CREATE**.
      The FILE NOT FOUND CUSTOM SIGNATURE dialog box appears.
   b. In the **Expression Type** list, select one of the following. Options are Plain Text, Regular Expression, and SPI Regular Expression.

      Tip: You can access the Regex Editor from the **Tools menu** ⋮.

   c. In the **Custom Expression** box, enter either plain text or a regular expression to match
   d. Click **OK**.
      The signature is added as a row to the table.

Editing an existing signature

To edit a custom signature:

1. Select the check box for the signature to edit, and click **EDIT**.
   The FILE NOT FOUND CUSTOM SIGNATURE dialog box appears.
2. Edit the values.
3. Click **OK**.

Deleting a signature

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Using auto detection of FNF

Some websites do not return a status "404 Not Found" when a client requests a resource that does not exist. Instead, they may return a status "200 OK" but the response contains

a message that the file cannot be found, or they might redirect to a home page or login page.

If you want the sensor to detect these "custom" file-not-found pages, slide the **Auto detect FNF page** option to enabled.

The sensor attempts to detect custom file-not-found pages by sending requests for resources that cannot possibly exist on the server. It then compares each response and measures the amount of text that differs between the responses. For example, most messages of this type have the same content (such as "Sorry, the page you requested was not found"), with the possible exception being the name of the requested resource. If you enable the **Auto detect FNF page** option, you can specify what percentage of the response content must be the same in the **Match FNF page with (%) certainty** box. The default is 90 percent.

Configuring crawl link parsing

The sensor follows all hyperlinks defined by HTML (using the `<a href>` tag) and those defined by scripts (JavaScript and VBScript). However, you may encounter other communications protocols that use a different syntax for specifying links. To accommodate this possibility, you can use the specialized link parsing feature and regular expressions to identify links that you want the sensor to follow. These are called special link patterns.

Adding a specialized link parsing pattern

To add a specialized link identifier:

1. Click **CREATE**.
   The SPECIAL LINK PARSING PATTERN dialog box appears.
2. In the **Specialized link pattern** box, enter a regular expression designed to identify the link.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. (Optional) Enter a description of the link in the **Comments** box.
4. Click **OK**.
   The rule is added as a row to the **Specialized Link Parsing** table.

Editing an existing pattern

To edit an existing pattern:

1. Select the check box for the pattern to edit, and click **EDIT**.
   The SPECIAL LINK PARSING PATTERN dialog box appears.

2. Edit the values as described in "Adding a specialized link parsing pattern" on the previous page.
3. Click **OK**.

Deleting a pattern

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring crawl link sources

The sensor crawler sends a request to a start URL and recursively parses links (URLs) from the response content. These links are added to a work queue and the crawler iterates through the queue until it is empty. The techniques used to extract the link information from the HTTP responses are collectively referred to as 'link parsing.' There are two choices for how the crawler performs link parsing: Pattern-based and DOM-based.

Pattern-based parsing

Pattern-based link parsing uses a combination of text searching and pattern matching to find URLs. These URLs include the ordinary content that is rendered by a browser, such as `<A>` elements, as well as invisible text that may reveal additional site structure.

This is a more aggressive approach to crawling the website and can increase the amount of time it takes to conduct a scan. The aggressive behavior can cause the crawler to create many extra links which are not representative of actual site content. For these situations, DOM-based parsing should expose the site's URL content with fewer false positives.

Note: All of the DOM-based Parsing techniques for finding links are used when Pattern-based Parsing is selected. Pattern-based Parsing, however, is not capable of computing the metadata for the link source. DOM-based Parsing is capable of computing this information and thus provides more intelligent parsing. DOM-based Parsing also provides more control over which parsing techniques are used.

DOM-based parsing

The Document Object Model (DOM) is a programming concept that provides a logical structure for defining and building HTML and XML documents, navigating their structure, and editing their elements and content.

A graphical representation of an HTML page rendered as DOM would resemble an upside-down tree: starting with the HTML node, then branching out in a tree structure to include the tags, sub-tags, and content. This structure is called a DOM tree.

Using DOM-based parsing, the sensor parses HTML pages into a DOM tree and uses the detailed parsed structure to identify the sources of hyperlinks with higher fidelity and greater confidence. DOM-based parsing can reduce false positives and may also reduce the degree of 'aggressive link discovery.'

On some sites, the crawler iteratively requests bad links and the resulting responses echo those links back in the response content, sometimes adding extra text that compounds the problem. These repeated cycles of 'bad links in and bad links out' can cause scans to run for a long time or, in rare cases, forever. DOM-based parsing and careful selection of link sources provide a mechanism for limiting this runaway scan behavior. Web applications vary in structure and content, and some experimentation may be required to get optimal link source configurations.

To refine DOM-based Parsing, select the options you want to use for finding links. Clearing options that may not be a concern for your site may decrease the amount of time it takes to complete the scan. For a more thorough scan, however, select all options or use Pattern-based Parsing. The DOM-based Parsing techniques are described in the following table. For more information, see "Limitations of link source settings" on page 272.

Option	Description
Include Comment Links (Aggressive)	Programmers may leave notes to themselves that include links inside HTML comments that are not visible on the site, but may be discovered by an attacker. Use this option to find links inside HTML comments. The sensor will find more links, but these may not always be valid URLs, causing the crawler to try to access content that does not exist. Also, the same link can be on every page and those links can be relative, which can exponentially increase the URL count and lengthen the scan time.
Include Conditional Comment Links	A conditional comment link occurs when the HTML on the page is conditionally included or excluded depending on the user agent (browser type and version) making the request. **Regular comment example:** `<!—hidden.txt -->` **Conditional comment example:** `<!--[if lt IE9]>` `<script src="//www.somesite.com/static/v/all/js/html5sh.js"></script>` `<link rel="stylesheet" type"text/css"`

Option	Description
	`href='//www.somesite.com/static/v/fn-hp/css/IE8.css'>` `<![endif]-->` The sensor emulates browser behaviors in evaluating HTML code and processes the DOM differently depending on the user agent. A link found in a comment by one user agent is a normal HTML link for other user agents. Use this option to find conditional links that are inside HTML commands, such as those commented out based on browser version. These conditional statements may also contain script includes that need to be executed when script parsing is enabled. Crawling these links will be more thorough, but can increase the scan time. Additionally, such comments may be out of date and pointless to crawl.
Include Plain Text Links	Plain text in a .txt file or a paragraph inside HTML code can be formatted as a URL, such as `http://www.something.com/mypage.html`. However, because this is only text and not a true link, the browser would not render it as a link, and the text would not be functionally part of the page. For example, the content may be part of a page that describes how to code in HTML using fake syntax that is not meant to be clicked by users. Use this option for the sensor to parse these text links and queue them for a crawl. Also, using smart pattern matches, the sensor can identify common file extensions, such as .css, .js, .bmp, .png, .jpg, .html, etc., and add these files to the crawl queue. Auditing these files that are referenced in plain text can produce false positives.
Include Links in Static Script Blocks	Use this option for the sensor to examine inside the opening and closing script tags for text that looks like links. Valid links may be found inside these script blocks, but developers may also leave comments that include text resembling links inside the opening and closing script tags. For example: `<script type="text/javascript">` `// go to http://www.foo.com/blah.html for help` `var url = "http:www.foo.com/xyz/" + path + "?help"` `</script>` Additionally, JavaScript code inside these tags can be handled by the JavaScript execution engine during the scan. However,

Option	Description
	searching for static links in a line of code that sets a variable, such as the “var url” in the example above, can create problems when those partial paths are added to the queue for crawling. If the variable includes a relative link with a common extension, such as “foo.html”, the crawler will append the extension to the end of every page that includes the line of code. This can produce unusable URLs and may create false positives.
Include URLs Embedded in URLs	Use this option for the sensor to parse any text that is inside an href attribute and add it to the crawl queue. The following is an example of a URL embedded in a URL: `<a href="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />` On some sites, however, file not found pages return the URL in a form action tag and append the URL to the original URL as follows: `<form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />` The sensor will then request the form action, and receive another file not found response, again with the URL appended in a form action, as shown below: `<form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />` On such a site, these URLs will continue to produce file not found responses that add more URLs to the crawl queue, creating an infinite crawl loop. To avoid adding this type of URL to the crawl queue, do not use this option.
Allow Un-rooted URLs (ex:	This option modifies the behavior of the previous five options.

Option	Description
somewhere/foo.php)	Some URLs do not include the specific scheme, such as http, and are not fully qualified domain names. These URLs, which may resemble `xyz.html`, are considered unanchored or "un-rooted." The assumption is that the un-rooted URL is relative to the request. For example, the non-fully qualified URL `<a href='foo.html' />` does not include a scheme. This URL uses the scheme of the context URL. If an HTTPS page requested to get the content, then HTTPS would be prepended to the URL. Use this option to treat un-rooted URLs as links when parsing. If this option is selected, the scan will be more thorough and more aggressive, but may take considerably longer to complete. **URL Samples and Parsing Results** The following samples describe various URLs and how they are parsed during a crawl. **A Normal URL** The URL in the following request includes a forward (or anchor) slash. Request from `http://www.foo.com/x/y/z/` For `<a href='/bar.html' />` Results in a link to `http://www.foo.com/bar.html`. **Simple Un-rooted URL** The URL in the following request is un-rooted because it does not include a forward slash. Request from `http://www.foo.com/` For `<a href='bar.html' />` Results in a link to `http://www.foo.com/bar.html`. **Long Un-rooted URL** The following request shows a long, un-rooted URL. Request from `http://www.foo.com/x/y/z/` For `<a href='bar.html' />` Results in a link to `http://www.foo.com/x/y/z/bar.html`. **Comments in Code** You may include comments, such as `<!-- baz_ads.js -->`, in your

Option	Description
	code before a script include. The following request shows how this comment is interpreted during an aggressive crawl. Request from `http://www.foo.com/x/y/z/` For `<!-- baz_ads.js -->` Results in a link to `http://www.foo.com/x/y/z/baz_ads.js` If you include this comment on your master page, then during an aggressive scan, the comment will be discovered on many, if not all, page responses in the site. This configuration can cause runaway scans. The comment `<!-- baz_ads.js -->` on the master page results in multiple links: `http://www.foo.com/baz_ads.js` `http://www.foo.com/x/baz_ads.js` `http://www.foo.com/x/y/baz_ads.js` `http://www.foo.com/x/y/z/baz_ads.js` And so on for all pages in the site.

Form actions, script includes, and stylesheets

Some link types–such as form actions, script includes, and stylesheets–are special and are treated differently than other links. On some sites, it may not be necessary to crawl and parse these links. However, if you want an aggressive scan that attempts to crawl and parse everything, the following options will help accomplish this goal. For more information, see "Limitations of link source settings" on page 272.

Note: You can also allow un-rooted URLs for each of these options. See “Allow Un-rooted URLs” in this topic.

Option	Description
Crawl Form Action Links	When the sensor encounters HTML forms during the crawl, it creates variations on the inputs that a user can make and submits the forms as requests to solicit more site content. For example, for forms with a POST method, the sensor can use a GET instead and possibly reveal information. In addition to this type of crawling, use this option for the sensor to treat form targets as normal links.
Crawl Script	A script include imports JavaScript from a .js file and processes

Option	Description
Include Links	it on the current page. Use this option for the sensor to crawl the .js file as a link.
Crawl Stylesheet Links	A stylesheet link imports the style definitions from a .css file and renders them on the current page. Use this option for the sensor to crawl the .css file as a link.

Miscellaneous options

The following additional options may help improve link parsing for your site. For more information, see "Limitations of link source settings" on the next page.

Option	Description
Crawl Links on FNF Pages	If you select this option, the sensor will look for and crawl links on responses that are marked as “file not found.” **Note:** This option is selected by default when the Scan Mode is set to **Crawl Only** or **Crawl and Audit**. The option is not available when the Scan Mode is set to **Audit Only**.
Suppress URLs with Repeated Path Segments	Many sites have text that resembles relative paths that become unusable URLs after the sensor parses them and appends them to the URL being crawled. These occurrences can result in a runaway scan if paths are continuously appended, such as `/foo/bar/foo/bar/`. This setting helps reduce such occurrences and is enabled by default. With the setting **enabled**, the options are: **1** – Detect a single sub-folder repeated anywhere in the URL and reject the URL if there is a match. For example, `/foo/baz/bar/foo/` will match because “`/foo/`” is repeated. The repeat does not have to occur adjacently. **2** – Detect two (or more) pairs of adjacent sub-folders and reject the URL if there is a match. For example, `/foo/bar/baz/foo/bar/` will match because “`/foo/bar/`” is repeated. **3** – Detect two (or more) sets of three adjacent sub-folders and reject the URL if there is a match.

Option	Description
	4 – Detect two (or more) sets of four adjacent sub-folders and reject the URL if there is a match. **5** – Detect two (or more) sets of five adjacent sub-folders and reject the URL if there is a match. If the setting is **disabled**, repeating sub-folders are not detected and no URLs are rejected due to matches.

Limitations of link source settings

Clearing a link source check box prevents the crawler from processing that specific kind of link when it is found using static parsing. However, these links can be found in many other ways. For example, clearing the **Crawl Stylesheet Links** option does not control path truncation nor suppress .css file requests made by the script engine. Clearing this setting only prevents static link parsing of the .css response from the server. Similarly, clearing the **Crawl Script Include Links** option does not suppress .js, AJAX, frameIncludes, or any other file request made by the script engine. Therefore, clearing a link source check box is not a universal filter for that type of link source.

The goal for clearing a check box is to prevent potentially large volumes of bad links from cluttering the crawl and resulting in extremely long scan times.

Configuring crawl session exclusions

The session exclusions configured for Crawl Settings apply to the crawl phase of a scan. You configure session exclusions in Crawl Settings the same way as for Scan Settings. You cannot, however, edit any exclusions in Crawl Settings that are configured in the Scan Settings.

Rejecting versus excluding

When configuring session exclusions for file extensions, hosts, and URLs, you can reject the session, exclude the session, or reject and exclude the session. Reject and Exclude are enabled by default. The following table describes how the sensor handles rejecting and excluding each session type.

Session Exclusion	Reject	Exclude
File extension exclusion	The sensor will not request files of the type you specify.	The sensor will request the files, but will not attack them (during

Session Exclusion	Reject	Exclude
	Note: By default, most image, drawing, media, audio, video, and compressed file types are rejected.	an audit) and will not examine them for links to other resources.
Host or URL exclusion	The sensor will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, because you don't want to log out of the application before the scan is completed.	During a crawl, the sensor will not examine the specified host or URL for links to other resources. During the audit portion of the scan, the sensor will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, such as to check for broken links on URLs that you don't want to process, select the **Exclude** option, but do not select **Reject**.

Adding a file extension exclusion

To add an exclusion for file extensions:

1. Click **add operation**+ at the top of the EXCLUDED OR REJECTED FILE EXTENSIONS table.
   A row is added to the table.
2. In the **File Extension** box, type the extension to exclude.

   Important! The file extension cannot contain the following special characters:

   `- , # % & $ * : < > ? / \ -`

   It can contain a period (.) character only at the beginning of the extension, such as `.jpg`, although the period will not be visible in the table after saving. The file extension cannot contain multiple period (.) characters.
3. To not request files with this extension, select **reject**.
4. To request files with this extension but not attack them, select **exclude**.
5. Click **confirm** ✔.

Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

The session exclusion is added to the table.

Adding a host exclusion

To add an exclusion for a host:

1. Click **add operation**+ at the top of the EXCLUDED OR REJECTED HOSTS table.
2. In the **Host** box, enter the fully qualified host name or a regular expression designed to match the targeted host to exclude.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. To not send any HTTP requests to the host, select **reject**.
4. To not examine the host for links to other resources, select **exclude**.
5. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Adding a URL exclusion

To add an exclusion for a URL:

1. Click **add operation**+ at the top of the EXCLUDED OR REJECTED URLS table.
2. In the **File Extension** box, enter the URL or a regular expression designed to match the targeted URL to exclude.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. To not send any HTTP requests to the URL, select **reject**.
4. To not examine the URL for links to other resources, select **exclude**.
5. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Adding a MIME-type exclusion

To add an exclusion for a MIME-type:

1. Click **add operation** + at the top of the EXCLUDED MIME TYPES table.
2. In the **MIME Type** box, enter a MIME type.
3. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Editing existing session exclusions

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting a session exclusion

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring audit session exclusions

The session exclusions configured for Audit Settings apply to the audit phase of a scan. You configure session exclusions in Audit Settings the same way as for Scan Settings. You cannot, however, edit any exclusions in Audit Settings that are configured in the Scan Settings.

Rejecting versus excluding

When configuring session exclusions for file extensions, hosts, and URLs, you can reject the session, exclude the session, or reject and exclude the session. Reject and Exclude are enabled by default. The following table describes how the sensor handles rejecting and excluding each session type.

Session Exclusion	Reject	Exclude
File extension exclusion	The sensor will not request files of the type you specify. **Note:** By default, most image, drawing, media, audio, video, and compressed file types are rejected.	The sensor will request the files, but will not attack them (during an audit) and will not examine them for links to other resources.
Host or URL exclusion	The sensor will not send any HTTP requests to the host or URL you specify. For example, you should usually reject any URL that deals with logging off the site, because you don't want to log out of the application before the scan is completed.	During a crawl, the sensor will not examine the specified host or URL for links to other resources. During the audit portion of the scan, the sensor will not attack the specified host or URL. If you want to access the URL or host without processing the HTTP response, such as to check for broken links on URLs that you don't want to process, select the **Exclude** option, but do not select **Reject**.

Adding a file extension exclusion

To add an exclusion for file extensions:

1. Click **add operation**+ at the top of the EXCLUDED OR REJECTED FILE EXTENSIONS table.
   A row is added to the table.
2. In the **File Extension** box, type the extension to exclude.

Important! The file extension cannot contain the following special characters:

`- , # % & $ * : < > ? / \ -`

It can contain a period (.) character only at the beginning of the extension, such as `.jpg`, although the period will not be visible in the table after saving. The file extension cannot contain multiple period (.) characters.

3. To not request files with this extension, select **reject**.
4. To request files with this extension but not attack them, select **exclude**.
5. Click **confirm** ✔.

Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

The session exclusion is added to the table.

Adding a host exclusion

To add an exclusion for a host:

1. Click **add operation** + at the top of the EXCLUDED OR REJECTED HOSTS table.
2. In the **Host** box, enter the fully qualified host name or a regular expression designed to match the targeted host to exclude.

Tip: You can access the Regex Editor from the **Tools menu** ⋮.

3. To not send any HTTP requests to the host, select **reject**.
4. To not examine the host for links to other resources, select **exclude**.
5. Click **confirm** ✔.

Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

The session exclusion is added to the table.

Adding a URL exclusion

To add an exclusion for a URL:

1. Click **add operation** + at the top of the EXCLUDED OR REJECTED URLS table.
2. In the **File Extension** box, enter the URL or a regular expression designed to match the targeted URL to exclude.

Tip: You can access the Regex Editor from the **Tools menu** ⋮.

3. To not send any HTTP requests to the URL, select **reject**.
4. To not examine the URL for links to other resources, select **exclude**.

5. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Adding a MIME-type exclusion

To add an exclusion for a MIME-type:

1. Click **add operation** + at the top of the EXCLUDED MIME TYPES table.
2. In the **MIME Type** box, enter a MIME type.
3. Click **confirm** ✔.

   Tip: When creating a session exclusion, clicking **discard** — in the top right of the table or **cancel** × to the right of new row removes the new row from the table.

   The session exclusion is added to the table.

Editing existing session exclusions

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting a session exclusion

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring audit attack exclusions

Audit attack exclusions settings enable you to configure parameters, cookies, or headers to exclude from attacks during a scan.

Excluding parameters

Excluding parameters prevents the sensor from using certain parameters in the HTTP request to attack the website. This feature is used most often to avoid corrupting query and POSTDATA parameters.

You can specify a parameter using either a text string or a regular expression.

Adding a parameter to exclude

To add an excluded parameter:

1. Under **EXCLUDED PARAMETERS**, click **CREATE**.
   The Excluded Parameter dialog box opens.
2. In the **HTTP Parameter** box, enter the name of the parameter you want to exclude or a regular expression pattern.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. In the **Look for parameters in** drop-down list, choose the area in which the parameter may be found. Options are HTTP query data, HTTP post data, and HTTP custom data. You can select all areas, if necessary.
4. Click **OK**.
   The parameter is added as a row to the excluded parameters table.

Excluding cookies

Excluding cookies prevents the sensor from using certain cookies in the HTTP request to attack the website. This feature is used to avoid corrupting cookie values.

This setting requires you to enter the name of a cookie.

In the following example HTTP response, the name of the cookie is "FirstCookie."

```
Set-Cookie: FirstCookie=Chocolate+Chip; path=/
```

You can specify a cookie using either a text string or a regular expression.

Adding a cookie to exclude

To add an excluded cookie:

1. Under **EXCLUDED COOKIES**, click **add operation** +.
   A row is added to the excluded cookies table.
2. In the **Cookie** box, type the cookie name.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. Click **confirm** ✔.

Excluding headers

Excluding headers prevents the sensor from using certain header fields in the HTTP request to attack the website. This feature is used to avoid corrupting header values.

You can specify a header fields using either a text string or a regular expression.

Adding a header to exclude

To add an excluded header field:

1. Under **EXCLUDED HEADERS**, click **add operation** +.
   A row is added to the excluded headers table.
2. In the **Header** box, type the header field name.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. Click **confirm** ✔.

Editing an excluded parameter, cookie, or header

To edit a row in a table:

1. Click **edit** for the row that you want to edit.
2. Edit the value or values in the row.
3. Click **confirm** ✔.

   Tip: Clicking **cancel** in the top right of the table or to the right of the entries being edited cancels all changes and returns the entries to their original values.

   The edits are saved.

Deleting an excluded parameter, cookie, or header

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Configuring audit attack expressions

You may select one of the following language code-country code combinations (as used by the CultureInfo class in the .NET Framework Class Library):

- en-us: English - United States
- es-es: Spanish - Spain
- ja-jp: Japanese - Japan
- ko-kr: Korean - Korea
- pt-br: Portuguese - Brazil
- zh-cn: Chinese - China
- zh-tw: Chinese - Taiwan

The CultureInfo class holds culture-specific information, such as the associated language, sublanguage, country/region, calendar, and cultural conventions. This class also provides access to culture-specific instances of DateTimeFormatInfo, NumberFormatInfo, CompareInfo, and TextInfo. These objects contain the information required for culture-specific operations, such as casing, formatting dates and numbers, and comparing strings.

Configuring vulnerability filtering

By applying certain filters, you can limit the display of certain vulnerabilities reported during a scan. The options are:

- **Standard Vulnerability Definition v***<version>* - This filter sorts parameter names for determining equivalency between similar requests. For example, if a SQL injection vulnerability is found in parameter "a" in both `http://x.y?a=x;b=y` and `http://x.y?b=y;a=x`, it would be considered equivalent.
- **Parameter Vulnerability Roll-Up** - This filter consolidates multiple parameter manipulation and parameter injection vulnerabilities discovered during a single session into one vulnerability.

- **403 Blocker** - This filter revokes vulnerabilities when the status code of the vulnerable session is 403 (Forbidden).
- **Response Inspection DOM Event Parent-Child** - This filter disregards a keyword search vulnerability found in JavaScript if the same vulnerability has already been detected in the parent session.

All available filters are listed in either the **Disabled Filters** list or the **Enabled Filters** list.

Enabling and disabling vulnerability filters

To enable filters:

- Select a filter in the **Disabled Filters** list and click **enable filter** >.

  The filter is removed from the **Disabled Filters** list and added to the **Enabled Filters** list.

  Tip: To enable all available filters, click **enable all filters** ».

To disable filters:

- Select a filter in the **Enabled Filters** list and click **disable filter** <.

  The filter is removed from the **Enabled Filters** list and added to the **Disabled Filters** list.

  Tip: To disable all available filters, click **disable all filters** «.

Suppressing off-site vulnerabilities

If your web application includes links to hosts that are not in your Allowed Hosts list, the sensor may identify passive vulnerabilities on those hosts. To suppress all vulnerabilities against sessions for off-site hosts that are not in your Allowed Hosts list, select the **Suppress Offsite Vulnerabilities** check box.

Configuring Smart Scan settings

Smart Scan is an "intelligent" feature that discovers the type of server that is hosting the website and checks for known vulnerabilities against that specific server type. For example, if you are scanning a site hosted on an IIS server, the sensor will probe only for those vulnerabilities to which IIS is susceptible. It would not check for vulnerabilities that affect other servers, such as Apache or iPlanet.

Enabling or disabling Smart Scan

Smart Scan is enabled by default.

To disable Smart Scan:

- Slide the **Enable Smart Scan** toggle to the disabled position.

To enable Smart Scan:

- Slide the **Enable Smart Scan** toggle to the enabled position.

Configuring Smart Scan options

If Smart Scan is enabled, you can choose one or more of the identification options described in the following table.

Option	Description
Use regular expressions on HTTP responses to identify server/application types	The sensor searches the server response for strings that match predefined regular expressions designed to identify specific servers.
Use server analyzer fingerprinting and request sampling to identify server/application types	The sensor sends a series of HTTP requests and then analyzes the responses to determine the server/application type.

Configuring custom server/application type definitions

If you know the server type for a target domain, you can configure it using the **Custom server/application type definitions** section. This identification method overrides any other selected method for the server you specify.

To specify a custom definition:

1. Click **CREATE**.
   The CUSTOM SERVER/APPLICATION DEFINITION dialog box appears.
2. In the **Host** box, enter the domain name or host, or the server's IP address.
   Alternatively, you can select the **Use Regular Expression** option, enter a regular expression designed to identify a server.

   Tip: You can access the Regex Editor from the **Tools menu** ⋮.
3. Select one or more entries from the **Server/Application Type** drop-down list.
4. Click **OK**.
   The server is added as a row to the Custom Server/Application Type Definitions table.

Editing an existing custom definition

To edit a custom definition:

1. Select the check box for the definition to edit, and click **EDIT**.
   The CUSTOM SERVER/APPLICATION DEFINITION dialog box appears.
2. Edit the values.
3. Click **OK**.

Deleting a signature

To delete a row in a table:

1. Select the check box for each row that you want to delete.
2. Click **REMOVE**.
   The selected rows are deleted.

Chapter 6: Working with scans

You can view the scans that are available in the ScanCentral DAST database in the Scans view. You can also start a new scan, refresh the scan table, delete scans, and download scans, settings, and logs. You can pause, stop, and resume scans that are currently running, and re-import completed scans that failed to import. You can view details about each scan in the scan detail panel.

Accessing the DAST Scans view

After you configure your ScanCentral DAST environment and enable DAST in the Administration view in Application Security, you can work with DAST scans directly in Application Security.

To access the DAST Scans view in Application Security:

- Select **SCANCENTRAL** > **DAST**.
  The Overview page appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Scans view

The Scans view displays in a table the scans that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information that are available for each scan.

Column	Description
Scan Id	Indicates the integer ID in the ScanCentral DAST database for the scan. **Note:** Each scan is assigned an integer ID when it is added to the

Column	Description
	ScanCentral DAST database.
Application	Indicates the application that was selected when the scan was configured.
Version	Indicates the version that was selected when the scan was configured. **Tip:** The versions listed in this column are links. You can click a link to open the Application Version Overview in a new tab in Application Security.
Name	Indicates the name of the scan. This is the name that was assigned in the scan settings.
Url	Identifies the target URL for the scan.
Critical **High** **Medium** **Low**	Indicates the number of findings for each severity category in the scan. For more information, see "Understanding vulnerability severity" on page 307.
Started On	Indicates the date and time that the scan started. The start time is stored in the dynamic scan database as UTC time and is converted to the local machine's system time when displayed in the user interface.
Status	Indicates the current status of the scan. Possible statuses are as follows: • **Queued** – The scan has been submitted and is waiting for an available sensor. • **Pending** – The scan has been accepted by a sensor but is waiting for the sensor to acknowledge that it has accepted and started the scan. • **License Unavailable** - No license is available for a sensor to start the scan. The scan remains in the queue until a license is available for use. **Note:** If the **Use this sensor only** option was not selected when the scan was submitted, the scan will use any available sensor in the assigned pool.

Column	Description
	• **Paused** – The sensor might have accepted the scan but not yet started it, or the user might have paused the scan so that it is not in a running state. • **Running** – The sensor is actively conducting the scan. • **Complete** – The sensor has finished the scan and results are available. If the **Submit for triage** option was selected during scan configuration, then the scan has been published to Application Security, where you can perform audit analysis of the findings. • **Interrupted** – Something went wrong with the sensor that was conducting the scan. For example, the sensor heartbeat has expired. • **Unknown** – The scan failed to complete for an unknown reason. • **Importing** – The scan is being imported from the ScanCentral DAST database and published to Application Security. • **Import Failed** – Something went wrong while importing a `.fpr` or `.scan` file from the sensor to the ScanCentral DAST database. • **Import Scan File Queued** – The `.scan` file has been uploaded to ScanCentral DAST and is being saved to the database so that it can be processed by the Utility Service. • **Pending Scan File Import** – The `.scan` file was successfully saved to the database and is waiting to be processed by the Utility Service. • **Importing Scan File** – The Utility Service is importing the `.scan` file. • **Failed to Import Scan File** – Something went wrong while uploading and saving the `.scan` file to the database or during processing of the file. • **Failed to Start** – A sensor accepted the scan, but the scan failed to start. Possible reasons include: • The Application Security DAST API is not running. • The connection to the ScanCentral DAST database has been lost. • Communication with the sensor has been lost. • The sensor failed to start. • The scan settings contain errors or invalid settings. • **Pausing** – The user has paused the scan, which now displays this

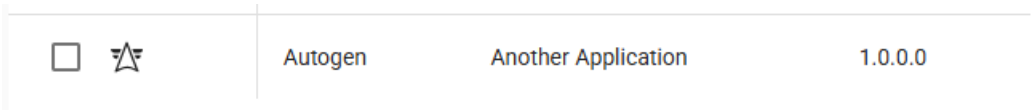
Column	Description
	transitional state before changing to Not Running. • **Resuming** – The user has resumed the scan, which now displays this transitional state before changing to Running. • **Completing Scan** – The user has paused the scan and subsequently clicked **Complete**, which stops the scan at that point and processes it as an incomplete scan. **Tip:** You can perform the same analysis and operations on an incomplete scan as you can a completed scan. • **Resume Scan Queued** – The user resumed a paused scan and the scan is waiting for the sensor to become available. • **Forced Complete** – The user paused a scan and subsequently clicked **Complete**. The scan completed with partial results.
Status Reason	Indicates the reason for Paused, Pausing, Resuming, Resume Scan Queued, Running, and Forced Complete statuses. Possible reasons are **Deny Interval**, **Scan Priority**, and **Deny Interval User Paused**. For more information, see "Working with deny intervals" on page 362, "Understanding advanced scan prioritization" on page 196, and "Configuring scan priority" on page 195. The following paragraphs describe the combined status and status reasons: • **Paused / Deny Interval** – The scan was running when a deny interval started. The scan is now paused until the deny interval ends. • **Paused / Deny Interval User Paused** – The scan was paused by a user, but has since entered a deny interval. • **Paused / Scan Priority** – The scan was running when a higher-priority scan started. The scan is now paused until the higher-priority scan completes or another sensor accepts the scan. • **Pausing / Deny Interval** – The scan was running when a deny interval started. The scan now displays this transitional state before changing to Paused Deny Interval. • **Pausing / Scan Priority** – The scan was running when a higher-priority scan started. The scan now displays this transitional state before changing to Paused Scan Priority. • **Resuming / Deny Interval** – The scan was paused for a deny

Column	Description
	interval, but the deny interval has ended. The scan now displays this transitional state before changing to Running. • **Resuming / Scan Priority** – The scan was paused for a higher-priority scan. The scan now displays this transitional state before changing to **Running Scan Priority**. • **Resume Scan Queued / Deny Interval** – The scan was paused due to a deny interval which has ended, so the scan is queued to be resumed. • **Resume Scan Queued / Scan Priority** - The scan was paused for a higher-priority scan which has completed, so the scan is queued to be resumed. • **Running / Deny Interval** – The scan was paused for a deny interval. The deny interval has ended and the sensor is actively conducting the scan. • **Running / Scan Priority** – The scan was paused for a higher-priority scan. The higher-priority scan has completed or another sensor has accepted the scan and is actively conducting it. • **Forced Complete / Deny Interval** – The scan was running when a deny interval started. The scan stopped and completed with partial results.
Duration	Indicates how long the scan ran before completion. For scans that are not completed, the column displays the last known duration that was received from the sensor.
Requests	Indicates the total number of requests sent during the scan.
Macro Playbacks	Indicates the number of times that macros have been played during the scan.
Priority	Indicates the scan priority from 0 through 10. For more information, see "Configuring scan priority" on page 195.
Purge date	If data retention is enabled, indicates the date when the scan will be purged from the database. The number in parentheses indicates the number of days until the purge date.
Publish Status	Indicates whether the scan has been published to Application Security. Possible statuses are as follows: • **Not Published** – The `.fpr` file has not been published.

Column	Description
	• **Published** – The `.fpr` file has been published. • **Failed to Publish** – ScanCentral DAST attempted to publish the `.fpr` file, but it failed. Application Security might be down or there might be a network issue.
Publish Status Reason	Indicates why the `.fpr` file was not published to Application Security. Only applicable when the Publish Status is **Not Published** or **Failed to Publish**. Possible reason is **Artifact is too large**. **Important!** The files you upload to Application Security must not exceed 2GB.

Pending Aviator jobs

When an item in the Scans view, Settings List view, or Base Settings view has a pending Aviator job, an **Aviator Macro Autogen** icon ( ) appears to the right of the item's selection check box.



Selecting the item opens the details panel, where Aviator-specific actions are available. For more information, see "Managing Aviator jobs" on page 479.

Understanding the scan detail panel

When you click a scan in the Scans view, the scan detail panel appears to the right. The scan detail panel provides options to view, rescan, download, and publish completed scans. For more information, see the following:

- "Viewing scan results" on page 304
- "Rescanning an application" on page 299
- "Downloading a file" on page 302
- "Publishing to Application Security" on page 296

In addition to these options, the scan detail panel provides information about the scan, as described in the following paragraphs.

Findings by severity

The number of findings for each severity category in the scan appears at the top of the panel. From left to right, the severity categories are: Critical, High, Medium, and Low.



Additional scan details

The detail panel displays the same information that is displayed in the Scans view for the selected scan, as well as the information described in the following table.

Item	Description
Created On	Indicates the date and time that the scan was created in the dynamic scan database and queued to be run.
Created By	Identifies the user who created or imported the scan. **Note:** Scans started by way of the API display user information from the Fortify login token. Scheduled scans, which are started by the Global Service, display **SystemProcess**.
Scan Type	Indicates the type of scan selected during scan configuration: **Standard Scan**, **Workflow-Driven Scan**, or **API Scan**.
Status Update	Indicates the date and time that the sensor last reported its status.
Has Site Authentication	Indicates whether site authentication was used to conduct the scan. Possible values are **Yes** and **No**.
Has Network Authentication	Indicates whether network authentication was used to conduct the scan. Possible values are **Yes** and **No**.
Has API Auth Credentials	For API scans, indicates whether authentication was used to conduct the scan. Possible values are **Yes** and **No**.
Failed Requests	Shows the number of failed requests that occurred during the scan.
KB Sent / KB Received	Shows the total number of kilobytes sent and received during the scan.
Pool	Identifies the pool to which the sensor belongs in Application

Item	Description
	Security.
Policy	Identifies the dynamic policy that was used to conduct the scan.
Completed Date	Indicates the date and time that the scan finished. Available only for scans with a "Complete" status. For more information, see "Understanding the Scans view" on page 285.
Sensor	Indicates the name of the dynamic sensor that conducted the scan.
Publish Status Update	Indicates the date and time that the scan was published to Application Security.
Scan Schedule	If the scan is the result of a schedule, indicates the name of the schedule.
Purge date	If data retention is enabled, indicates the date when the scan will be purged from the database. The number in parentheses indicates the number of days until the purge date.

Understanding the scan EVENTS tab

ScanCentral DAST records events for the scan that are not specific to the Fortify DAST sensor in the EVENTS tab of the detail panel. The events are chronologically ordered and may be of use in troubleshooting issues with scans.

To update the entries, click **REFRESH**.

Understanding the scan LOGS tab

ScanCentral DAST records Fortify DAST sensor logs that are displayed in the LOGS tab of the detail panel. The sensor logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with scans.

To update the entries, click **REFRESH**.

Working with active scans

You can pause, stop, resume, and re-import active scans in the Scans view. The actions that you can take depend on the current status of the scan. Active scans are those that do not show a status of Complete.

Pausing a scan

You can pause a scan that has a status of Running.

To pause a scan, do one of the following:

- In the Scans view, click **pause** ❚❚ for the scan you want to pause.
- In the scan detail panel for a selected scan, click **pause** ❚❚.

The scan is paused.

Stopping a scan

You can stop a scan that has a status of Not Running, Interrupted, Unknown, or Queued.

To stop a scan, do one of the following:

- In the Scans view, click **stop** ■ for the scan you want to stop.
- In the scan detail panel for a selected scan, click **stop** ■.

The scan is stopped.

Resuming a scan

You can resume a scan that has a status of Not Running or Interrupted.

To resume a scan, do one of the following:

- In the Scans view, click **start** ▶ for the scan you want to resume.
- In the scan detail panel for a selected scan, click **start** ▶.

The scan is resumed.

Re-importing a scan

If the "Submit for triage" option was selected during scan configuration, the scan is imported to Application Security upon completion. Importing a scan could take some time, during which the status in the scans view is "Importing." The status changes to "Import Failed" if unsuccessful. You can attempt to re-import a scan with the "Import Failed" status.

To re-import a scan, do one of the following:

- In the Scans view, click **retry** ↻ for the scan you want to re-import.
- In the scan detail panel for a selected scan, click **retry** ↻.

Another attempt is made to import the scan.

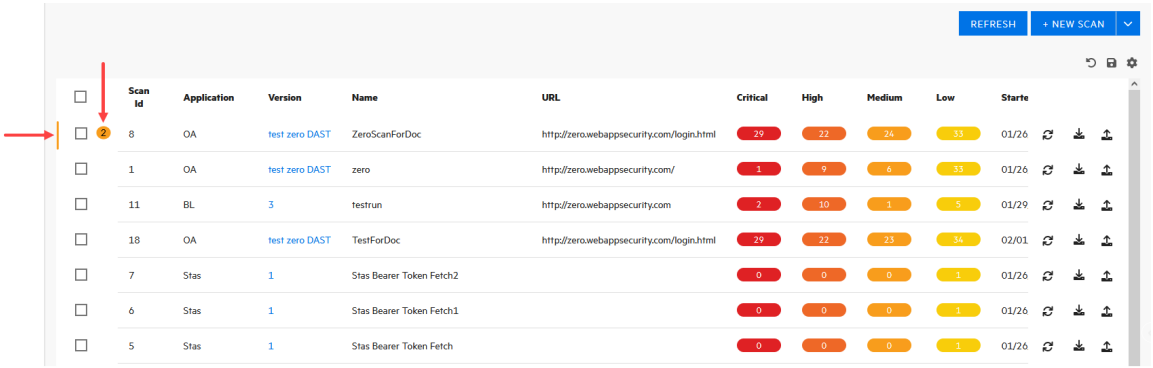
Working with alerts

Alerts occur when situations arise that *could* adversely affect scan performance or results. Alerts dealing with scan settings might provide you with suggested settings changes to improve performance of future scans. Other alerts may provide actionable information to help with a scan that is currently running.

Tip: The alerts feature includes sample intervals and active intervals. Sample interval alerts may occur as often as once per minute on the ALERTS tab. Although these alerts may not indicate a functional issue with the scan, if the number of alerts received becomes problematic, contact Customer Support for assistance in disabling the alerts feature. For more information, see "Preface" on page 30.

Identifying scans with active alerts

If a scan has an active and unacknowledged alert, the scan will be marked with an orange vertical bar on the left margin and a scan alerts icon indicating the number of alerts.



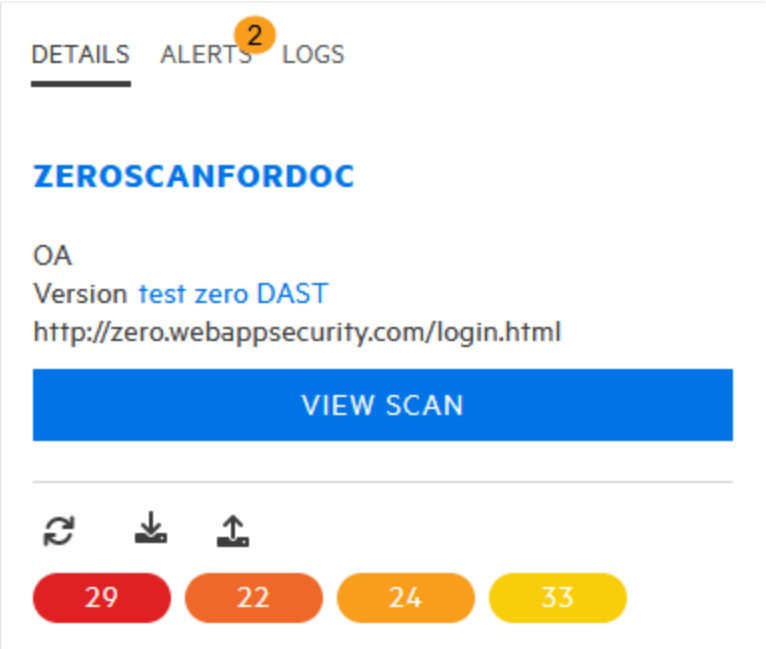
Accessing alerts

When you click a scan with an active and unacknowledged alert, the detail panel appears to the right. The number of unacknowledged alerts appears in an orange circle next to the ALERTS tab.

Note: Alerts are written to the scan log in near real time. However, you must refresh the page to view updates to the ALERTS tab.

To access the alerts:

1. Click the scan that has an active and unacknowledged alert in the Scans view.
   The scan detail panel appears to the right.



2. Click the **ALERTS** tab.
   The alerts that the scan triggered are listed.

Understanding the ALERTS Tab

The ALERTS tab displays the following categories of alerts:

- **NEW** – Lists the alerts that are active and have not yet been acknowledged. The number of alerts listed in this category should match the number displayed in the orange circle.
- **ACTIVE** – Lists the alerts that are active and have been acknowledged. These alerts are still affecting the scan.
- **HISTORY** – Lists alerts that are no longer active, but that occurred during the scan. These alerts are no longer affecting the scan.

Note: After the scan has completed or been forced to complete, all alerts become historical alerts.

Acknowledging new alerts

To acknowledge an alert in the NEW category:

1. On the **ALERTS** tab, click the alert.
   A check mark appears next to the alert, indicating that the alert is selected.
2. Click **MARK AS ACKNOWLEDGED**.
   The alert is moved to the ACTIVE category.

Important! Acknowledging an alert does not resolve the issue that caused the alert. You must perform troubleshooting to determine the cause and resolve it. For more information, see "Troubleshooting alerts" on page 496.

Managing the DAST Scans view

You can configure and submit a new scan, refresh the scans view, search for scans, publish scans to Application Security, and delete scans from the scans view on the Scans page. You can also import `.scan` files. For more information, see "Importing a scan" on the next page.

Starting a new scan

You can configure new settings or use existing settings, and then run a scan, which queues the scan in the scans view.

To configure settings or use existing settings for a new scan:

- Click **+ NEW SCAN**.
  The SETTINGS CONFIGURATION wizard opens.

Refreshing the Scans view

You must manually refresh the Scans view to see new scans that have been queued or scan statuses that have changed.

To refresh the Scans view:

- Click **REFRESH**.

Searching for scans

You can search by scan ID for a specific scan in the scans view.

To search for a scan:

1. In the **Scan Id** box, type the scan ID.
2. Click **SEARCH**.
   The scans view is updated to include only the exact match to the scan ID.

Publishing to Application Security

You can publish FPR artifacts to Application Security.

Note: If a scan does not have FPR artifacts, the publish icon is not available.

To publish FPR artifacts for a scan:

- Do one of the following:
  - In the Scans view, click **publish** for the scan whose FPR artifacts you want to publish.
  - In the scan detail panel for a selected scan, click **publish**.

  The FPR artifacts are published to the Application Security database.

Deleting scans

The scans displayed in the scans view come from the ScanCentral DAST database. You can delete scans from the database that you no longer need, depending on the scan status. Deleting scans from the database has no effect on scans that have already been published to Application Security.

You can delete scans that have a status of Complete, Queued, Pending, Failed to Start, Import Failed, Interrupted, Not Running, and Unknown.

To delete scans, do one of the following:

- Select one or more check boxes for scans in the scans view, and then click **DELETE** at the bottom of the table.
- Select a scan to view the scan details, and then click **DELETE** at the bottom of the scan details panel.

Using the force delete option

In some cases, scans may not be deleted from the ScanCentral DAST database after you click the delete button. When this occurs, a user with administrator-level privileges can force the deletion of the scan. For more information, see "Permissions in Application Security" on page 45.

To force delete a scan:

1. Select one or more check boxes for scans in the scans view, and then click **DELETE** at the bottom of the table.

   The Delete Scans dialog opens.
2. Select **Force delete**, and then click **OK**.

   Note: The Force delete option is available only for users with administrator-level privileges.

Importing a scan

You can import a `.scan` file that was created by Fortify DAST or another ScanCentral DAST sensor. Afterward, the imported scan settings, scan results, scan logs, site tree,

and FPR are available for download or for publishing to Application Security.

Important! The Utility Service starts the import process, and the Global Service completes the import process. Hence, both services must be running to import a scan.

To import a scan:

1. On the **Scans** view, click the **+ NEW SCAN** drop-down arrow and select **Import scan**.

   The SCAN IMPORT dialog box opens.
2. In the **APPLICATION** area, select an application to associate with the scan being imported.

   Tip: You can search for the application and application version. For more information about searching, see "Searching in input boxes" on page 147.
3. In the **APPLICATION VERSION** area, select a version to associate with the scan being imported.
4. In the **IMPORT SCAN** area, click **IMPORT**.

   A standard Windows Open dialog box appears.
5. Locate and select the `.scan` file to import, and then click **Open**.
6. If the scan already exists in the ScanCentral DAST database, you are prompted with the following options:
   - **CANCEL** – Stops the import
   - **CREATE** – Creates a new scan with a new Fortify DAST scan ID
   - **REPLACE** – Replaces the existing scan with the contents of the scan being imported
   - **OPEN** – Opens the existing scan
7. (Optional) To submit the completed scan for triage in Application Security, select **Submit for triage**. Submitting for triage enables you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

   A FILE UPLOAD dialog box shows the progress.

   Important! It might take some time for large scans to complete the import process. After the initial phase, the dialog box shows the "parsing" phase. OpenText recommends that you do not cancel the import during the parsing phase. Doing so will cause the scan to be queued for import. However, the scan will not import, and you will need to delete the scan.

For information about scan statuses related to importing a scan, see "Understanding the Scans view" on page 285.

Tip: If the import fails, check the Global Service and Utility Service log files. For more information, see "Locating log files" on page 484.

Rescanning an application

The rescan feature enables you to easily rescan an application from an existing scan. This feature is useful for conducting an identical scan of an updated site (using the same settings that were used for the original scan) to determine if previously discovered vulnerabilities have been fixed and if new ones have been introduced.

To rescan an application:

1. Do one of the following:
   - In the Scans view, click **rescan** for the scan whose application you want to rescan.
   - In the scan detail panel for a selected scan, click **rescan**.

   The RUN SCAN dialog box opens.
2. (Optional) in the **Name** box, enter a name for the scan.

   Tip: The original scan name is prepopulated in the **Name** box. Prepending the original name with "Rescan_" might help you to identify scan results for rescanned applications in your scans view.
3. Select a ScanCentral DAST sensor from the **Sensor** list.

   The list of sensors comes from the Application Security sensor pools. **Any Available** is the default.
4. (Optional) If you select a sensor, but it is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
5. Click **RUN**.

   The scan is queued to run.

Rescan and key store placeholders

If the scan settings, base settings, or macro parameters of the original scan use key store placeholders, a rescan will use the latest values from the key store. The latest values may not be the values that were used in the original scan.

Downloading DAST scans, settings, and logs

You can download a scan settings file (`.xml` format) from the ScanCentral DAST database to your local machine for any scan in the Scans view, except certain scans with the License Unavailable status. (For more information, see "License Unavailable scan status" on the next page.) Depending on the status of the associated scan, you can also download a log file, the site tree (`.csv` format), or the scan results (`.scan` or `.fpr` format).

Suppressed findings (`.json` format) are available for download regardless of scan status. If there are no suppressed findings, however, then the file contents will be an empty array.

Note: You must have Fortify DAST, Log Viewer, Traffic Viewer, or another Fortify DAST tool on your local machine to work with the log file or scan results.

Important! While downloading a file, you must keep the browser open. Closing the browser will end the download prematurely.

Important information about settings

Settings that do not exist in Fortify DAST, such as Scan Priority, Submit for Triage, Enable SAST Correlation, and so forth, will not be exported when exporting ScanCentral DAST settings. If you have multiple ScanCentral DAST environments, and you export settings from one environment to another, settings that do not exist in Fortify DAST will be dropped. However, when performing an upgrade from the previous version of ScanCentral DAST to the current version, these settings are successfully migrated.

Settings that include key store placeholders

If an administrator changes the value for a key store placeholder, the scan settings that use the key store placeholder will consume the new value when the settings are downloaded or used to start a scan. When downloading scan settings that use key store placeholders, it may take time to replace the placeholders with the corresponding values from the key store entries. For more information about key stores, see "Understanding key stores" on page 446.

Paused scans

Anytime a scan is paused—by a user, due to scan priority, or due to deny interval—the partial scan results are uploaded to the ScanCentral DAST database and are available for download. After the partial results have been uploaded, the scan is deleted from the sensor.

ScanCentral DAST does not send the results to Application Security until the scan is complete or forced complete.

License Unavailable scan status

If a scan has not started because a license is unavailable, then scan settings are not created. Therefore, no file types are available for download for these scans with the License Unavailable status.

However, if a scan is paused and then resumed, but no license is available, then scan settings, scan results, site tree, and scan log files are available for download for these scans with the License Unavailable status.

File types available

The following table describes the file types that are available for download for each scan status.

Scan Status / Status Reason	File Types Available for Download				
	Scan Settings	Scan Result / Site Tree / FPR	Scan Logs / SC DAST Service Logs	Suppressed Findings	Notes
Complete	x	x	x	x	
Completing Scan	x			x	
Failed to Start	x			x	
Forced Complete Forced Complete / Deny Interval	x	x	x	x	Scans with a Forced Complete status might not have scan results or a site tree, depending on when the scan was stopped. For this reason, Scan Result and Site Tree might not be available file types to download.
Import Scan File Queued Pending Scan File Import Importing Scan File Failed to Import Scan File		x		x	Only Scan Results are available for these import statuses.
Importing Import Failed	x			x	
Interrupted	x		x	x	
Not Running	x			x	
Paused Paused / Deny Interval Paused / Deny Interval User Paused Paused / Scan	x	x		x	Scans with a Paused status do not include an FPR and cannot be published to Application Security.

Scan Status / Status Reason	File Types Available for Download				
	Scan Settings	Scan Result / Site Tree / FPR	Scan Logs / SC DAST Service Logs	Suppressed Findings	Notes
Priority					
Pausing Pausing / Deny Interval Pausing / Scan Priority	x			x	
Pending	x			x	
Queued	x			x	
Resume Scan Queued Resume Scan Queued / Deny Interval Resume Scan Queued / Scan Priority	x			x	
Resuming Resuming / Deny Interval Resuming / Scan Priority	x			x	
Running Running / Deny Interval Running / Scan Priority	x			x	
Unknown	x			x	

For more information about the scan statuses, see "Understanding the Scans view" on page 285.

Downloading a file

To download a file for a scan:

1. Do one of the following:
   - In the Scans view, click **download** for the scan whose file you want to download.
   - In the scan detail panel for a selected scan, click **download**.

The DOWNLOAD dialog box opens.

2. Select the file type to download from the list.

   Note: The available file types to download depend on the scan status. For details, see "File types available" on page 301.

3. Click **DOWNLOAD**.

   By default, the file is downloaded to the folder on your local machine that is specified in your browser settings for downloads.

Performing actions on multiple scans

You can select one or more scans in the scans view and perform an action for all selected scans. The following actions can be performed on multiple scans:

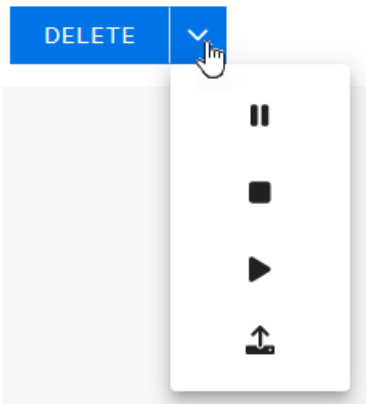
- Pause
- Stop
- Start
- Publish

Note: You can also select and delete multiple scans. For more information, see "Deleting scans" on page 297.

Clicking an action performs the action for all selected scans. If the action is successful for all selected scans, then a success message appears. If the action cannot be performed for one or more selected scans, an error message appears indicating which scan or scans the action was not performed on.

To perform an action on multiple scans:

1. In the scans view, select the check boxes for the scans on which to perform the action.
2. Click the drop-down arrow next the **DELETE** button.



3. Continue according to the following table.

To...	Click...
Pause the scans	**Pause selected scans** ⏸.
Stop the scans	**Stop selected scans** ■.
Restart the scans	**Restart selected scans** ▶.
Publish the results of the scans	**Publish selected scans** ⤴.

A success or error message appears.

Viewing scan results

You can examine the scan results for scans with a status of Complete or Forced Complete. For more information about scan statuses, see "Understanding the Scans view" on page 285.

To view scan results:

1. In the Scans view, click the scan that you want to view.
   The scan detail panel appears to the right.
2. Click **VIEW SCAN**.
   The scan opens in a new tab with the scan name displayed. This view of the scan is called scan visualization.

Tip: If you run a scan in ScanCentral DAST, the findings are automatically imported. If the completed scan fails to import or if the completed scan was not conducted in ScanCentral DAST, the button will be labeled **IMPORT FINDINGS**. When this occurs, you must import the findings before you can view the scan.

Working with the Site Tree

By default, the Site Tree displays an unfiltered tree view of all traffic that was generated during the scan. The tree includes a list of hosts and all sub-directories within those hosts. In this view, you can select a top-level host and expand the sub-directories to examine the requests and responses that occurred at each level. To display the requests that were made to a resource, select the resource in the Site Tree.

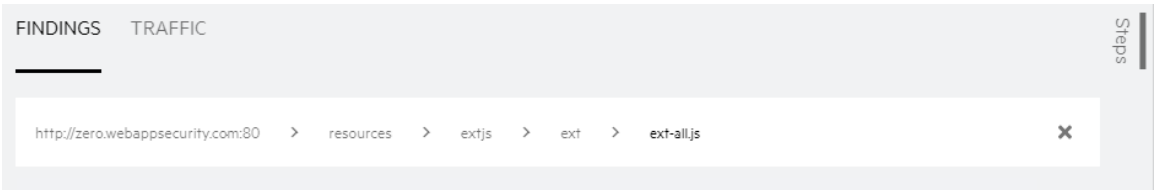
Site Tree icons

The following table identifies the icons that appear in the Site Tree.

Icon	Name	Represents
	Server/host	The top level of your site's tree structure **Note:** You might have multiple server/host icons in your site tree representing different protocols and ports.
/	Folder	A directory
	Page	A file
	Operation	An API operation followed by the operation name in the following format: • `Operation: GetClients` • `Operation: UpdateClient`
	Parameter	An API parameter followed by the parameter name in the following format: • `Parameter: id` • `Parameter: first_name`

Using breadcrumbs

When you select a resource in the Site Tree, breadcrumbs appear at the top of the Findings and Traffic tables, similar to the sample shown here.



Breadcrumbs provide a visual aid that indicates the location of the resource within the website's hierarchy. You can click a breadcrumb in the path to view findings or traffic for that resource.

To filter the findings or traffic for a specific resource listed in the breadcrumbs:

- Click the resource in the breadcrumbs.

  For example, if you want to view all findings or traffic for the extjs folder shown in the previous image, click **extjs**.

  The selected resource becomes the final breadcrumb and the Findings and Traffic tables are updated to show only data for the selected resource.

To remove the filter completely:

- Click **Clear Breadcrumbs** × at the end of the breadcrumbs list.
  The breadcrumbs are removed and the findings and traffic data are no longer filtered.

Understanding the Findings table

The Findings table displays information about each vulnerability discovered during an audit of your web presence. Each row (or session) in the Findings table represents a single finding.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

Available columns

The following table describes the available columns.

Column	Description
Severity	A relative assessment of the vulnerability, ranging from low to critical. For more information, see "Understanding vulnerability severity" on the next page.
Check ID	The identification number of an Fortify DAST probe that checks for the existence of a specific vulnerability. For example, Check ID 742 tests for database server error messages.
Name	An Fortify DAST probe for a specific vulnerability, such as Cross-site Scripting, Unencrypted Log-in Form, and so on.
URL	The hierarchical path to the resource along with parameters.
Parameter Name	The name of the vulnerable parameter.
Parameter Value	The value assigned to the vulnerable parameter.
CWE	The Common Weakness Enumeration identifier(s) associated with the vulnerability.
Method	The HTTP request method used for the attack.
Kingdom	The vulnerability category from the Seven Pernicious Kingdoms taxonomy for ordering and organizing vulnerabilities. For more information, see https://vulncat.fortify.com/.

Column	Description
Session ID	The unique session ID for the request and response in the ScanCentral DAST database.

Known limitation with suppressed findings

Currently, findings that are suppressed in Application Security are not suppressed in the ScanCentral DAST Findings table.

Understanding vulnerability severity

Every check in Fortify's SecureBase includes a severity. The severity is determined and assigned by Fortify Security Researchers.

Severity descriptions

Severity descriptions are as follows:

- **Low** – Interesting issues, or issues that could potentially become more severe.
- **Medium** – Non-HTML errors or issues that could be sensitive.
- **High** – Generally, the ability to view source code, files out of the Web root, and sensitive error messages.
- **Critical** – An attacker might have the ability to execute commands on the server or retrieve and modify private information.

How severity is determined

When assigning a severity, Fortify Security Researchers consider the real world impact of the vulnerability, including the following aspects:

- The maximum damage that could result if the vulnerability were exploited
- The conditions of the issue that the check can detect
- Any related Common Vulnerabilities and Exposures (CVEs)

The Research Team then debates to reach consensus and assigns a number as described in the following table.

Assigned Number	Severity
0 - 9	Normal [1]
10	Information [2]
11 - 25	Low

Assigned Number	Severity
26 - 50	Medium
51 - 75	High
76 - 100	Critical

[1]This severity is not displayed in ScanCentral DAST findings.

[2]This severity is not displayed in ScanCentral DAST findings.

Working with Findings

You can view the vulnerabilities discovered during the scan on the Findings tab, which includes the Findings table and the Vulnerability Description, HTTP, and Steps tabs.

Tip: Remember that selecting a resource in the Site Tree filters the data to that resource in the Findings table. For more information, see "Working with the Site Tree" on page 304.

Viewing the Vulnerability Description

The Vulnerability Description tab displays content from SecureBase related to the selected vulnerability. In addition to a detailed description of the vulnerability, the SecureBase content might include information on how to verify the issue, possible implications if the issue is not fixed, remediation information, and links to additional references.

To view the Vulnerability Description:

- Select a finding in the **FINDINGS** table.
  The VULNERABILITY DESCRIPTION tab displays information about the vulnerability.

Viewing the Request and Response

The HTTP tab includes the request and response session details for the selected vulnerability.

To view the request and response:

1. Select a finding in the **FINDINGS** table.
2. Click the **HTTP** tab.
   In the REQUEST area, the attack is highlighted. In the RESPONSE area, the vulnerability is highlighted.

Viewing Steps

The Steps tab displays the route taken by the sensor to arrive at the session selected in the Findings table. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology.

To view the steps:

1. Select a finding in the **FINDINGS** table.
2. Click the **Steps** tab.

   The STEPS table displays the route taken by the sensor to arrive at the session selected.

To close the Steps tab, do one of the following:

- Press the **ESC** key.
- Click the **Steps** tab again.

Working with suppressed findings

Findings in ScanCentral DAST are referred to as issues when they are published to Application Security and managed in the AUDIT page. If you have configured Kafka settings in ScanCentral DAST to provide support for the syncing of audit history changes in Application Security, then when issues are suppressed in the AUDIT page, that action is synced in ScanCentral DAST. For more information on using the AUDIT page, see *OpenText™ Application Security User Guide*.

Understanding suppressed findings and issues

If you are familiar with OpenText DAST (Fortify WebInspect), then you most likely know about the following types of suppressed findings:

- **False Positive** - A finding that upon further investigation by a developer is determined not to be a vulnerable URL, operation, or parameter.
- **Ignored** - A finding that a security lead or developer has chosen to ignore. Generally, these should be low-level or informational findings that carry little risk of exploitation, or have mitigation that is outside the scope of testing.

However, in Application Security, there are no **False Positive** or **Ignored** tags. The following table maps these types of suppressed issues between the two products.

Fortify DAST	Application Security
False Positive	**Suppressed** with **Not an Issue** tag
Ignored	**Suppressed**

How suppressed issues are synced

Suppressed issues are correlated at the application version level. For application versions that are referenced in ScanCentral DAST, a background process requests that audits in Application Security be published to the Kafka message queue. ScanCentral DAST processes the audits and reflects any suppressed issues in its Scans view and scan visualization. For more information about these views, see "Understanding the Scans view" on page 285 and "Viewing scan results" on page 304.

Known limitation with suppressed findings

Suppressed findings do not currently include the full audit history. In ScanCentral DAST, you will see only the latest audit data per tag from Application Security, with no audit history.

Audits in imported scans

Any audits that are in the ScanCentral DAST database, either from Application Security or from an imported scan, are reflected in the Scans view and scan visualization. When an imported scan is published, audits from the ScanCentral DAST database are sent to Application Security.

Important! The following imported scans will not show suppressed issues after selecting the option to include suppressed findings:

- Scans imported prior to the 24.2.0 release
- Scans that were exported from Fortify DAST prior to the 24.2.0 release and that are imported into ScanCentral DAST

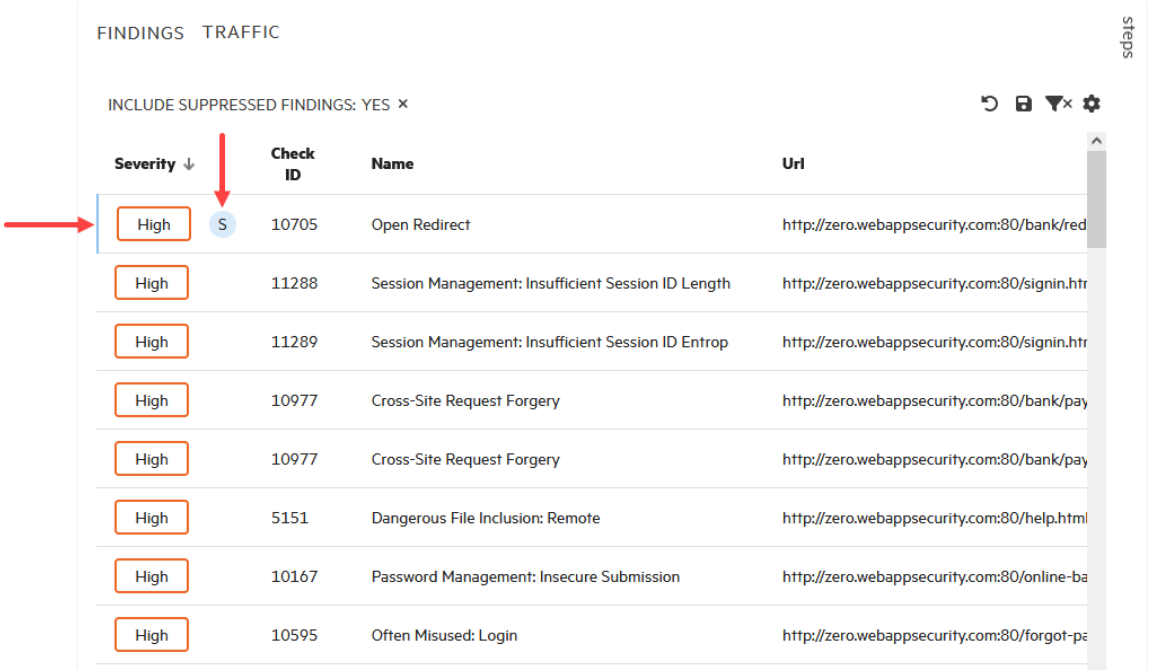
Including and hiding suppressed findings

By default, suppressed findings are hidden in the Scans view and when viewing scan results (scan visualization). You can use the table preferences panel to include suppressed findings in the Scans view table or in the Findings table in scan visualization.

To include suppressed findings:

1. Click **Table Preferences** ⚙.
   The table preferences panel opens.
2. In the **FILTER** area, slide the **Hide suppressed findings** toggle to **Include suppressed findings**.
3. Click **OK**.
   If suppressed findings are included in a scan in the Scans view table, the number of findings for the affected severity categories are updated to include the suppressed findings.

If suppressed findings are included in a scan in scan visualization, the Findings table is updated to include the suppressed findings. Each suppressed finding is marked with a blue left side border on the table row and a suppressed S icon.



To hide suppressed findings:

- Click **Remove Filter** × for the **INCLUDE SUPPRESSED FINDINGS: YES** filter.

Understanding the Traffic table

The Traffic table displays traffic generated during the scan, enabling you to explore the traffic for the scan. The Traffic table is always available in the scan results. If you enabled traffic monitor logging in the scan settings, then the Traffic table lists all of the scan traffic. For more information, see "Enabling traffic monitor" on page 199 and "Enabling traffic monitor in base settings" on page 410.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

Available columns

The following table describes the available columns.

Column	Description
Request Start	The date and time the sensor started sending the request.

Column	Description
Request End	The date and time the sensor finished sending the request.
Host	The top-level URL of the target website.
Port	The port number over which the requests were sent.
Path	The hierarchical path to the resource on the web server.
Method	The HTTP request method used, such as GET, POST, and PUT.
Status	The HTTP status code returned from the host. For more information, see "HTTP status codes" on page 525.
Category	Broadly defines the source of the request, such as audit, crawl, and so forth. This information might be useful for diagnostics.
Sequence	The order in which the request appeared in the traffic.
Scheme	The protocol used to make the request, such as `http://` or `https://`.
Error Code	An error code that indicates the request failed at the TCP/IP level, such as the connection closed or a time out occurred.
Request Length	The request length, expressed in bytes.
Response Length	The response length, expressed in bytes.
Scan.Sid	The unique session ID for the request and response in the ScanCentral DAST database.
Scan.Psid	The unique parent session ID for the request and response in the ScanCentral DAST database.
Scan.Sessiontype	Identifies why there is a session in the database, such as crawl, attack, triggered macro, and so on.
Scan.Attacktype	Identifies what the sensor did in the request, such as cookie injection, query injection, and so on.

Column	Description
Scan.Checkid	The identification number of an Fortify DAST probe that checks for the existence of a specific vulnerability.
Scan.Attacksequence	Shows the order of requests sent by the audit engine. This information might be useful for debugging a specific engine.
Scan.Engine	Name of the audit engine that sent the request.
Scan.Attackparamdesc	Name of the parameter being attacked in the request.
Scan.Attackparamindex	Identifies a parameter by index instead of by name. This might be useful because not all parameters have names and in some applications names are duplicated. Index of the parameter. The index count starts at 0, so if your site has 10 cookies and the audit engine attacked the third one, then the parameter index of the attacked cookie will be 2.
Scan.Attackparamsubindex	When we break up something smaller than Post and Query and cookie, such as a JSON document.
Scan.Crawltype	Identifies the type of crawl, such as from script execution, forms submission, dynamically generated URLs, HREF, and so forth.
Scan.Attributename	Used for diagnostics to help identify the request source.
Scan.Format	Used for diagnostics to help identify the request source.
Scan.Linkkind	Used for diagnostics to help identify the request source.
Scan.Locations	Used for diagnostics to help identify the request source.
Scan.Source	Used for diagnostics to help identify the request source.

Column	Description
Scan.Nodename	Used for diagnostics to help identify the request source.

Working with Traffic

You can view the traffic generated during the scan on the Traffic tab, which includes the Traffic table and the HTTP, Parameters, and Steps tabs.

Tip: Remember that selecting a resource in the Site Tree filters the data to that resource in the Traffic table. For more information, see "Working with the Site Tree" on page 304.

Viewing the Request and Response

The HTTP tab includes the request and response session details for the selected vulnerability.

To view the request and response:

1. Select a session in the **TRAFFIC** table.
2. Click the **HTTP** tab.
   In the REQUEST area, the attack is highlighted. In the RESPONSE area, the vulnerability is highlighted.

Viewing Parameters

You can view the Type, Name, and Value for parameters used in a traffic session. The Parameters detail view displays a table with one record for each cookie or query string used in the traffic session.

A parameter can be one of the following:

- Cookie data
- A query string submitted as part of the URL in the HTTP request (or contained in another header)
- Data submitted using the Post method (such as `set_<parametername>`)

To view the parameter details for a session:

1. Select a session in the **TRAFFIC** table.
2. Click the **PARAMETERS** tab.
   The PARAMETERS table displays the parameters used in the selected session.

Viewing Steps

The Steps tab displays the route taken by the sensor to arrive at the session selected in the Traffic table. Beginning with the parent session (at the top of the list), the sequence reveals the subsequent URLs visited and provides details about the scan methodology.

To view the steps:

1. Select a session in the **TRAFFIC** table.
2. Click the **Steps** tab.

   The STEPS table displays the route taken by the sensor to arrive at the session selected.

To close the Steps tab, do one of the following:

- Press the **ESC** key.
- Click the **Steps** tab again.

Understanding the logs table

The Logs table displays the Fortify DAST sensor scan log for the selected scan.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

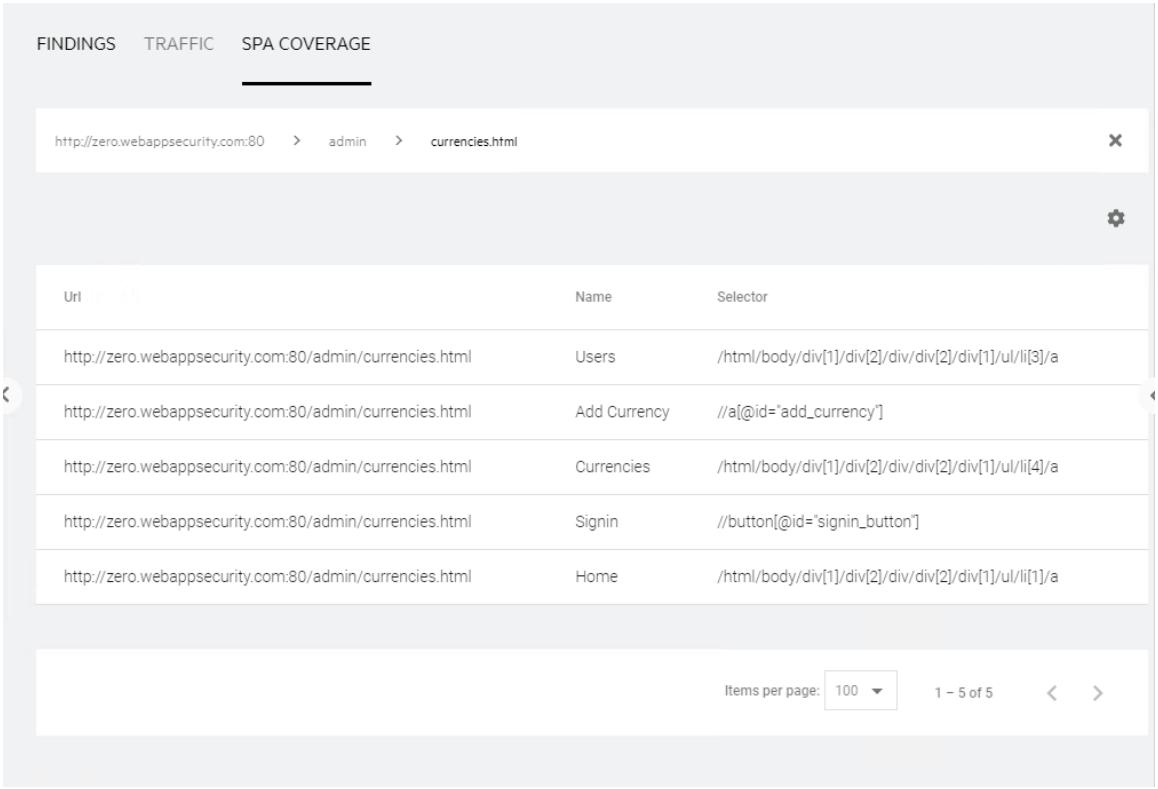
Available columns

The following table describes the available columns.

Column	Description
Entry Level	Specifies the severity of the log entry. Possible levels are Debug, Alert, Information, Warning, Error, or Critical.
Sequence	Indicates the sequential order in which the log entry was written.
Entry Time	Indicates the time at which the log entry was written.
Entry Type	Indicates the type of log entry, such as ScanCompleted, VerifyAuditComplete, VerifyAuditStart, LogMessageOccured, and so forth.
Message	Provides a text description for the log entry.
Is Active	Indicates that the issue that caused the log entry is active and still affecting the scan.

Understanding SPA Coverage

The single-page application (SPA) Coverage view is available only if the scan includes SPA events. This view displays the elements in the page that the crawler interacted with during the crawl. The SPA events are filtered based on what you select in the Site Tree.



The SPA Coverage view lists the URLs where the elements were discovered, along with the following additional information:

- **Name** – The visible text, symbol, link, HTML tag name, or other UI information related to the element.
- **Selector** – The XPath location of the element in the page. This is used to find and perform operations on the element.

For more information, see "Scanning single-page applications" on page 198.

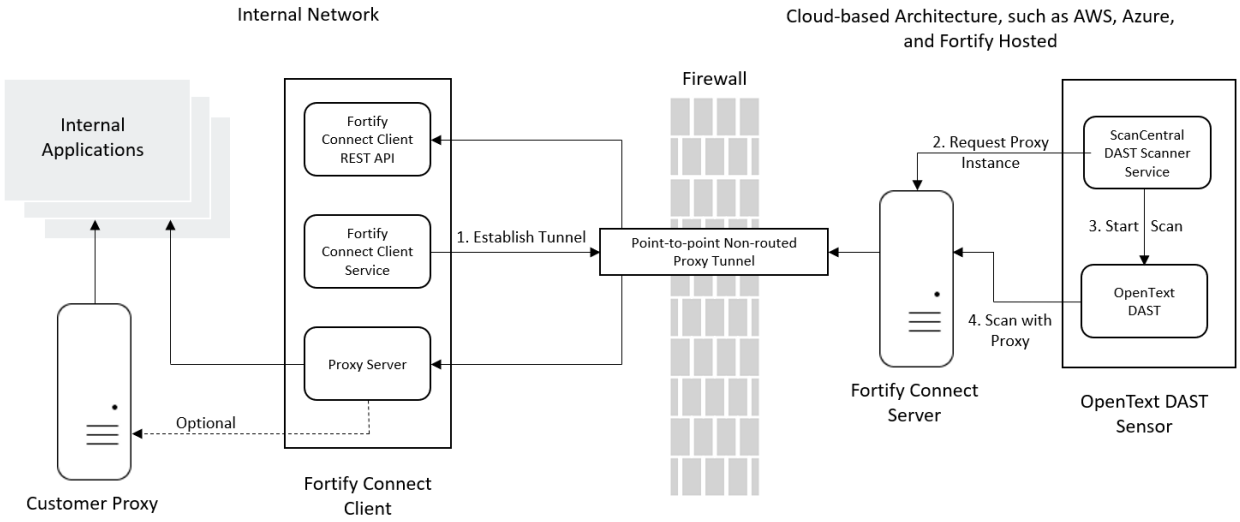
Chapter 7: Working with Fortify Connect for private application scanning

Normally, a scan of a private application–an application that is hidden behind a firewall–would be interrupted because the OpenText DAST (Fortify WebInspect) sensor cannot reach the application. Fortify Connect establishes a point-to-point non-routed proxy tunnel using SSH that enables you to perform scans of private applications from the cloud without exposing the application through your firewall. No other traffic can be routed over this connection. Fortify Connect uses non-standard ports, and the proxy tunnel is always encrypted and secure.

Scenario 1: OpenText DAST (Fortify WebInspect) sensor running in the cloud (remote mode)

This scenario applies when you are running the ScanCentral DAST containers in the cloud and have internal applications that need to be scanned, but are not accessible from outside of your internal network. If Fortify Connect is enabled and a Fortify Connect Client has been configured for the application, then when starting a scan the DAST scanner service requests a proxy instance from the Fortify Connect Client that is running in your internal network. After the connection is established and the proxy is available, the Fortify DAST sensor uses the proxy server associated with the connection to access internal application(s).

The following diagram illustrates how Fortify Connect works when all ScanCentral DAST components are running in the cloud.

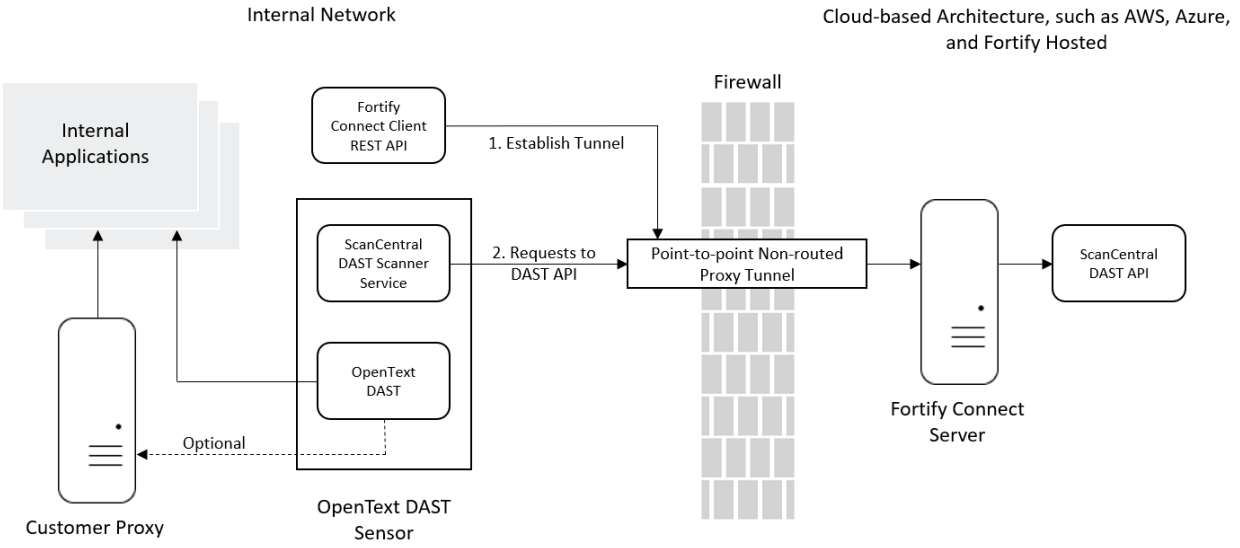


Note: It is not necessary to set up a Docker environment inside your network. The Fortify Connect client is an executable file that you can download and run on any machine. For more information, refer to the *OpenText™ Application Security Software System Requirements*.

Scenario 2: Fortify DAST sensor running on premises (local mode)

This scenario applies when you are running the Fortify DAST sensor inside your internal network and the ScanCentral DAST API container in the cloud and have internal applications that need to be scanned, but are not accessible from outside of your internal network. If Fortify Connect is enabled and a Fortify Connect client has been configured for the application, then when starting a scan the ScanCentral DAST scanner service establishes a connection to the Fortify Connect server instance. After the connection is established, any requests to the ScanCentral DAST API are tunneled through the connection.

The following diagram illustrates how Fortify Connect works when you have a Fortify DAST sensor running inside your network.



Fortify Connect client service

The Fortify Connect client is an executable that runs behind your firewall, establishes a secure proxy tunnel through the firewall, and connects to the Fortify Connect server running in the cloud.

When running in local mode, the ScanCentral DAST Scanner Service and Fortify Connect client must be running on the same machine.

Fortify Connect client REST API

The client executable includes an internal REST API for communicating with the Fortify DAST sensor.

Proxy server

The client executable starts a proxy server that traffic from the Fortify DAST sensor passes through to reach the internal application. Optionally, you can chain this proxy server to your own proxy server.

Fortify Connect server

The Fortify Connect server is a Linux container that is an SSH server. It enables the ScanCentral DAST API and Fortify DAST API to communicate with the Fortify Connect client API through the secure proxy tunnel. The image name is `scancentral-dast-fortifyconnect:26.4.ubi.9`.

Currently, you can run only one Fortify Connect server in your ScanCentral DAST environment. You can, however, run multiple Fortify Connect clients, allowing you to conduct multiple scans of internal applications simultaneously through the secure proxy tunnel.

Important! OpenText does not recommend running more than one scan at a time for the same application using Fortify Connect.

Configuring and using Fortify Connect

The following table describes the process for configuring Fortify Connect and using it to scan an internal application.

Stage	Description
1.	Configure Fortify Connect settings in the settings file used to configure your ScanCentral DAST environment. For more information, see "Fortify Connect server settings" on page 86.
2.	Configure a Fortify Connect client in the Fortify Connect page, assigning an internal application to the Fortify Connect client. For more information, see "Creating a Fortify Connect client" on page 327.

Stage	Description
3.	Download the executable file for the Fortify Connect Client. Run this client in your network behind your firewall. For more information, see "Downloading the start script" on page 328. The downloaded file is `StartFortifyConnectClient<ID>.tar.gz`, where `<ID>` is the ID of the Fortify Connect client.
4.	On a machine inside your network, unzip the `tar.gz` file . The packaged files are as follows: • `StartFortifyConnectClient_<ID>.sh` – a script to start the executable file. **Important!** The `StartFortifyConnectClient_<ID>.sh` file contains a placeholder named "`<currentdir>`" for the `--settingsfile` parameter. This value is automatically replaced with the directory from which the script is run. If the settings file is located in a different directory, the full path to the settings file must to be specified. • `FortifyConnectClientSettings_<ID>.json` – a settings file with the settings specified for your ScanCentral DAST environment. It includes information that the Fortify Connect client needs to connect to the Fortify Connect server.
5.	Edit the `FortifyConnectClientSettings_<ID>.json` file to configure certificate settings. See "Configuring certificate settings for Fortify Connect" on the next page.
6.	On a Linux machine inside your network, start the Fortify Connect client as follows: • At the terminal prompt, enter the following command: `./StartFortifyConnectClient_<ID>.sh` The client connects to the Fortify Connect server and establishes a port for the internal REST API.
7.	In ScanCentral DAST, you should see a running port showing a connection to the client. For more information, see "Understanding the Ports tab" on page 326.
8.	In ScanCentral DAST, do the following: 1. Configure scan settings for the internal application.

Stage	Description
	2. Start a scan of the internal application. For more information, see "Configuring a scan" on page 150. When an Fortify DAST sensor accepts the scan, it sends a request through the secure tunnel for a proxy instance for accessing the internal application. When the scan is complete, the proxy instance and the port used to access the proxy are shut down. The Fortify Connect client REST API port remains open.

Requirements for validating API definitions and saving settings

Be aware of the following requirements for validating an API definition or saving settings when Fortify Connect is enabled for the application:

- In Local mode, the ScanCentral DAST API must have access to the API definition URL.

  Important! If the API definition URL is inside your private network and the ScanCentral DAST API is in the cloud, then you must expose the API definition URL to the ScanCentral DAST API or use Remote mode.

- In Remote mode, the machine running the Fortify Connect client must have access to the API definition URL.

Requirements for running an API scan

Be aware of the following requirements for running an API scan when Fortify Connect is enabled for the application:

- In Local mode, the ScanCentral DAST Scanner Service must have access to the API definition URL.
- In Remote mode, the machine running the Fortify Connect client must have access to the API definition URL.

Configuring certificate settings for Fortify Connect

The Fortify Connect client no longer generates a self-signed certificate. You must extract and edit the `FortifyConnectClientSettings_{id}.json` file to configure the certificate

settings as described in this topic. Settings files from earlier versions will not work with Fortify Connect client 25.2.0.

General guidelines

Follow these guidelines when configuring certificate settings:

- Certificates should be created using OpenSSL or your tool of choice for certificates.
- Environment variables in the format of `"name__property__etc"` can be used in place of `appsettings.json`. Environment variables will be used with Docker containers.

Configuring TLS authentication

For TLS authentication, you must configure the Kestrel endpoints in the `FortifyConnectClientSettings_{id}.json` file. Follow these guidelines for the Kestrel settings:

- The `Endpoints` value can be any name as long as it is unique from other entries.
- The `Url` must use the `https` scheme.
- The `SslProtocols` must have `Tls12` and `Tls13`.
- The `Certificate` > `Path` must be the full path to the certificate. For example:

  `"/home/fortifyconnectsshuser/scdast/certificates/fortify-connect-api-certificate.pem"`
- The `Certificate` > `Password` is required only if the certificate requires a password.
- The `Certificate` > `KeyPath` is required only if the certificate file requires a key file. If needed, specify the full path. For example:

  `"/home/fortifyconnectsshuser/scdast/certificates/fortify-connect-api--key.key"`

  Otherwise remove or comment out the `KeyPath` line.

Configuring mTLS authentication

For mTLS authentication, you must configure the Kestrel endpoints described previously. In addition, you can use the `AdditionalCertificateAuthenticationSettings` to override system certificate authentication settings. The following table describes these settings.

Setting	Description
`Enabled`	If `true`, the additional certificate settings will be used. If `false`, the additional certificate settings will not be used.
`AllowedCertificateTypes`	Indicates the types of certificates accepted by the

Setting	Description
	authentication middleware. Valid values are: • `All` – Chained and self-signed certificates are allowed. • `Chained` – Only chained certificates are allowed. • `SelfSigned` – Only self-signed certificates are allowed.
`RevocationModeType`	Specifies conditions under which verification of certificates in the X509 chain should be conducted. Valid values are: • `NoCheck` – No revocation check is performed on the certificate. • `Online` – A revocation check is made using an online certificate revocation list (CRL). • `Offline` – A revocation check is made using a cached CRL.
`ChainTrustValidationModeType`	Indicates the method used to validate certificate chains. Valid values are: • `System` – Use the default (system) root trust. • `CustomRootTrust` – When this value is used, the CustomRootTrustDirectory and CustomRootTrustCertificates will be used instead of the default root trust. • `CustomRootTrustDirectory` – Specifies the directory wher3 certificates are stored. Any `.pem`, `.cer`, `.crt`, `.pfx` or `.p12` files in the specified directory will be loaded and used when validating the certificate(s). If the certificate requires a password or key file, you must explicitly declare those using the `CustomRootTrustCertificates` property. • `CustomRootTrustCertificates` – Specifies the password or key file for the certificate. Valid values are: ◦ The full path to the certificate file. ◦ The full path to the key file if required by

Setting	Description
	the certificate ◦ The certificate password if required by the certificate. This value can be encrypted or clear text.

Configuring certificate forwarding settings

For mTLS authentication, you can configure settings that are useful when a load balancer or proxy forwards the client certificate to the application. The following table describes these settings.

Setting	Description
`Enabled`	If `true`, the client certificate forwarding settings will be used. If `false`, the client certificate forwarding settings will not be used.
`CertificateHeader`	Indicates the name of the header containing the client certificate.
`UrlDecodeCertificate`	Indicates whether the client certificate is URL encoded. For example, NGINX will URL encode the client certificate. Options are `true` or `false`.

Accessing the Fortify Connect view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with Fortify Connect directly in Application Security.

Note: If you disabled Fortify Connect or left the Fortify Connect server settings null in the settings file for your ScanCentral DAST environment, then you will not be able to configure and use a Fortify Connect server and client.

To access the Fortify Connect view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Fortify Connect** .
   The Fortify Connect view appears.

User Role Determines Capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Fortify Connect view

The Fortify Connect view displays in a table the Fortify Connect clients that are configured in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information that are available for each client.

Column	Description
Id	Indicates the ID assigned to the client and stored in the ScanCentral DAST database upon creation. You can use the ID in conjunction with ScanCentral DAST API endpoints.
Name	Identifies the name of the client.
Description	Optionally, provides a description of the client.
Service Port	Specifies the port on which the client service and API run.
Fortify Connect Server External Host	Specifies the external IP address or host name for the Fortify Connect server in the internal network.
Fortify Connect Server External Port	Specifies the external port on which the Fortify Connect server will run for secure proxy connections in the internal network. The default port number is `2022`. **Important!** This port must be open in the firewall for the client to be able to connect to the server.
Fortify Connect Server Internal Host	Specifies the internal IP address or host name for the Fortify Connect server in the cloud.

Column	Description
Fortify Connect Server Internal Port	Specifies the internal port on which the Fortify Connect server will run for secure proxy connections in the cloud. The default port number is `2022`.
Fortify Connect Mode Type	Indicates the type of connection between the Fortify DAST sensor and the applications being scanned. Possible values are: • **Remote** – where the Fortify DAST sensor is running in the cloud and the application to be scanned is running in your internal network. • **Local** – where the Fortify DAST sensor is running in your internal network and the ScanCentral DAST API is running in the cloud. For more information about these scenarios, see "Working with Fortify Connect for private application scanning" on page 317.

Understanding the client detail panel

When you select an entry in the Fortify Connect view, the client detail panel appears. The detail panel displays the information from the Fortify Connect table for the selected client.

The detail panel enables you to download the start script that launches the client executable. The panel also lists the applications that are assigned to the client and provides options to edit and delete the selected client.

Understanding the Ports tab

The PORTS tab displays the same information that is displayed in the of the detail panel for the selected client, as well as the information described in the following table.

Item	Description
Id	Indicates the ID for the port connection. You can use the ID in conjunction with ScanCentral DAST API endpoints.
Start Proxy	Indicates whether a proxy instance for the port should be started. Possible values are **true** and **false**.
Status	Indicates the current status of the port. Possible values are:

Item	Description
	• **Queued** – The client port is queued but not currently running. • **Pending Start** – The service is trying to start the port. • **Running** –The client port is currently running. • **Failed** – The client port failed to start. • **Pending Delete** – A request has been received to delete the client port.

Creating a Fortify Connect client

When you create a Fortify Connect client, you can assign the client to specific internal applications. These assignments determine which internal applications can be accessed through the client.

To create a new client:

1. On the **Fortify Connect** page, click **+ FORTIFY CONNECT CLIENT**.
   The FORTIFY CONNECT CONFIGURATION dialog box opens with the Getting Started page in view.
2. Configure the following settings for the client:
   a. In the **Client Name** box, type a name for the client.
   b. In the **Client Description** box, type a useful description for the client.
   c. In the **Service Port** list, select the port on which the client service and API will run.

      Note: After creation, this setting cannot be edited.

   d. In the **Connection Mode** list, select a mode for the client. The modes are as follows:
      - **Remote** – where the Fortify DAST sensor is running in the cloud and the application to be scanned is running in your internal network.
      - **Local** – where the Fortify DAST sensor is running in your internal network and the ScanCentral DAST API is running in the cloud.

      Note: After creation, this setting cannot be edited.
3. Click **Application Selection** in the menu or click **NEXT**.
   The APPLICATIONS list appears.

   Note: Application selection does not apply to Fortify Connect in Local mode. Application selection is optional for Remote mode. However, if no applications are assigned to the Fortify Connect client, it will never be used.

4. Optionally, select one or more applications to add to the client.
   The applications are added to the APPLICATIONS SELECTED list.

   Important! If you select an application that is already assigned to another Fortify Connect client, the application will automatically be unassigned from the first client.

5. Click **Review** in the menu or click **NEXT**.
   The Review page appears.
6. Click **SAVE**.

Managing Fortify Connect clients

You can download the start script for a client executable, edit and delete clients, and refresh the clients list on the Fortify Connect view.

Downloading the start script

After you have configured a Fortify Connect client, you must download the `tar.gz` file that contains the client executable file and a start script to launch the executable inside your network.

To download the start script for a client from the Fortify Connect client list:

- Click **download** .

To download the start script from the client detail panel:

1. In the Fortify Connect list, select the client.
   The client detail panel appears.
2. Click **download start script** .

By default, the `tar.gz` file is downloaded to the folder on your local machine that is specified in your browser settings for downloads.

Editing a client

To edit a client:

1. In the Fortify Connect client list, do one of the following:
   - Click **Edit** .
   - Select the client to edit, and then click **EDIT** in the client detail panel.

   The FORTIFY CONNECT CONFIGURATION dialog box opens with the client settings visible.

2. To make edits, follow the procedure listed in "Creating a Fortify Connect client" on page 327.

Note: You cannot edit the **Service Port** and **Connection Mode** for an existing client.

Refreshing the Fortify Connect view

Generally, the changes that you make to the clients appear right away on the Fortify Connect view. However, if other users have access to the same clients, any changes they make will not be updated in your view. To see such changes, you can manually refresh the Fortify Connect view.

To refresh the Fortify Connect view:

- Click **REFRESH**.

Deleting a client

To delete a client, do one of the following:

1. In the Fortify Connect list, select the client to delete.
   The client detail panel appears.
2. Click **DELETE**.
   The DELETE FORTIFY CONNECT CLIENT dialog box opens.
3. Select the **Confirm deletion of Fortify Connect client** check box, and then click **OK**.

Managing client ports

You can view all client ports, close a port's connection, and refresh the client ports view on the Fortify Connect page.

Ports in local mode

Each Fortify Connect client starts a remote port that is used to access the internal API for the Fortify Connect client. In Local mode, an additional port is required to forward requests to the DAST API that is running in the cloud. Deleting either of these ports causes Fortify Connect to fail.

Viewing all client ports

If you have configured multiple Fortify Connect clients, you might want to view all client ports to see which port or ports are currently in use.

To view all client ports:

- On the Fortify Connect page, click **VIEW ALL CLIENT PORTS**.
  The FORTIFY CONNECT ALL PORTS dialog box appears.

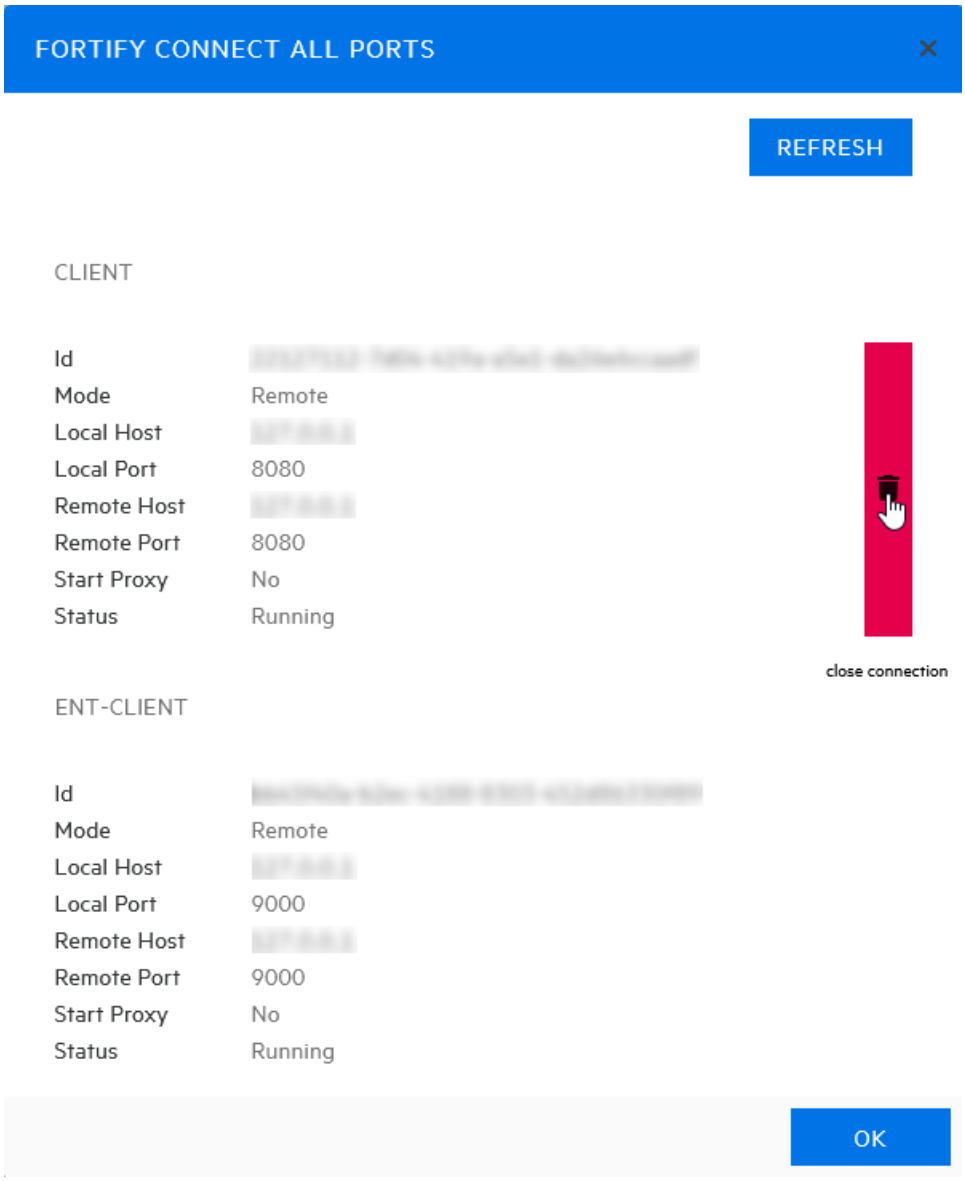
Tip: If you see "FAILED TO GET FORTIFY CONNECT CLIENT PORTS" listed for a client, it might mean that the client port is not currently running or that the service port has been deleted.

Closing a port's connection

Closing a port's connection You can close a port's connection on the FORTIFY CONNECT ALL PORTS dialog box or on the PORTS tab.

To close a connection on the FORTIFY CONNECT ALL PORTS dialog box:

1. Locate the port whose connection you want to close, and then click **close connection**.



A confirmation message appears.

2. Select the **Force Close Ports** check box, and then click **close connection**.
   The port is closed and the ports list is refreshed.

To close a connection on the PORTS tab:

1. Click **close connection**.
   A confirmation message appears.
2. Select the **Force Close Ports** check box, and then click **close connection**.
   The port is closed and the PORTS tab is refreshed.

Refreshing the client ports

Generally, the changes that you make to the client ports appear right away on the FORTIFY CONNECT ALL PORTS dialog box or on the PORTS tab. However, if other users have access to the same clients, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the client ports:

- On the **FORTIFY CONNECT ALL PORTS** dialog box or **PORTS** tab, click **REFRESH**.

Chapter 8: Working with sensors, sensor pools, and auto scale job templates

You can view and manage the ScanCentral DAST sensors in your environment as well as the sensor pools that handle sensor licensing and determine which applications each sensor can scan. Depending on your user role and permissions in Application Security, you can also work with auto scale job templates. The following pages describe managing sensors, sensor pools, and auto scale job templates.

Working with sensors

You can view all of the sensors that are stored in the ScanCentral DAST database in the Sensors view. You can view a sensor's status and whether it is enabled, as well as other details, in the sensor detail panel. From the sensor detail panel, you can also enable or disable sensors.

Accessing the ScanCentral DAST Sensors view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with ScanCentral DAST sensors directly in Application Security.

To access the ScanCentral DAST Sensors in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Sensors**.
   The Sensors view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Sensors view

The Sensors view displays in a table all sensors that are stored in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each sensor.

Column	Description
Sensor ID	Indicates the integer ID for the sensor in the ScanCentral DAST database.
Name	Displays the value specified as `--hostname` in the Docker run command. **Note:** If the host name is not set or returns an empty value for any reason, then ScanCentral DAST uses the internal Docker container ID. The value is automatically truncated to 15 characters and is displayed in upper case.
Description	Displays the value specified as the `ScannerDescription` environment variable in the Docker run command or in the `appsettings.json` file.
Pool	Identifies the pool to which the sensor belongs. **Note:** If the pool has been configured for sensor auto scaling but has been deleted, then "(deleted)" is appended to the pool name until all scaled sensors in the pool have completed their scans and been shut down. For more information, see "Understanding sensor auto scaling" on page 343.
Sensor Type	Indicates one of the following sensor types: • **Fixed** – A sensor that is configured outside of Kubernetes or is in a pool that does not allow auto-scaling. • **Auto-Scaled** – A replicated instance of a sensor that is installed in your Kubernetes environment and is in a pool that allows auto-scaling. For more information, see "Configuring sensor auto scaling" on page 342.
Current Scan ID	Indicates the integer ID in the ScanCentral DAST database for the scan that the sensor is actively conducting. **Note:** Each scan is assigned an integer ID when it is added to the ScanCentral DAST database.

Column	Description
Sensor Enabled	Indicates whether the sensor is enabled to perform scans. Possible values are **Enabled** and **Disabled**.
Status	Indicates the current status of the sensor. Possible values are **Online** and **Offline**.

Excluding or including auto-scaled sensors

In addition to the table preferences described in "Working with tables" on page 136, you can also exclude or include the display of auto-scaled sensors in the view.

To exclude or include auto-scaled sensors:

1. Click **Table Preferences** ⚙.
   The table preferences panel opens.
2. Do one of the following:
   - To exclude auto-scaled sensors, slide the **Include auto-scaled sensors** toggle to the disabled position.
   - To include auto-scaled sensors, slide the **Include auto-scaled sensors** toggle to the enabled position.
3. Click **OK**.

Understanding the sensor detail panel

When you select a sensor in the Sensors view, the sensor detail panel appears. The sensor details show the sensor's status and whether is it enabled.

The detail panel displays the same information that is displayed in the Sensors view for the selected sensor, as well as the information described in the following table.

Item	Description
IP Address	Identifies the IP address assigned to the sensor when the image was started.
Pool	Identifies the pool to which the sensor belongs.
Current Scan ID	Indicates the integer ID in the ScanCentral DAST database for the scan that the sensor is actively conducting. **Note:** Each scan is assigned an integer ID when it is added to the ScanCentral DAST database.

Item	Description
Last Connect	Indicates the last time the sensor sent an update on its status to the scanner service.
Operating System	Indicates the operating system of the VM or machine that is running the Docker container.
Version	Indicates the operating system version of the VM or machine that is running the Docker container.
Application Version	Indicates the version of ScanCentral DAST Sensor Service.
WebInspect Version	Indicates the version of OpenText DAST (Fortify WebInspect) being used to conduct scans.

Enabling or disabling sensors

The Sensors view shows all sensors that are stored in the ScanCentral DAST database. Depending on your permissions in Application Security, you can enable and disable the sensors in the view.

Facts about disabled sensors

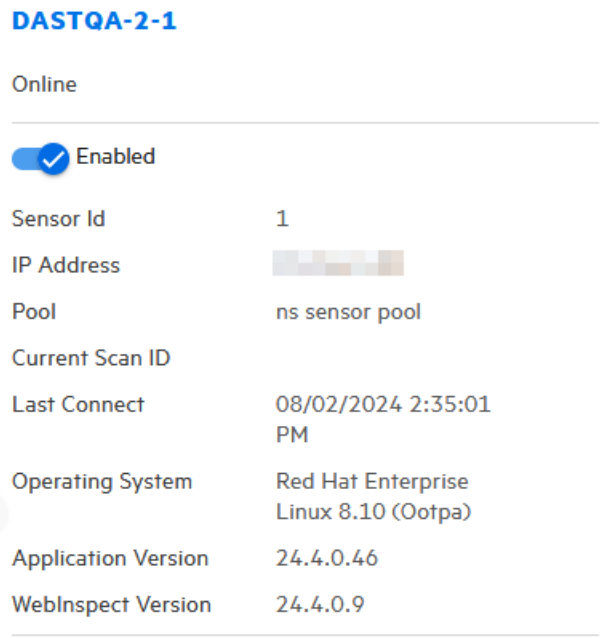
You should understand the following facts that apply to disabling a sensor:

- If a sensor is disabled, it is still online but cannot process any new scans.
- If a sensor is currently running a scan and you disable the sensor, the scan that is running will finish and then the sensor will not process any more scans until it is enabled again.

Enabling or disabling a sensor

To enable or disable a sensor:

1. In the Sensors view, select the sensor to enable or disable.
   The sensor details panel appears.



2. Do one of the following:
   - To enable the sensor, toggle the switch to **Enabled**.
   - To disable the sensor, toggle the switch to **Disabled**.

Working with sensor pools

A sensor pool provides a way for you to license your ScanCentral DAST sensors with a specific license pool in the Fortify License and Infrastructure Manager (LIM) and designate which applications each sensor can scan. You can also configure sensor auto scaling for a sensor pool.

Accessing the ScanCentral DAST Sensor Pools view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with ScanCentral DAST sensor pools directly in Application Security.

To access the ScanCentral DAST sensor pools view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Sensor Pools**.
   The Sensor Pools view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Sensor Pools view

The Sensor Pools view displays in a table the ScanCentral DAST sensor pools that are configured in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information that are available for each pool.

Column	Description
Name	Identifies the name of the sensor pool.
Description	Provides a description of the pool.
LIM Pool	Identifies the license pool that is configured in the LIM.
Default	Indicates whether the pool is designated as the default pool. Possible values are **Yes** or **No**. If you spin up a new sensor and do not assign it to a pool, the sensor will be assigned to the default pool automatically.
2FA Server	Indicates the name of the two-factor authentication server that is configured for the pool. For more information, see "Working with two-factor authentication" on page 425.
Sensor Scaling	Indicates whether sensor auto scaling is enabled for the pool. Possible values are **Enabled** or **Disabled**.
Sensor Scaling Host	Identifies the host URL for the Kubernetes environment that was configured for sensor auto scaling.
Sensor Scaling Namespace	Identifies the Kubernetes namespace that was configured for sensor auto scaling.
Sensor	Specifies the maximum number of sensor replicas that can be run in

Column	Description
Scaling Max Replicas	the pool in the Kubernetes environment.
Sensor Scaling Template Name	Specifies the job template that manages Kubernetes pods for automatic sensor scaling. For more information, see "Working with auto scale job templates" on page 345.

Note: The **Sensor Scaling Host**, **Sensor Scaling Namespace**, and **Sensor Scaling Template Name** columns are not displayed when **Sensor Auto Scaling** has been configured using the CLI. See "Database settings" on page 61 for more information on turning on Sensor Auto Scaling with the Configuration Tool CLI.

Understanding the pool detail panel

When you select a pool in the Sensor Pools view, the pool detail panel appears. If the pool you select is the default pool, it will be identified as DEFAULT at the top of the pool detail panel. Otherwise, an option is available to make the pool the default pool. For more information, see "Managing sensor pools" on page 343.

The detail panel displays the same information that is displayed in the Sensor Pools view for the selected pool, as well as the information described in the following table.

Item	Description
ASSIGNED APPLICATIONS	Lists the applications that sensors in the pool can scan.
ASSIGNED SENSORS	Lists the sensors that are assigned to the pool.

Creating a ScanCentral DAST sensor pool

When you create a ScanCentral DAST sensor pool, you can assign a single sensor or group of sensors to specific applications. These assignments determine which sensors can scan each application in your environment.

To create a new sensor pool:

1. On the **Sensor Pools** page, click **+ NEW POOL**.
   The SENSOR POOL - CREATE dialog box opens with the Getting Started page in view.
2. In the **Name** box, type a name for the pool.

3. In the **Description** box, type a description for the pool.
4. In the **Pool** list, select the LIM license pool for licensing the sensors in the pool.
5. In the **Password** box, type the password associated with the LIM license pool.
6. To verify that you can connect to the LIM with the license pool and password, click **VALIDATE**.
7. Click **Sensors** in the menu or click **NEXT**.
   The SENSORS list appears.
8. Select one or more sensors to add to the pool.

   Important! If you are creating a pool to allow sensor auto scaling, make sure that you select sensors that managed in Kubernetes.

   The sensors are added to the SENSORS SELECTED list.
9. Click **Application Selection** in the menu or click **NEXT**.
   The APPLICATIONS list appears.
10. Select one or more applications to add to the pool.
    The applications are added to the APPLICATIONS SELECTED list.
11. Click **Sensor Scaling** in the menu or click **NEXT**.
    The SENSOR AUTO SCALING settings appear.
12. Slide the **SENSOR AUTO SCALING** toggle to **Enabled**.
13. In the **Maximum Replicas** list, enter the maximum number of sensor replicas that can be run in this pool in the Kubernetes environment.

    Note: The minimum number of replicas allowed is 1.

    For more information on Sensor Auto Scaling and replicas, see "Configuring sensor auto scaling" on page 342.
14. Click **Review** in the menu or click **NEXT**.
    Review your sensor pool settings.
15. Click **SAVE**.
    The pool is added to the Sensor Pools list.

Configuring a WISE client

To connect the DAST scanner to a StatefulSet WISE client, you must use a Kubernetes WISE headless service domain name and namespace as follows:

```
ws://<wise-headless-service-name>.<namespace>:9442
```

This is known as the WISE address. Examples of WISE addresses are as follows:

- `ws://wise-sset.default:9442`
- `ws://wise.default:9442`

The following paragraphs provide sample code for connecting the DAST scanner to a StatefulSet WISE client.

WISE StatefulSet YAML file

The following sample shows YAML configuration for the simplest WISE StatefulSet installation.

```
# Deployment for wise image:
apiVersion: apps/v1
kind: StatefulSet
metadata:
  name: wise-sset
  labels:
    app: wise-sset
spec:
  replicas: 3
  minReadySeconds: 10 # default 0
  serviceName: "wise-sset"
  selector:
    matchLabels:
      app: wise-sset
  template:
    metadata:
      labels:
        app: wise-sset
    spec:
      terminationGracePeriodSeconds: 60
      nodeSelector:
        kubernetes.io/os: linux
        kubernetes.io/arch: amd64
      containers:
      - name: wise-sset
        image: "fortifydocker/wise:26.4.ubuntu.2204"
        ports:
        - containerPort: 9442
        lifecycle:
          preStop:
            exec:
              command: ["/bin/sh","-c","/etc/wise/prestop.sh"]
```

WISE headless service YAML file

The following sample shows YAML configuration for the simplest WISE headless service installation.

```
apiVersion: v1
kind: Service
metadata:
  name: wise-sset
  labels:
    app: wise-sset
spec:
  ports:
  - name: ws
    port: 9442
    protocol: TCP
    targetPort: 9442
  clusterIP: None
  selector:
    app: wise-sset
```

WISE StatefulSet scaling

You can adjust existing manual horizontal scaling by using the following command:

```
k scale statefulset wise-sset --replicas 3
```

For automatic horizontal scaling, use the Kubernetes HorizontalPodAutoscaler. Refer to the Kubernetes documentation for more information.

Configuring sensor auto scaling

Important facts about sensor auto scaling

Before you begin, be aware of the following facts:

- When sensor auto scaling is configured, the ScanCentral DAST Global Service manages the scaling of sensors within your Kubernetes environment.
- When configuring sensor auto scaling, the job namespace must already exist in Kubernetes. The access token must have the ability to list, get, create, and delete jobs, and list pods in the job namespace.

Understanding sensor auto scaling

When creating or editing a sensor pool, you can configure sensor auto scaling for the pool. Sensor auto scaling applies only to sensors that are installed in your Kubernetes environment. These sensors are known as “scaled" or "scalable” sensors.

When sensor auto scaling is enabled for the sensor pool and a scan is queued, the ScanCentral DAST Global Service checks the number of running instances of a sensor. If the number of running instances is less than the maximum replica specified in the settings for sensor auto scaling, then the ScanCentral DAST Global Service will create a Kubernetes job that starts the container, runs the scan, and shuts down the container.

If a sensor is in the sensor pool but has been configured outside of Kubernetes, and the sensor is online and available, ScanCentral DAST will use this sensor rather than sensor auto scaling. Sensors that are configured outside of Kubernetes are known as “fixed” sensors.

Note: When the scannerAutoScalingRestrictions setting is set to true using the Configuration Tool CLI, the following are not displayed in sensor pool information: **Sensor Scaling Host**, **Sensor Scaling Namespace**, and **Sensor Scaling Template Name**. For more information, see "Understanding the Sensor Pools view" on page 338 and "Database settings" on page 61

Important information about privileges for service account tokens

Configuring sensor auto scaling requires the use of an access token for the Kubernetes environment. Ensure that the token does not have rights to create namespaces. Allowing the creation of namespaces might create a privilege escalation vulnerability in Kubernetes.

Managing sensor pools

You can edit and delete pools, refresh the pools list, and change the default pool on the Sensor Pools page.

Important! OpenText recommends that scan queues be empty before modifying sensors pools.

Facts about managing sensor pools

You should understand the following facts about managing sensor pools:

- You cannot delete the default sensor pool.
- If you delete a sensor pool, all sensors and applications assigned to that pool will be reassigned to the default pool.

Editing a sensor pool

To edit a sensor pool:

1. In the Sensor Pools list, select the pool to edit.
   The pool detail panel appears.
2. Click **EDIT**.
   The pool settings appear in a dialog box that is similar to the CREATE NEW POOL dialog box.
3. To make edits, follow the procedure listed in "Creating a ScanCentral DAST sensor pool" on page 339.

Refreshing the Sensor Pools View

Generally, the changes that you make to the sensor pools appear right away on the Sensor Pools view. However, if other users have access to the same sensor pools, any changes they make will not be updated in your view. To see such changes, you can manually refresh the pools view.

To refresh the Sensor Pools view:

- Click **REFRESH**.

Deleting a sensor pool

To delete a sensor pool, do one of the following:

- Select one or more check boxes for pools in the Sensor Pools view, and then click **DELETE** at the bottom of the table.
- Select a pool to view the pool details, and then click **DELETE** at the bottom of the pool details panel.

Tip: You cannot delete the default sensor pool.

Changing the default sensor pool

The first pool you configure becomes the default pool. If you have only one pool configured, it will always be the default pool. If you have multiple pools configured, however, you can change the default pool at any time.

To change the default pool:

- Select a pool to view the pool details, and then select **Make default** in the pool details panel.

Working with auto scale job templates

Job templates are Kubernetes configuration YAML files that contain template information for Kubernetes jobs. ScanCentral DAST uses auto scale job templates to automatically start sensors to perform scans and then stop the sensors upon scan completion.

When an ScanCentral DAST environment is created, default auto scale job templates are created and stored in the ScanCentral DAST database. For Linux® containers, two default template versions are created: one for SQLExpress and one for PostgreSQL. The template file name specifies the database for which it applies. For example, `Linux WebInspect 26.4 SQLExpress` and `Linux WebInspect 26.4 PostgreSQL`.

You can view and manage auto scale job templates on the Auto Scale Job Templates page.

Accessing the Auto Scale Job Templates view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with auto scale job templates directly in Application Security.

To access the Auto Scale Job Templates view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. Select **Auto Scale Job Templates** from the menu.
   The Auto Scale Job Templates view appears.

Note: Auto Scale Job Templates might not be available in your view of ScanCentral DAST if it was turned off in the settings file.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to auto scale job templates may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Understanding the auto scale job templates view

The Auto Scale Job Templates view table displays the auto scale job templates that are configured in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information that are available for each job template.

Column	Description
Name	Identifies the name of the job template.
Description	Provides a description of the job template.

Managing auto scale job templates

You can import job templates, edit and delete job templates, and refresh the job templates table on the Auto Scale Job Templates view.

Importing a job template

You can import a new or edited auto scale job template to the ScanCentral DAST database.

To import a job template:

1. On the **Auto Scale Job Templates** page, click **+ JOB TEMPLATE**.
   The SCANNER AUTO SCALE JOB TEMPLATE dialog box opens.
2. Click **IMPORT**.
   A standard Windows file selection dialog box opens.
3. Locate and select the `YML` or `YAML` file, and then click **Open**.
4. In the **Name** box, enter a job template name. This is the name that will appear in the Sensor Pools list when the job template is assigned to the pool.
5. Optionally, in the **Description** box, type a meaningful description of the job template.
6. Click **OK**.

Editing a job template

You can download and edit a default template in your editor of choice, and then import the edited version back to the ScanCentral DAST database.

Caution! Do not edit file content that is marked "`# DO NOT EDIT. Required for SC DAST.`" Doing so will invalidate the file.

Use the following process to edit a job template.

Stage	Description
1.	In the **Auto Scale Job Template** view, click the download icon (⭳) for the job template to edit.

Stage	Description
2.	Edit the downloaded file and save the changes in your editor of choice.
3.	Do the following: 1. In the **Auto Scale Job Templates** view, select the check box for the job template to edit. 2. Click **EDIT**. The SCANNER AUTO SCALE JOB TEMPLATE dialog box opens. 3. Follow steps 2 through 7 of the procedure in "Importing a job template" on the previous page.

Deleting a job template

You can delete only one job template at a time, and you must select a replacement job template for the affected sensor pools to use. Also, you must have at least one job template.

To delete a job template:

1. In the **Auto Scale Job Templates** view, select the job template to delete.
2. Click **DELETE**.
   The DELETE SENSOR AUTO SCALE JOB TEMPLATE dialog box opens requesting a confirmation.
3. Select the **I'm sure. Select replacement template.** check box.
4. In the **Replacement Job Template** list, select a job template for the affected sensor pools to use.
5. Click **DELETE**.

Refreshing the Auto Scale Job Templates view

Generally, the changes that you make to the job templates appear right away on the Auto Scale Job Templates view. However, if other users have access to the same job templates, any changes they make will not be updated in your view. To see such changes, you can manually refresh the job templates view.

To see an updated job templates view:

- Click **REFRESH**.

Chapter 9: Working with scan settings

You can view the scan settings that are available in the ScanCentral DAST database in the Settings List view. You can view the application, version, and URL that are configured for each settings file, as well as other details, in the settings detail panel. From the Settings List view, you can also configure new scan settings, edit existing settings, download settings, and delete settings.

Accessing the ScanCentral DAST scan Settings List view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with DAST scan settings directly in Application Security.

To access the ScanCentral DAST scan Settings List view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Settings List**.
   The Settings List view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Settings List view

The Settings List view displays in a table the scan settings that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

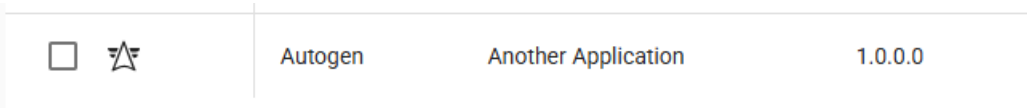
The following table describes the columns of information provided for each settings file.

Column	Description
Name	Indicates the name of the settings file. This is the name that was assigned at the time the settings were configured and saved.
Application	Indicates the application for which the settings apply.
Version	Indicates the version for which the settings apply.
Scan Type	Indicates the type of scan to be conducted using the settings. Types are: • **Standard Scan** • **Workflow-driven Scan** • **API Scan**
Modified	Indicates the date and time that the settings were created, or if edited, the last date and time that the settings were changed.
DAST Settings Status	Indicates the status of the process for generating composite settings that you can download and use in OpenText DAST (Fortify WebInspect). Statuses are: • **Not Available** - The process has not yet created the settings, so composite settings are not available for use in Fortify DAST. • **Pending** - The creation process has started. • **Available** - Composite settings are ready for download and use in Fortify DAST. • **Failed** - Composite settings were not created. Check the settings LOGS tab for specific details. • **Pending retry create** - A user has selected the retry create option and the process is underway. **Note:** By default, Fortify DAST uses XML settings. To use composite settings in Fortify DAST, enable the "Use Composite Scan Settings" option in **Application Settings > General**. If XML settings are imported, they must be converted to composite settings. The following statuses apply to imported XML settings: • **Needs conversion** - XML settings have not been converted to composite settings. • **Pending conversion** - The conversion process has started.

Column	Description
	• **Conversion failed** - The conversion process failed and composite settings were not created. Check the settings LOGS tab for specific details. For more information, see "Converting settings" on page 352.
DAST Settings Status Update	Indicates the date and time that the DAST Settings Status was last updated.
CICD Identifier	Identifies the settings identifier GUID that was assigned to the settings.

Pending Aviator jobs

When an item in the Scans view, Settings List view, or Base Settings view has a pending Aviator job, an **Aviator Macro Autogen** icon ( ) appears to the right of the item's selection check box.



Selecting the item opens the details panel, where Aviator-specific actions are available. For more information, see "Managing Aviator jobs" on page 479.

Understanding the scan settings detail panel

When you click a settings file in the Settings List view, the settings detail panel appears to the right. The application, version, and URL that are configured in the scan settings are listed at the top of the panel.

The detail panel displays the same information that is displayed in the Settings List view for the selected settings, as well as the information described in the following table.

Item	Description
Created	Indicates the date and time that the settings were saved.
Policy	Identifies the dynamic policy to be used to conduct the scan.
User Agent	Indicates one of the following user agents: • **Default**

Item	Description
	• **Custom** • **Google Chrome (Windows)** • **Safari (macOS)** • **Microsoft Edge (Windows)** • **Safari (iOS)** • **Google Chrome (Android)** • **Googlebot 2.1** • **Bingbot** • **Yahoo! Slurp** • **Safari (iPadOS)** **Note:** Default uses the user agent that is defined in Fortify DAST.
Login Macro	If applicable, indicates the file name of the login macro specified in the settings.
Has Network Auth	Indicates whether network authentication is specified in the settings. Possible values are **Yes** and **No**.
Allowed Hosts	If applicable, lists the first (or only) allowed host from the settings file. If the settings include more than one allowed host, a plus sign and number indicate the number of additional allowed hosts. **Tip:** To view the additional allowed hosts, click **EDIT**.
SPA Option	Indicates how SPA support is configured in the settings.
Traffic Monitor	Indicates whether the Traffic Monitor is enabled in the settings. Possible values are **Enabled** and **Disabled**.
Submit for Triage	Indicates whether a scan run from these settings is uploaded to Application Security upon completion. Possible values are **Yes** and **No**.
SETTINGS IDENTIFIER	Indicates the settings identifier GUID that was assigned to the settings.

Understanding the settings LOGS tab

ScanCentral DAST records Fortify DAST sensor logs that are displayed in the LOGS tab of the detail panel. The sensor logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with scan settings.

To update the entries, click **REFRESH**.

Managing scan settings

You can configure new scan settings, edit existing settings, convert ScanCentral DAST settings for use in Fortify DAST, download settings, and delete settings from the Settings List view.

Creating new settings

You can access the Settings Configuration wizard from the Settings List view and create new settings.

To create new settings:

- Click **+ NEW SETTINGS**.
  The Settings Configuration wizard opens.

Editing settings

You can access the Settings Configuration wizard from the settings detail panel and edit settings.

To edit settings:

1. In the **Settings List** view, select the settings to edit.
   The settings detail panel appears.
2. In the settings detail panel, click **EDIT**.
   The Settings Configuration wizard opens pre-populated with the selected scan settings.

For more information, see "Editing settings that need to be converted" on the next page.

Converting settings

ScanCentral DAST uses composite settings, which consist of a JSON version of the scan settings packaged in a ZIP file with any binary files required for the scan, such as macros, client certificates, custom policies, and so forth. When you import a scan from an earlier version of ScanCentral DAST or Fortify DAST, ScanCentral DAST automatically

converts the settings to composite settings. When you create and save settings in ScanCentral DAST, it automatically creates composite settings that you can download and use in Fortify DAST.

The conversion status is displayed in the Settings List view. If the settings have not been converted, you can convert them in the Settings List view. For more information on the conversion statuses, see "DAST Settings Status" in "Understanding the Settings List view" on page 348

To convert settings:

- Click **convert** for the settings you want to convert.

  Tip: If the conversion is not successful, a **retry create** icon appears. Use this icon to attempt to create the settings again.

Editing settings that need to be converted

For settings that have a **DAST Settings Status** of **Needs conversion** or **Conversion failed**, the **CONVERT SETTINGS** button is displayed rather than the **EDIT** button in the settings detail panel. You must convert these settings before you can edit them.

To convert the settings:

- Click **CONVERT SETTINGS**.

  After conversion, the **EDIT** button is available.

Note: If you click **RUN** in the settings detail panel without converting the settings, a message appears in the Run Scan dialog advising that the scan settings will be converted before the scan is run. Clicking the **OK** button in the Run Scan dialog starts the conversion process and queues the scan to run.

Downloading settings

You can download settings from the ScanCentral DAST database to your local machine.

Note: The download option may not be immediately available for newly created settings. The Settings Configuration wizard uses the Fortify DAST API to create the settings file. In some environments and situations, it might take several seconds to several minutes for the API to complete the process.

To download settings:

- Click **download** for the settings you want to download.

  By default, the file is downloaded to the folder on your local machine that is specified in your browser settings for downloads.

Caution! Fortify DAST supports only Standard scan settings that are downloaded from ScanCentral DAST. Other types of scan settings may cause undesirable results in Fortify DAST.

Deleting settings

To delete settings:

1. Do one of the following:
   - Select one or more check boxes for settings in the Settings List view, and then click **DELETE** at the bottom of the table.
   - Select the settings in the Settings List view to view the details, and then click **DELETE** at the bottom of the settings detail panel.

   If the settings have dependencies, such as scheduled scans, a DELETE ERROR dialog box opens. In this case, you must resolve the dependencies before you can delete the settings.
2. To aid in resolving dependencies, in the **DELETE ERROR** dialog box, click **Copy list of dependencies**.
   A JSON string of the error summary is copied to the clipboard.

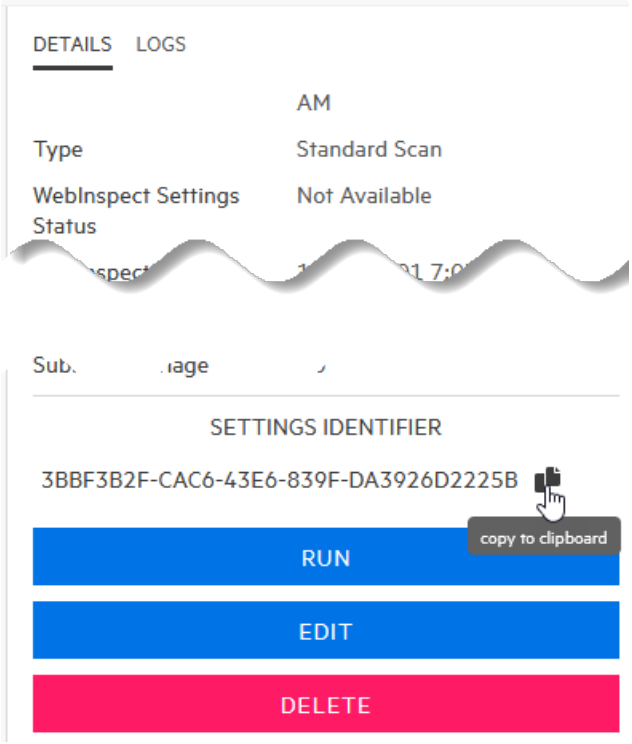
Copying the Settings ID for use in the API

You can copy the settings identifier and use it to conduct a scan by way of the Application Security API.

To copy the settings identifier:

1. In the **Settings List** view, select the settings to copy.
   The settings detail panel appears.

2. In the settings detail panel, click **copy to clipboard** as shown below.



The scan settings identifier is copied to the clipboard.

Chapter 10: Working with scan schedules

You can view all of the scan schedules that are available in the ScanCentral DAST database in the Scan Schedules view. You can also configure a new scan schedule, edit an existing schedule, enable or disable schedules, and delete schedules. You can view whether a schedule is enabled, as well as other details, in the schedule detail panel. From the schedule detail panel, you can also enable or disable schedules.

Accessing the ScanCentral DAST Scan Schedules view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with ScanCentral DAST scan schedules directly in Application Security.

To access the ScanCentral DAST Scan Schedules view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Scan Schedules**.
   The Scan Schedules view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Scan Schedules view

The Scan Schedules view displays in a table the scan schedules that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each schedule.

Column	Description
Application	Indicates the application for the scheduled scan.
Version	Indicates the version for the scheduled scan.
Name	Indicates the name of the schedule as assigned in the SETTINGS CONFIGURATION wizard.
Scan Settings	Indicates the name of the settings file that is used to conduct the scan.
Recurrence Type	Indicates how often the scheduled scan is run: **Daily**, **Weekly**, **Monthly**, or **Yearly**.
Last Occurrence	Indicates the last date and time that the scheduled scan ran.
Next Occurrence	Indicates the next date and time that the scheduled scan will be run.
Schedule Enabled	Indicates whether the schedule is enabled. Possible values are **Enabled** and **Disabled**.
CICD Identifier	Identifies the settings identifier GUID that was assigned to the settings.

Understanding the schedule detail panel

When you click a scan schedule in the Scan Schedules view, the schedule detail panel appears to the right. The detail panel displays the same information that is displayed in the Scan Schedules view for the selected schedule, as well as the information described in the following table.

Item	Description
Start Date	Indicates the initial date and time that the schedule ran a scan.
End Date	Indicates the last date and time that the schedule will run a scan, based on the number of occurrences or actual date that was configured in the Settings Configuration wizard.

Copying the settings identifier GUID

After saving the settings, the GUID in the **Settings Identifier** field provides a unique identifier for the settings.

Note: This GUID is also known as the CICD Identifier.

To copy the GUID:

- Click **copy to clipboard**.

Understanding the schedule LOGS tab

ScanCentral DAST records Fortify DAST sensor logs that are displayed in the LOGS tab of the detail panel. The sensor logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with scan schedules.

To update the entries, click **REFRESH**.

Managing schedules

You can configure a new scan schedule, edit an existing schedule, enable or disable schedules, and delete schedules from the Scan Schedules view.

Creating a new schedule

You can configure a new schedule from an existing template saved in Application Security or in a file.

To configure a new schedule:

1. On the Scan Schedules view, click **+ NEW SCHEDULE**.
   The SCAN SCHEDULE wizard opens.
2. In the **APPLICATIONS** area, select an application from the application **Name** list.

   Tip: To search for an application, type the application name in the **Application** box.

   The APPLICATION VERSIONS area appears.
3. In the **APPLICATION VERSIONS** area, select a version from the application version **Name** list.

   Tip: To search for an application version, type the application version name in the **Application version** box.

   The GETTING STARTED area appears with a START list that provides options for creating new settings or editing existing settings. A RECENT list also appears, displaying recently-opened scan settings for the specified application and version.

4. Do one of the following:
   - To use a template from Application Security, select **Open from SSC** in the **START** list, and then click **NEXT**.
   - To use a template saved to a file, select **Open file** in the **START** list, and then click **NEXT**.
   - To use a recently opened template, select a template under **RECENT**.

   The SCAN SCHEDULE dialog box opens.
5. Type a name for the scheduled scan in the **Name** box.
6. Enter a date for the scan to run in the **Start Date** box.

   Tip: To select a date from the calendar, click the **calendar** button.
7. Enter a time for the scan to start in the **Start Time** box.

   Note: The schedule uses the time zone from your browser.
8. To schedule a recurring scan, in the **Pattern** section specify how often to run the scan according to the following table.

To run...	Then...
Daily	a. Select **DAILY**. b. Select a recurrence in the **Occur every ___ day** box.
Weekly	a. Select **WEEKLY**. b. Select a recurrence in the **Occur every ___ week** box. c. Select the days to run each week.
Monthly	a. Select **MONTHLY**. b. Select a recurrence in the **Occur every ___ month** box. c. Do one of the following: ◦ Select **Occur on day** and enter a date in the box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list and a day from the **Day** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.
Yearly	a. Select **YEARLY**. b. Do one of the following: ◦ Select **Occur on**, and then select a month from the **Month** list

To run...	Then...
	and enter a date in the **Day** box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list, a day from the **Day** list, and a month from the **Month** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.

9. Under **Range**, do one of the following:
   - To leave the recurrence open ended, select **Never ends**.
   - To set an end date, select **Ends by**, and then enter an end date in the **End Date** box or enter the number of occurrences after which to end in the **occurrence** box.

     Note: Entering data into the **End Date** box automatically updates the **occurrence** box, and conversely.
10. Select a dynamic sensor from the **Sensor** list.

    The list of sensors comes from the Application Security sensor pools. **Any Available** is the default.
11. (Optional) If you select a sensor that is currently unavailable, another sensor may conduct the scan instead. To ensure that the selected sensor conducts the scan, select **Use this sensor only**.
12. Click **OK**.

    The scan schedule is added to the ScanCentral DAST database.

Editing a schedule

To edit a schedule:

1. On the Scan Schedules view, select the schedule to edit.

   The schedule detail panel appears.
2. In the settings detail panel, click **EDIT**.

   The SCHEDULE SCAN dialog box opens pre-populated with the selected schedule settings.
3. Follow the procedure for completing the SCAN SCHEDULE dialog box in "Creating a new schedule" on page 358.

Enabling or disabling schedules

You can enable or disable schedules in the schedule detail pane. If a schedule is enabled, the scan runs as scheduled. If it is disabled, no additional scans are run.

To enable or disable a schedule:

1. On the Scan Schedules view, select the schedule to enable or disable.
   The schedule detail panel appears.
2. Do one of the following:
   - To enable the schedule, toggle the switch to **Enabled**.
   - To disable the schedule, toggle the switch to **Disabled**.

Deleting a schedule

To delete a schedule, do one of the following:

- Select one or more check boxes for schedules in the Scan Schedules view, and then click **DELETE** at the bottom of the list.
- Select a schedule to view the schedule details, and then click **DELETE** at the bottom of the schedule detail panel.

Chapter 11: Working with deny intervals

A deny interval is a block of time during which scans are not permitted. ScanCentral DAST will not prevent you from scheduling a scan or attempting to start a scan manually during a blackout period. It will, however, place the job in the pending job queue and will start the scan when the deny interval ends.

Similarly, if a scan is running when a deny interval begins, then ScanCentral DAST will do one of the following:

- Pause the scan and finish it when the deny interval ends
- Force the scan to complete

Deny intervals apply to applications

Deny intervals are applied to one or more applications. However, an application can have only one deny interval. If you create and apply a deny interval to an application with an existing deny interval, the existing deny interval is overwritten with the new one.

Deny intervals are global settings

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools. For example, all scans that are running when a deny interval starts may be paused or forced to complete, depending on the deny interval settings.

Accessing the Deny Intervals view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with ScanCentral DAST deny intervals directly in Application Security.

To access the ScanCentral DAST Deny Intervals view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Deny Intervals**.
   The Deny Intervals view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to deny intervals may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Understanding the Deny Intervals view

The Deny Intervals view displays in a table the deny intervals that are stored in the ScanCentral DAST database. Deny intervals are applied to applications. If you create a deny interval and apply it to 100 applications, you will have 100 entries in the Deny Intervals view table.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each application that is configured with a deny interval.

Column	Description
Application	Identifies the application to which the deny interval applies.
Recurrence Type	Indicates how often the deny interval occurs: **Daily**, **Weekly**, **Monthly**, or **Yearly**. Sorting by the Recurrence Type column is not alphabetical. This column sorts by the length of the deny interval—either shortest to longest interval or longest to shortest interval.
Last Occurrence	Indicates the last date and time that the deny interval occurred.
Next Occurrence	Indicates the next date and time that the deny interval will occur.
Modified	Indicates the date and time that the deny interval was created, or if edited, the last date and time that the deny interval was changed.

Understanding the deny intervals detail panel

When you select an entry in the Deny Intervals view, the deny interval detail panel appears. The detail panel displays the information from the deny intervals list table for

the selected deny interval.

The detail panel also provides options to edit and delete the selected deny interval.

Creating a deny interval

When you create a ScanCentral DAST deny interval, you must assign it to one or more applications. You create the deny interval and assign applications to it in the DENY INTERVAL wizard.

To create a deny interval:

1. On the **Deny Intervals** view, click **+ NEW DENY INTERVAL**.
   The DENY INTERVAL wizard opens.
2. On the **General** page, continue according to the following table.

To configure a...	Then...
Recurring deny interval **Note:** The **Recurring** option is selected by default.	a. Enter a date and time for the deny interval to start in the **Start Date** and **Start Time** boxes. b. In the **Duration** area, specify a duration in the **Days**, **Hours**, and **Minutes** boxes. **Tip:** To calculate the duration, click **CALCULATE DURATION**, enter a date and time for the deny interval to end in the **End Date** and **End Time** boxes, and then click **OK**. The duration is automatically calculated and added to the **Days**, **Hours**, and **Minutes** boxes.
Non-recurring deny interval	a. Clear the **Recurring** option. b. Enter a date and time for the deny interval to start in the **Start Date** and **Start Time** boxes. c. Enter a date and time for the deny interval to end in the **End Date** and **End Time** boxes. **Tip:** To select a date from the calendar, click the **calendar** button .

3. In the **Scan action** area, select an action. Options are:
   - **Pause scan** – the running scan is paused until the deny interval has ended.
   - **Force complete scan** – the running scan is forced to complete. If the **Submit for triage** option was selected in the scan settings, the scan results will be published to Application Security when the action is completed.

4. Click **NEXT**.

   The Recurrence page appears. If you did not select the Recurring option on the General page, you cannot configure settings on the Recurrence page. Go to step 7.
5. To schedule a recurring deny interval, in the **Pattern** section specify how often to apply the deny interval according to the following table.

To apply...	Then...
Daily	a. Select **DAILY**. **Note:** If you selected a Duration longer than 24 hours from the Start Date and Start Time on the General page, then the Daily option is not visible on the Recurrence page. b. Select a recurrence in the **Occur every ___ day** box.
Weekly	a. Select **WEEKLY**. **Note:** If you selected a Duration longer than a week from the Start Date and Start Time on the General page, then the Daily and Weekly options are not visible on the Recurrence page. b. Select a recurrence in the **Occur every ___ week** box. c. Select the days to run each week.
Monthly	a. Select **MONTHLY**. **Note:** If you selected a Duration longer than a month from the Start Date and Start Time on the General page, then the Daily, Weekly, and Monthly options are not visible on the Recurrence page. b. Select a recurrence in the **Occur every ___ month** box. c. Do one of the following: ◦ Select **Occur on day** and enter a date in the box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list and a day from the **Day** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.
Yearly	a. Select **YEARLY**.

To apply...	Then...
	Note: If you selected a Duration longer than a year from the Start Date and Start Time on the General page, then the Yearly option is visible on the Recurrence page. However, you cannot configure a duration that is longer than the recurrence interval. b. Do one of the following: ◦ Select **Occur on**, and then select a month from the **Month** list and enter a date in the **Day** box. ◦ Select **Occur on the**, and then select an interval from the **Interval** list, a day from the **Day** list, and a month from the **Month** list. **Note:** Interval options are First, Second, Third, Fourth, and Last.

6. Under **Range**, do one of the following:
   - To leave the recurrence open ended, select **Never ends**.
   - To set an end date, select **Ends by**, and then enter an end date in the **End Date** box or enter the number of occurrences after which to end in the **occurrence** box.

     Note: Entering data into the **End Date** box automatically updates the **occurrence** box, and conversely.
7. Click **NEXT**.

   The Application Selection page appears, listing all available applications.
8. In the **APPLICATIONS** list, select one or more applications to which you want the deny interval to apply.

   The selected applications are added to the APPLICATIONS SELECTED area.
9. Click **NEXT**.

   The Review page appears.
10. Click **SAVE**.

    The deny interval is added to the ScanCentral DAST database for the applications selected.

Managing deny intervals

You can edit and delete deny intervals, and refresh the Deny Intervals view.

Facts about editing a deny interval

Because each entry in the Deny Interval view is for a specific application, be aware of the following facts when editing a deny interval:

- When you select a deny interval from the Deny Interval view to edit, by default the changes apply only to the selected application. You can, however, apply changes to other applications while editing.
- Applications can have only one deny interval. When you edit a deny interval and apply it to an application, it replaces any existing deny interval already applied to that application.
- If you edit the start date and start time of an existing deny interval so that the current time is included in the deny interval, any scan that is currently running for the specified application will be paused or forced to complete.

Editing a deny interval

To edit a deny interval:

1. In the **Deny Interval** view, select the deny interval to edit.
   The deny interval detail panel appears.
2. Click **EDIT**.
   The DENY INTERVAL wizard opens with the deny interval settings visible for the selected application.

   Important! You are editing the settings for the selected application only. To apply your changes to multiple applications, you must select them in the **APPLICATIONS** list in the DENY INTERVAL wizard.
3. To make edits, follow the procedure in "Creating a deny interval" on page 364.

Deleting a deny interval

To delete a deny interval, do one of the following:

- Select one or more check boxes on the **Deny Intervals** view, and then click **DELETE** at the bottom of the table.
- Select a deny interval to view the deny interval details, and then click **DELETE** at the bottom of the deny interval detail panel.

Refreshing the Deny Intervals view

Generally, the changes that you make to deny intervals appear right away on the deny intervals view. However, if other users have access to the same view, any changes they

make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Deny Intervals view:

- Click **REFRESH**.

Chapter 12: Working with policies

You can import into the ScanCentral DAST database policies that have been customized using the OpenText DAST (Fortify WebInspect) Policy Manager tool. Afterward, you can view the custom policies that are available in the ScanCentral DAST database in the Policies view. You can view the policy description, the applications to which the policy is assigned, and other details in the policy detail panel. From the policy detail panel, you can also edit and delete policies.

Accessing the Policies view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with ScanCentral DAST policies directly in Application Security.

To access the Policies view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Policies**.
   The **Policies** view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to policies may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Understanding the Policies view

The Policies view displays in a table the custom policies that have been imported into ScanCentral DAST from OpenText DAST (Fortify WebInspect).

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each policy.

Column	Description
Name	Identifies the name of the imported policy.
Created	Indicates the date and time that the policy was imported into ScanCentral DAST.
Created By	Identifies the user who created or imported the policy.
Modified	Indicates the last date and time that the policy was edited. **Note:** You can only edit the name, description, and the applications to which the policy is assigned.
Modified By	Identifies the user who modified the policy.
All Application Access	Indicates whether the policy applies to all applications.

Understanding the policy detail panel

When you select a policy in the Policies view, the policy detail panel appears. The policy name and description are displayed at the top.

The detail panel displays the same information that is displayed in the Policies view for the selected policy, as well as the information described in the following table.

Item	Description
ASSIGNED APPLICATIONS	Lists the applications to which the policy has been assigned.

Importing a custom policy

When you import a custom policy into ScanCentral DAST, you must assign it to one or more applications. You import the policy and assign applications to it in the CUSTOM POLICY wizard.

To import a policy:

1. On the **Policies** view, click **+ CUSTOM POLICY**.
   The CUSTOM POLICY wizard opens.
2. On the **General** page, click **IMPORT**.
3. Using the standard file-selection window, locate the `.policy` file and click **Open**.

The **File** name, policy **Name**, and **Description** fields in the General page are populated.

4. Edit the **Name** and **Description** fields as needed.
5. Click **NEXT**.
   The Application Selection page appears.
6. In the **APPLICATIONS** list, select one or more applications to which you want the policy to apply.
   The selected applications are added to the APPLICATIONS SELECTED area.
7. Click **NEXT**.
   The Review page appears.
8. Click **SAVE**.
   The policy is added to the ScanCentral DAST database for the applications selected.

Managing policies

You can edit and delete policies, and refresh the list on the Policies view.

Editing a policy

To edit a policy:

1. In the **Policies** view, select the policy to edit.
   The policy detail panel appears.
2. Click **EDIT**.
   The CUSTOM POLICY wizard opens.
3. Edit the **Name** and **Description** fields as needed.
4. Click **NEXT**.
   The Application Selection page appears.
5. In the **APPLICATIONS** list, select one or more applications to which you want the policy to apply.
   The selected applications are added to the APPLICATIONS SELECTED area.
6. Click **NEXT**.
   The Review page appears.
7. Click **SAVE**.
   The changes are saved in the ScanCentral DAST database.

Deleting a policy

To delete a custom policy:

1. Do one of the following:
   - Select one or more check boxes for policies in the **Policies** view, and then click **DELETE** at the bottom of the table.
   - Select a policy to view the policy details, and then click **DELETE** at the bottom of the policy detail panel.

   A confirmation message appears with a prompt to select a replacement policy.
2. In the **Replacement policy** drop-down list, select a replacement policy to be used in all scan settings that contain the policy or policies being deleted.

   Important! If you are deleting multiple policies, then the replacement policy you choose will be used for all deleted policies.

Refreshing the Policies view

Generally, the changes that you make to policies appear right away on the Policies view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Policies view:

- Click **REFRESH**.

Chapter 13: Working with base settings

If you have Admin Role privileges in Application Security, you can create and edit base settings and apply them to applications. All users who have access to the selected applications can use these base settings as templates to create new settings or conduct a scan.

This chapter describes how to configure the Basic settings that are available in the Base Settings Configuration wizard. For information about the Advanced settings, see "Working with Advanced scan settings" on page 219.

Differences between base settings and templates

A template from Application Security:

- Is a complete set of settings with all fields containing data
- Applies to one application and version

Base settings may:

- Be an incomplete set of settings with some fields missing data
- Apply to multiple applications and versions

Base settings are global settings

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools. For example, base settings may apply to multiple applications and versions.

Accessing base settings in Application Security

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with ScanCentral DAST base settings directly in Application Security.

To access DAST base settings in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.

2. In the left panel, select **Base Settings**.
   The Base Settings view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to base settings may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Restricting or allowing edits

If you have permissions to manage restricted scan settings, then you can restrict the editing of base settings. If a setting is already restricted, you can allow editing.

To restrict editing:

- Click the **restrict *<setting name>*** button .

To allow editing:

- Click the **allow *<setting name>*** button .

If you do not have permissions to manage restricted scan settings, then you cannot edit any base settings that display the restricted button .

For more information, see "Permissions in Application Security" on page 45.

Using key stores in base settings

To learn about using key store placeholders in base settings, see "Using key stores in settings" on page 155.

Using artifacts from a repository in base settings

To learn about using artifacts from repositories in scan settings, see "Using artifacts from a repository in settings" on page 157.

Understanding the Base Settings view

The Base Settings view displays in a table the base settings that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each base settings file.

Column	Description
Name	Indicates the name of the base settings file.
Scan Type	Indicates the type of scan to be conducted using the base settings. Types are: • **Standard Scan** • **Workflow-driven Scan** • **API Scan**
Modified	Indicates the date and time that the settings were created, or if edited, the last date and time that the settings were changed.
All Application Access	Indicates whether the base settings apply to all current applications as well as any applications created in the future. Options are **Yes** and **No**.

Converting base settings

ScanCentral DAST uses composite settings, which consist of a JSON version of the scan settings packaged in a ZIP file with any binary files required for the scan, such as macros, client certificates, custom policies, and so forth. When you import a scan from an earlier version of ScanCentral DAST or Fortify DAST, ScanCentral DAST automatically converts the settings to composite settings. When you create and save settings in ScanCentral DAST, it automatically creates composite settings that you can download and use in Fortify DAST.

If base settings require conversion, the **convert** icon appears for the settings in the Base Settings view. If the settings have not been converted, you can convert them in the Base Settings view.

To convert base settings, do one of the following:

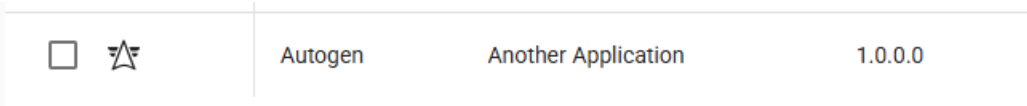
- Click **convert** for the base settings you want to convert.

  Tip: If the conversion is not successful, a **retry create** icon appears. Use this icon to attempt to create the settings again.

- On the base settings detail panel, click **CONVERT SETTINGS**.
  After conversion, the **EDIT** button is available.

Pending Aviator jobs

When an item in the Scans view, Settings List view, or Base Settings view has a pending Aviator job, an **Aviator Macro Autogen** icon ( ) appears to the right of the item's selection check box.



Selecting the item opens the details panel, where Aviator-specific actions are available. For more information, see "Managing Aviator jobs" on page 479.

Understanding the base settings detail panel

When you click settings in the Base Settings view, the base settings detail panel appears to the right. The assigned applications that are configured in the base settings are listed at the top of the panel.

The detail panel displays the same information that is displayed in the Base Settings view for the selected settings, as well as the information described in the following table.

Item	Description
Created	Indicates the date and time that the settings were saved.
Policy	Identifies the dynamic policy to be used to conduct the scan.
User Agent	Indicates the user agent one or more of the following: • **Default** • **Custom** • **Google Chrome (Windows)** • **Safari (macOS)** • **Microsoft Edge (Windows)** • **Safari (iOS)** • **Google Chrome (Android)** • **Googlebot 2.1** • **Bingbot** • **Yahoo! Slurp** • **Safari (iPadOS)**

Item	Description
	Note: Default uses the user agent that is defined in Fortify DAST.
Login Macro	If applicable, indicates the file name of the login macro specified in the settings.
Has Network Auth	Indicates whether network authentication is specified in the settings. Possible values are **Yes** and **No**.
Allowed Hosts	If applicable, indicates the number of allowed hosts configured in the settings.
SPA Option	Indicates how SPA support is configured in the settings.
Traffic Monitor	Indicates whether Traffic Monitor is enabled in the settings. Possible values are **Enabled** and **Disabled**.
Submit for Triage	Indicates whether a scan run from these settings is uploaded to Application Security upon completion. Possible values are **Yes** and **No**.

Creating base settings

You create base settings in the Base Settings configuration wizard. To access this wizard from the ScanCentral DAST Base Settings view:

- Click **+ BASE SETTINGS**.
  The Base Settings configuration wizard opens to the Target page.

What's next?

Do one of the following:

- To configure base settings for a standard scan, proceed with "Configuring base settings for a standard scan" below.
- To configure base settings for a workflow-driven scan, proceed with "Configuring base settings for a workflow-driven scan" on page 380.
- To configure base settings for an API scan, proceed with "Configuring base settings for an API scan" on page 383.

Configuring base settings for a standard scan

A standard scan performs an automated analysis, beginning from the start URL.

To configure base settings for a standard scan:

1. On the Target page, click **STANDARD SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).
   - **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.
3. Type the complete URL or IP address in the **Url** field.

   If you enter a URL, it must be precise. For example, if you enter MYCOMPANY.COM, the sensor will not scan WWW.MYCOMPANY.COM or any other variation unless you specify alternatives in the **Allowed Hosts** setting. For more information, see "Adding and managing allowed hosts in base settings" on page 407.

   An invalid URL or IP address will result in an error. If you want to scan from a certain point in your hierarchical tree, append a starting point for the scan, such as http://www.myserver.com/myapplication/.

   Important! If the URL resolves to an IP address that is not in the valid range for scanning, then a warning appears. If you start the scan with an IP address that is not in the valid range, then the scan will stop and a reason will be provided.

   Scans by IP address will not follow links that use fully qualified URLs (as opposed to relative paths).

   Note: The sensor supports both Internet Protocol version 4 (IPV4) and Internet Protocol version 6 (IPV6). You must enclose IPV6 addresses in brackets.
4. (Optional) To limit the scope of the scan to a specified area, select **Restrict to folder**, and from the list, select one of the following options:
   - **Directory only** – The sensor crawls and/or audits only the URL that you specify. For example, if you select this option and specify the URL www.mycompany/one/two/, the sensor will assess only the "two" directory.
   - **Directory and subdirectories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is higher in the directory tree.
   - **Directory and parent directories** – The sensor begins crawling and/or auditing at the URL you specify, but does not access any directory that is lower in the directory tree.
5. (Optional) To submit the completed scan for triage in Application Security, select **Submit for triage**.

   Note: Submitting for triage enables you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, the selected policy is displayed above the Policy list box. You can select a different policy than the default selection or you can configure multiple policies for better coverage or for additional focus on a specific type of vulnerability. For example, if you want to run a scan using the Standard policy, but want additional focus on SQL Injection, you can select the Standard policy and the SQL Injection policy for the scan. The sensor aggregates all selected policies during the scan.

   Note: The **Standard** policy is the default policy for standard and workflow-driven scan settings in the Settings Configuration wizard. The **API** policy is the default policy for API scan settings in the Settings Configuration wizard. You can, however, choose different policies if needed.

   Continue according to the following table.

To...	Then...
Select one or more policies	a. Click in the **Policy** list box. A list of policies appears. **Tip:** Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter. b. Select a policy from the list. The policy is added to the list of selected policies. c. Repeat steps a and b for each policy you want to select.
Remove a policy from the list of selected policies	• Click **remove** × for the selected policy. The policy is cleared from the list of selected policies.

   Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 519. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

7. Do one of the following:
   - To use a standard user agent, select it from the User Agent **Profile** list.

     Note: Default uses the user agent that is defined in Fortify DAST.

   - To use a custom user agent, select **Custom** from the User Agent **Profile** list, and then type the user-agent string in the **User-Agent** box.

Tip: User-agent strings generally use the following format:

<browser>/<version> (*<system and browser information>*) *<platform>* (*<platform details>*) *<extensions>*

What's next?

Do one of the following:

- To configure proxy settings in the base settings, proceed with "Configuring proxy settings in base settings" on page 389.
- To configure authentication in the base settings, click **NEXT** and proceed with "Configuring authentication in base settings for standard and workflow-driven scans" on page 391.

Configuring base settings for a workflow-driven scan

A workflow-driven scan audits only those URLs included in a macro that you previously recorded. It does not follow any hyperlinks encountered during the audit. A logout signature is not required. This type of macro is used most often to focus on a particular subsection of the application. If you select multiple macros, all of them will be included in the same scan.

Types of macros supported

You can use `.webmacro` files, HTTP archive (`.har`) files, or Burp Proxy captures.

Important! If you use a login macro in conjunction with a workflow macro or startup macro or both, all macros must be of the same type: all `.webmacro` files, all `.har` files, or all Burp Proxy captures. You cannot use different types of macros in the same scan. Likewise, `.webmacro` login and workflow files must have been created using the same version of Web Macro Recorder. You cannot use a login file that was recorded in the Event-based Web Macro Recorder and a workflow file that was recorded in the Session-based Web Macro Recorder.

Configuring base settings for a workflow-driven Scan

To configure base settings for a workflow-driven scan:

1. On the Target page, click **WORKFLOW-DRIVEN SCAN**.
2. Select one of the following scan modes:
   - **Crawl Only**: Maps the hierarchical data structure of the site.
   - **Crawl and Audit**: Maps the hierarchical data structure of the site and audits each resource (page).

- **Audit Only**: Applies the methodologies of the selected policy to determine vulnerability risks, but does not crawl the website. This scan mode does not follow or assess links on the site.

3. Continue according to the following table.

To...	Then...
Add a macro to the scan settings	a. Click **MANAGE**. b. Type a name for the macro in the **Name** field. c. Click **IMPORT** and browse to locate the workflow to add to the scan settings. d. Click **OK**. e. Repeat steps a through d to add another macro to the scan settings.
Remove a macro from the list of macros	a. Select the macro in the macro list. b. Click **REMOVE**.

Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

You can use a key store placeholder for any field that displays **Open keystore** . For more information, see "Using key stores in settings" on page 155.

4. (Optional) To submit the completed scan for triage in Application Security, select **Submit for triage**.

Note: Submitting for triage enables you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

5. Under **Audit Depth (Policy)**, the selected policy is displayed above the Policy list box. You can select a different policy than the default selection or you can configure multiple policies for better coverage or for additional focus on a specific type of vulnerability. For example, if you want to run a scan using the Standard policy, but want additional focus on SQL Injection, you can select the Standard policy and the SQL Injection policy for the scan. The sensor aggregates all selected policies during the scan.

Note: The **Standard** policy is the default policy for standard and workflow-driven scan settings in the Settings Configuration wizard. The **API** policy is the default policy for API scan settings in the Settings Configuration wizard. You can, however, choose different policies if needed.

Continue according to the following table.

To...	Then...
Select one or more policies	a. Click in the **Policy** list box. A list of policies appears. **Tip:** Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with the text that you enter. b. Select a policy from the list. The policy is added to the list of selected policies. c. Repeat steps a and b for each policy you want to select.
Remove a policy from the list of selected policies	• Click **remove** × for the selected policy. The policy is cleared from the list of selected policies.

Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 519. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

6. Do one of the following:
   - To use a standard user agent, select it from the User Agent **Profile** list.

     Note: Default uses the user agent that is defined in Fortify DAST.

   - To use a custom user agent, select **Custom** from the User Agent **Profile** list, and then type the user-agent string in the **User-Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/*<version>* (*<system and browser information>*) *<platform>* (*<platform details>*) *<extensions>*

What's next?

Do one of the following:

- To configure proxy settings in the base settings, proceed with "Configuring proxy settings in base settings" on page 389.

- To configure authentication in the base settings, click **NEXT** and proceed with "Configuring authentication in base settings for standard and workflow-driven scans" on page 391.

Configuring base settings for an API scan

For Open API, OData, and Postman scans, the sensor creates a macro from the REST API definition, and then performs an automated analysis. For GraphQL, gRPC, and SOAP scans, a more traditional scanning method is used.

Important! The ScanCentral DAST Utility Service container must be up and running to configure and run a Postman scan. Also, if the Postman scan requires a proxy, you must configure the proxy settings before you validate the Postman collection file(s). For more information, see "Configuring proxy settings" on page 173.

Note: If Fortify Connect is enabled for the application, Fortify Connect is not used when validating an API definition URL in base settings.

To configure base settings for an API scan:

1. On the **Target** page, click **API SCAN**.
2. In the **Type** list, select the API type to be scanned. The options are:
   - **GraphQL**
   - **GRPC**
   - **OData**
   - **Open API** (also known as Swagger)
   - **Postman**
   - **SOAP**
3. Continue according to the following table.

For this API type...	Do this...
GraphQL **GRPC** **OData** **Open API**	To use a file: a. In the **API Definition Source Type** list, select **File**. b. Click **IMPORT** and import the definition file. **Tip:** Alternatively, you can paste in the full path to a definition file that is saved on your local machine. **Important!** Open API definition files must specify the host,

For this API type...	Do this...
	scheme, and service path. Otherwise, undesirable results may occur. To use a URL: a. In the **API Definition Source Type** list, select **URL**. b. Provide the URL to the API definition file, as shown in the following examples: `http://172.16.81.36/v1` `http://myapi/protos/client.proto` `http://myapi/graphql/`
Postman	a. Do one of the following: ◦ To import a workflow collection, select **IMPORT** and then import the Postman collection file. ◦ To import an authentication collection, select **Authentication** from the **IMPORT** drop-down list, and then import the Postman collection file. ◦ To import an environment file, select **Environment** from the **IMPORT** drop-down list, and then import the Postman environment file. The file is added to the list of collection files. Repeat this Step to import additional files. **Important!** You can import only one authentication collection and one environment file. b. Click **VALIDATE** to validate the collection file(s). **Note:** At least one workflow collection must be imported before you can validate the files. The **VALIDATE** button is not available if only authentication and environment collections have been imported. **Tip:** To cancel the validation process, click **Cancel validation** ×. Upon successful validation, the POSTMAN

For this API type...	Do this...
	VALIDATION dialog box opens, displaying a list of sessions contained in the collection file(s). If authentication sessions are identified, they are preselected as **Auth** sessions. All other sessions are preselected as **Audit** sessions. Additionally, the Postman Authentication Results area displays the type of authentication detected as **None**, **Static**, or **Dynamic**. **Note:** **Auth** sessions will be used for authentication for the scan. **Audit** sessions will be audited in the scan. c. (Optional) Select the **Auth** or **Audit** check box for a session to change its type as needed. d. (Optional) Make changes to the **Postman Authentication Results** as follows: ◦ For **Static** authentication, enter a token in the **Custom Header Token** box. ◦ For **Dynamic** authentication, do the following: • Select the **Regex (Custom)** option to the right of the **Response Token Name** box, and then enter a custom regular expression in the **Response Token Name** box. • Select the **Regex (Custom)** option to the right of the **Request Token Name** box, and then enter a custom regular expression in the **Request Token Name** box. • Clear the **Use Auto Detect** option to the right of the **Logout Condition** box, and then enter a new logout condition string in the **Logout Condition** box. e. Did you make changes to the Postman Authentication Results? ◦ If yes, click **VALIDATE** to validate the new authentication settings, and then click **OK**. **Note:** Clicking **VALIDATE** regenerates all sessions for the postman collection. It does not retain any previous changes to **Auth** or **Audit** sessions even if the collection and sessions are the same. **Tip:** To cancel the validation process, click **Cancel**

For this API type...	Do this...
	validation ×. ◦ If no, click **OK**. **Note:** After validation, an **EDIT** button is available. This button opens the POSTMAN VALIDATION dialog box for editing the sessions contained in the collection file(s) as described previously in this procedure.
SOAP	To use a file: a. In the **API Definition Source Type** list, select **File**. b. In the **API Definition Version Type** list, select a version to allow filtering of operations by the specific version. Options are as follows: ◦ **Legacy** – filters against the lowest supported version. ◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available. ◦ **Newest** – the default setting, filters against the latest version. c. Click **IMPORT** and import the definition file. **Tip:** Alternatively, you can paste in the full path to a definition file that is saved on your local machine. To use a URL: a. In the **API Definition Source Type** list, select **URL**. b. In the **API Definition Version Type** list, select a version to allow filtering of operations by the specific version. Options are as follows: ◦ **Legacy** – filters against the lowest supported version. ◦ **Mixed** – uses a combination of Legacy and Newest, depending on what is available. ◦ **Newest** – the default setting, filters against the latest version. c. Provide the URL to the API definition file, as shown in the following example: `http://172.16.81.36/web-services/infoService?wsdl`

4. If you imported a definition file, the **API location is different from API definition location** option is selected. Specify the following:
   a. In the **API Scheme Type** list, select a type. Options are **HTTP**, **HTTPS**, and **HTTP/HTTPS**.
   b. In the **API Host** box, type the URL or hostname.
   c. In the **API Service Path** box, type the directory path for the API service.

   Note: The GraphQL service location is always the same as the definition location. For SOAP, if the query string "?wsdl" value is removed, then the SOAP service location may or may not be the same as the definition location. The gRPC service location is always different from the definition location.

   Note: If the service path is not defined for an Open API scan, then the sensor will use the basePath that is defined in the Open API definition contents. For Open API scans, select **API location is different from API definition location** unless your service is explicitly run at the same location as the docs folder for Open API. Optionally, you may choose to define a service path if it differs from the basePath.

5. (Optional) To submit the completed scan for triage in Application Security, select **Submit for triage**.

   Note: Submitting for triage enables you to perform audit analysis of the findings so that you can assign a user and an analysis value to the findings.

6. Under **Audit Depth (Policy)**, the selected policy is displayed above the Policy list box. You can select a different policy than the default selection or you can configure multiple policies for better coverage or for additional focus on a specific type of vulnerability. For example, if you want to run a scan using the Standard policy, but want additional focus on SQL Injection, you can select the Standard policy and the SQL Injection policy for the scan. The sensor aggregates all selected policies during the scan.

   Note: The **Standard** policy is the default policy for standard and workflow-driven scan settings in the Settings Configuration wizard. The **API** policy is the default policy for API scan settings in the Settings Configuration wizard. You can, however, choose different policies if needed.

   Continue according to the following table.

To...	Then...
Select one or more policies	a. Click in the **Policy** list box. A list of policies appears. **Tip:** Begin typing the policy name in the **Policy** list box to filter the list of policy names that begin with

To...	Then...
	the text that you enter. b. Select a policy from the list. The policy is added to the list of selected policies. c. Repeat steps a and b for each policy you want to select.
Remove a policy from the list of selected policies	• Click **remove** × for the selected policy. The policy is cleared from the list of selected policies.

Note: The default policies are stored in SecureBase tables in the ScanCentral DAST database. For more information about the list of default policies, see "Policies" on page 519. Custom policies are assigned to specific applications and are stored in the ScanCentral DAST database. Only those custom policies that are assigned to the selected application appear in the Policy list.

7. Do one of the following:
   - To use a standard user agent, select it from the User Agent **Profile** list.

     Note: Default uses the user agent that is defined in Fortify DAST.

   - To use a custom user agent, select **Custom** from the User Agent **Profile** list, and then type the user-agent string in the **User-Agent** box.

     Tip: User-agent strings generally use the following format:

     <browser>/<version> (*<system and browser information>*) *<platform>* (*<platform details>*) *<extensions>*

What's next?

Do one of the following:

- To configure proxy settings in the base settings, proceed with "Configuring proxy settings in base settings" on the next page.
- To configure authentication in the base settings, click **NEXT** and proceed with "Configuring authentication in base settings for API scans" on page 396.

Configuring proxy settings in base settings

To configure proxy settings in the base settings:

1. On the Target page, click **PROXY SETTINGS**.
   The PROXY CONFIGURATION dialog box opens.
2. Select the **Use Proxy Server** option.
   The settings become available for you to configure.
3. Configure the settings according to the following table.

To...	Then...
Use the Web Proxy Autodiscovery Protocol (WPAD) to locate and use a proxy autoconfig file to configure the web proxy settings	Select **Auto detect proxy settings**.
Import your proxy server information from Firefox	Select **Use Firefox proxy settings**. **Note:** Using browser proxy settings does not guarantee that you can access the Internet through a proxy server. If the Firefox browser connection settings are configured for "No proxy," then a proxy will not be used.
Load proxy settings from a Proxy Automatic Configuration (PAC) file	a. Select **Configure proxy settings using a PAC file**. b. In the **URL** box, type the URL location for the PAC file.
Access the Internet through a proxy server	a. Select **Explicitly configure proxy** settings. b. In the **Server** box, enter the URL or IP address of your proxy server. c. In the **Port** box, enter the port number (for example, 8080). d. From the **Type** list, select the protocol type for handling TCP traffic through the proxy server. The

To...	Then...
	options are: **Standard**, **SOCKS4**, or **SOCKS5**. **Important!** Socks4 proxy servers do not support authentication. When using a Socks proxy server that requires authentication, you must use a Socks5 proxy. e. If authentication is required, select a type from the **Authentication** list. The options are: **None**, **Basic**, **NTLM**, **Digest**, **Automatic**, **Kerberos**, or **Negotiate**. **Note:** For sensors running on the Linux OS, ADFS_CBT will be used if Negotiate is selected. f. If your proxy server requires authentication, enter the qualifying user name in the **User Name** field and the qualifying password in the **Password** field. g. If you do not need to use a proxy server to access certain IP addresses (such as internal testing sites), enter the addresses or URLs in the **Bypass** field. Use semicolons to separate entries.

4. Click **OK**.
   The proxy settings are saved and the PROXY CONFIGURATION dialog box closes.

What's next?

To configure authentication for the scan, click **NEXT** and proceed with "Configuring authentication in base settings for standard and workflow-driven scans" on the next page or "Configuring authentication in base settings for API scans" on page 396.

Configuring authentication in base settings for standard and workflow-driven scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Configuring site authentication

You can use a recorded login macro containing one or more usernames and passwords that allow you to log in to the target site. The macro must also contain a "logout condition," which indicates when an inadvertent logout has occurred so that the sensor can rerun the macro to log in again.

To configure site authentication:

1. Select **Site Authentication**.
2. Do one of the following:
   - To import an existing login macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays **Open keystore** 🔑. For more information, see "Using key stores in settings" on page 155.
   - To record a login macro, click **Open Macro Recorder 26.4**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 26.4 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder tool" on the next page.
   - To have Aviator automatically create a login macro, proceed with "Using Aviator for login macro creation" below.

     Tip: The Aviator service must be configured and enabled for the Autogen UI to appear. For more information, see "Working with Aviator auto-generated macros" on page 475.

Using Aviator for login macro creation

To use Aviator for automatic login macro creation, do the following:

1. Select the **Aviator Autogen Macro** tab.
2. In the **Username** box, type a user name.

3. In the **Password** box, type the corresponding password.
4. Optionally, to use TOTP, slide the **Use TOTP** option to enabled and continue according to the following table:

To...	Then...
Use a QR code image	a. Select the **Upload Image** tab. b. Upload or drag and drop the QR code image into the upload image area. A message indicates whether the secret is successfully extracted. After which, you can either replace or remove the uploaded image.
Manually enter the secret	a. Select the **Enter Text** tab. b. In the **TOTP Secret** box, enter the secret.

Important! You may continue configuring the scan settings and save the configuration. However, when an Aviator auto-gen macro is pending, scan settings in the Getting Started section of the Settings configuration wizard become temporarily read-only. The settings remain visible but are disabled with a "pending macro validation" message. After macro generation completes, the settings become fully editable and selectable.

Validating the login macro

You can have Fortify DAST test the login macro at the start of the scan to ensure that the log in is successful. If the macro is invalid and fails to log in to the application, the scan stops and an error message is written in the scan log file. For more information and troubleshooting tips, see "Testing login macros" on page 498.

To validate the login macro:

- Select **Enable macro validation**.

Downloading the Macro Recorder tool

The Scan Settings Configuration wizard enables you to download the Event-based Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is available for both Microsoft Windows® and Mac® operating systems. You cannot use the Event-based Web Macro Recorder on Linux® operating systems.

To download the Macro Recorder tool:

1. Do one of the following:
   - On the **Workflow-Driven Scan** tab on the **Target** page of the Scan Settings Configuration wizard, click **Download Macro Recorder 26.4**.
   - Under **Site Authentication** on the **Authentication** page of the Scan Settings Configuration wizard, click **Download Macro Recorder 26.4**.

   The DOWNLOAD MACRO RECORDER dialog box opens.
2. Do one of the following:
   - To download the Microsoft Windows® version, select **Macro Recorder Windows (x64) Setup**.

     The `MacroRecorderWindowsX64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

     Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.
   - To download the Mac® version, select **Macro Recorder MacOS (arm64) Setup**.

     The `MacroRecorderMacOSArm64Setup.dmg` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the DMG file.

     Tip: For instructions on installing and launching the Mac® version, refer to the *OpenText™ Fortify DAST Tools Guide*.

Using a client certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

To use a client certificate:

1. Select **Use Client Certificate**.
2. Click **IMPORT**.

   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.

   The certificate file is added to the Client certificate box.
4. If the certificate requires a password, do the following:
   a. Select **Requires password**.
   b. Enter the password in the **Client certificate password** box.
5. Optionally, click **VALIDATE** to perform basic validation of the certificate.

Note: Basic validation only confirms that the file is a certificate, verifies the password if applicable, and checks for a private key. If the certificate is not valid, the scan will fail upon startup.

Configuring network authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Network Authentication**.
2. Select an **Authentication Type**. Options are as follows:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Digest**
   - **Kerberos**
   - **NT LAN Manager (NTLM)**
   - **OAuth 2.0 Bearer**
3. For all authentication methods except OAuth 2.0 Bearer, do the following:
   a. Type the authentication user name in the **Username** box.
   b. Type the authentication password in the **Password** box.
4. For the OAuth 2.0 Bearer method, continue with "Configuring OAuth 2.0 bearer credentials" below.

Caution! The sensor crawls all servers granted access by this password (if the sites/servers are included in the Allowed Hosts setting). To avoid potential damage to your administrative systems, do not use credentials that have administrative rights. If you are unsure about your access rights, contact your System Administrator or internal security professional.

Configuring OAuth 2.0 bearer credentials

Open authorization (OAuth) 2.0 is an open-standard authorization protocol that shares authorization tokens between services or applications to prove the identity of a user. You can configure the following types of OAuth 2.0 authentication flows:

- **Client Credentials Grant** – The client uses its client credentials, such as client ID and client secret, when requesting access to the protected resources.
- **Password Credentials Grant** – The client obtains the resource owner's credentials, such as user name and password, usually by way of an interactive form.

If you configure OAuth 2.0 authentication, then the sensor will use the retrieved token for the entire scan. The token will be refreshed if it expires.

After selecting **OAuth 2.0 Bearer** as network authentication type in scan settings, to configure OAuth 2.0 bearer credentials:

1. In the **Access Token URL** box, type the URL that is used to generate tokens, such as `https://<yourDomain>/oauth2/token`.
2. In the **OAuth Flow Type** list, select a flow. Options are **Client Credentials Grant** and **Password Credentials Grant**.
3. Optionally, if your service supports different scopes (or permissions) for the OAuth flow, specify the scope to use in the **Scope** box.
4. Provide information that will be included in the authorization request header according to the following table.

To configure...	Then...
A Client Credentials Grant flow	In the **Client ID** box, enter the application (client) ID. In the **Client Secret** box, enter the client secret that you generated for your application in the OAuth provider's registration portal.
A Password Credentials Grant flow	In the **User Name** box, enter the user name. In the **Password** box, enter the password.

5. Optionally, to specify additional parameters:
   a. Select **Use Additional Parameters**.
   b. Click **add oauth parameter** +.
   c. In the **parameter name** box, enter a parameter name.
   d. In the **parameter value** box, enter a parameter value.
   e. To add another parameter name-value set, return to Step 5b. Otherwise, go to Step 6.

   Important! The `grant_type` and `scope` parameter names are reserved and cannot be used in the additional parameters list.

   If the OAuth Flow Type is Client Credentials Grant, then `client_credentials`, `client_id`, and `client_secret` cannot be used in the additional parameters list.

   If the OAuth Flow Type is Password Credentials Grant, then `username` and `password` cannot be used in the additional parameters list.
6. By default, the sensor uses Status Code 403 for the logout signature. Optionally, if you use a custom status code, in the **Logout Signature** box, enter the status code or a regular expression to indicate the logout signature. Use the following syntax:

   `[STATUSCODE]<Number>`

7. Optionally, click **Test** to validate access to the server and receipt of a bearer token.
   To see the response of the validation request, click **SEE RESPONSE**.

What's next?

To configure details for the scan, click **NEXT** and proceed with "Configuring base settings details" on page 403.

Configuring authentication in base settings for API scans

If your site or network or both require authentication, you can configure it on the Authentication page.

Options for configuring authentication include the following:

- "Using a client certificate" below
- "Configuring network authentication" below
- "Using custom headers" on page 401
- "Configuring SOAP settings" on page 401

Using a client certificate

Client certificate authentication allows users to present client certificates rather than entering a user name and password. You can enable the use of a certificate and then import the certificate to the scan settings.

Note: Client certificates do not apply to OData or Open API definition types.

To use a client certificate:

1. Select **Use API Client Certificate**.
2. Click **IMPORT**.
   A standard Windows file selection dialog box opens.
3. Locate and select the certificate file, and then click **Open**.
   The certificate file is added to the Client certificate box.
4. Enter the password in the **Client certificate password** box.

Configuring network authentication

If server authentication is required, you can configure authentication using network credentials.

To configure network authentication:

1. Select **Use API Network Authentication**.
2. Select an **Authentication Type**. The API Type determines the available authentication types. The complete list of authentication types is:
   - **ADFS CBT**
   - **Automatic**
   - **Basic**
   - **Bearer**
   - **Custom**
   - **Digest**
   - **Kerberos**
   - **NT LAN Manager (NTLM)**
   - **OAuth 2.0 Bearer**
3. Continue according to the following table.

For this authentication type...	Do this...
ADFS CBT **Automatic** **Basic** **Digest** **Kerberos** **NTLM**	a. Type the authentication user name in the **Username** box. b. Type the authentication password in the **Password** box.
Bearer	Optionally, type the JSON token, generally from a response to a login form, in the **Token Value** box. When using Bearer, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a token value" on the next page. **Note:** Not available for SOAP web service scans.
Custom	a. Type the token name in the **Scheme** box. b. Optionally, type the token value in the **Parameter** box.

For this authentication type...	Do this...
	When using Custom, you can fetch a token that is generated from a response to a workflow macro, and then use the token to apply state. For more information, see "Fetching a token value" below. **Note:** Not available for SOAP web service scans.
OAuth 2.0 Bearer	Continue with "Configuring OAuth 2.0 bearer credentials" on the next page.

Fetching a token value

You can use a custom regular expression to fetch the token value from a login or workflow macro. If a match to the regular expression occurs in the response, then the value is fetched and used as a bearer token. If the regular expression contains parentheses, then the value inside the parentheses will be extracted and used as a bearer token. Only the first value inside parentheses will be used.

Note: Fetching a token value does not apply to OData or Open API definition types.

To fetch a token value:

1. Select **Use Fetch Token**.
2. Do one of the following:
   - To import an existing macro, click **IMPORT**, and then locate and select the file to import.

     Tip: If a macro contains parameters, a **param** button appears to the right of the macro name. Click the button to open the TRU CLIENT PARAMETERS dialog box and enter values to use during the scan.

     You can use a key store placeholder for any field that displays **Open keystore** 🔑. For more information, see "Using key stores in settings" on page 155.

   - To record a macro, click **Open Macro Recorder 26.4**.

     Tip: If you have not already downloaded and installed the Macro Recorder tool, the Open Macro Recorder 26.4 link will not open the tool. You must first download the tool and install it on your local machine as described in "Downloading the Macro Recorder tool" on page 400.
3. Type a regular expression for pattern matching in the **Search Pattern** box.

4. Do one of the following:
   - To have each scan thread run its own fetch macro playback and apply the bearer token value to the thread, select the **Isolate state** check box.
   - To have only one fetch macro playback run for all scan threads and the single shared bearer token value apply to all threads, clear the **Isolate state** check box.

Configuring OAuth 2.0 bearer credentials

Open authorization (OAuth) 2.0 is an open-standard authorization protocol that shares authorization tokens between services or applications to prove the identity of a user. You can configure the following types of OAuth 2.0 authentication flows:

- **Client Credentials Grant** – The client uses its client credentials, such as client ID and client secret, when requesting access to the protected resources.
- **Password Credentials Grant** – The client obtains the resource owner's credentials, such as user name and password, usually by way of an interactive form.

If you configure OAuth 2.0 authentication, then the sensor will use the retrieved token for the entire scan. The token will be refreshed if it expires.

After selecting **OAuth 2.0 Bearer** as network authentication type in scan settings, to configure OAuth 2.0 bearer credentials:

1. In the **Access Token URL** box, type the URL that is used to generate tokens, such as `https://<yourDomain>/oauth2/token`.
2. In the **OAuth Flow Type** list, select a flow. Options are **Client Credentials Grant** and **Password Credentials Grant**.
3. Optionally, if your service supports different scopes (or permissions) for the OAuth flow, specify the scope to use in the **Scope** box.
4. Provide information that will be included in the authorization request header according to the following table.

To configure...	Then...
A Client Credentials Grant flow	In the **Client ID** box, enter the application (client) ID. In the **Client Secret** box, enter the client secret that you generated for your application in the OAuth provider's registration portal.
A Password Credentials Grant flow	In the **Username** box, enter the user name. In the **Password** box, enter the password.

5. Optionally, to specify additional parameters:
   a. Select **Use Additional Parameters**.
   b. Click **add oauth parameter** +.
   c. In the **parameter name** box, enter a parameter name.
   d. In the **parameter value** box, enter a parameter value.
   e. To add another parameter name-value set, return to step b. Otherwise, go to Step 6.

   Important! The `grant_type` and `scope` parameter names are reserved and cannot be used in the additional parameters list.

   If the OAuth Flow Type is Client Credentials Grant, then `client_credentials`, `client_id`, and `client_secret` cannot be used in the additional parameters list.

   If the OAuth Flow Type is Password Credentials Grant, then `username` and `password` cannot be used in the additional parameters list.
6. By default, the sensor uses Status Code 403 for the logout signature. Optionally, if you use a custom status code, in the **Logout Signature** box, enter the status code or a regular expression to indicate the logout signature. Use the following syntax:

   `[STATUSCODE]<Number>`
7. Optionally, click **Test** to validate access to the server and receipt of a bearer token.

   To see the response of the validation request, click **SEE RESPONSE**.

Downloading the Macro Recorder tool

You can download the Event-based Web Macro Recorder tool from the ScanCentral DAST REST API container.

Important! The Event-based Web Macro Recorder is a Microsoft Windows®-based application. You cannot use the Event-based Web Macro Recorder on Linux operating systems.

To download the Macro Recorder tool:

- Under **Site Authentication**, do one of the following:
  - To download the Microsoft Windows® version, select **Macro Recorder Windows (x64) Setup**.

    The `MacroRecorderWindowsX64Setup.exe` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the EXE file as usual.

    Tip: After installation, you can launch the Macro Recorder tool from the Windows Start menu under **Fortify ScanCentral DAST**.
  - To download the Mac® version, select **Macro Recorder MacOS (arm64) Setup**.

The `MacroRecorderMacOSArm64Setup.dmg` file is downloaded to the default download directory that is specified in your browser settings. Navigate to the download directory and install the DMG file.

Tip: For instructions on installing and launching the Mac® version, refer to the *OpenText™ Fortify DAST Tools Guide*.

Using custom headers

You can configure multiple custom headers.

Important! OpenText recommends that you do not configure more than one custom header using the same HTTP header name.

To add a custom header:

1. Select **Use Custom Headers**.
2. Click **add custom header** +.
3. In the **header name** box, type the custom HTTP header name. For example, `X-MyCustomAuth`.

   Important! The header must be unique and cannot be `Authorization`.
4. In the **header scheme** box, type the header value prefix name. For example, `CustomToken`.
5. In the **header value** box, type the custom header value.
6. Click **confirm** ✔.

   The custom header is added to the list.

To edit a custom header:

- Click **edit** for the custom header you want to edit.

To delete a custom header:

- Click **delete** × for the custom header you want to delete.

Configuring SOAP settings

You can configure message-based authentication for SOAP scans.

To configure SOAP authentication settings:

1. Select **Use SOAP Configuration**.
2. Select that authentication method to use from the **SOAP Method** list. Options are **Username Token** and **Certificate Pair**.
3. Continue according to the following table.

For this authentication method...	Do this...
Username Token	a. In the **Username** box, type the user name whose credentials are used to access the SOAP service. b. In the **Password** box, type the password for the user name. c. In the **Username Token Type** list, select the type of token. Options are **Text** and **Hash**. d. In the **Timestamp** list, select an option for when the Username Token was created and when it expires. Options are **Created**, **Full**, and **None**. e. If nonce is enabled for the token, select **Includes nonce**. **Important!** Nonce is required for hash tokens because it helps the server to recalculate the hash and compare it to the data the client sent.
Certificate Pair	a. Click **IMPORT** to the right of the **Client Certificate** box. A standard Windows file selection dialog box opens. b. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Client Certificate box. c. In the **Client Certificate Password** box, type the password. d. Click **IMPORT** to the right of the **Server Certificate** box. A standard Windows file selection dialog box opens. e. Locate and select the certificate file, and then click **Open**. The certificate file is added to the Server Certificate box. f. If the server certificate requires a password, select **Requires password** and type the password in the **Server Certificate Password** box.

4. Optionally, to identify the Web Services Addressing (WS-Addressing) schema version used by the SOAP service, select **Use WS Addressing** and continue as follows:
   a. In the **Schema Version** list, select the version. Options are **NONE**, **WSA0408**, and **WSA0508**.
   b. In the **WSA: To** box, enter the URL override for the Web service host.

   Note: SOAP services may be exposed by way of a load balancer or reverse proxy. This configuration may prevent the sensor from getting the correct

information for the internal Web service host name. The "WSA: To" URL override provides the correct address into WS Addressing.

The URL override uses the following format:

`https://<host_name><service_path>/<port_name>`

What's Next?

To configure details for the scan, click **NEXT** and proceed with "Configuring base settings details" below.

Configuring base settings details

You can configure the following settings on the Base Settings Details page:

- Content and filters (API scans only. For more information, see "Configuring API content and filters in base settings" below.)
- Allowed hosts (For more information, see "Adding and managing allowed hosts in base settings" on page 407.)
- Scan priority (For more information, see "Configuring scan priority in base settings" on page 408.)
- Data retention (For more information, see "Configuring data retention in base settings" on page 409.)
- Single-page application (SPA) support (Standard and Workflow-driven scans only. For more information, see "Scanning single-page applications in base settings" on page 409.)
- Traffic Monitor (For more information, see "Enabling traffic monitor in base settings" on page 410.)
- Exclusions (For more information, see "Creating and managing basic exclusions in base settings" on page 411.)
- Redundant page detection (Standard and Workflow-driven scans only. For more information, see "Configuring redundant page detection in base settings" on page 413.)

What's next?

After you configure the scan details, click **NEXT** and proceed with "Applying base settings to applications" on page 414.

Configuring API content and filters in base settings

When configuring API scans, you can use the Content and Filters page to configure the preferred content type, as well as operations and parameter names and types to include or exclude during the scan.

Specifying the preferred content type

The preferred content type setting specifies the preferred content type of the request payload. If the preferred content type is in the list of supported content types for an operation, then the generated request payload will be of that type. Otherwise, the first content type listed in an operation will be used. By default, the preferred content type is application/json.

To change the preferred type:

- Type the preferred content type in the **Preferred Content Type** box.

Defining specific operations to include

The Include feature defines an allow list of operation IDs that should be included in the output.

To define a specific operation to include:

1. Select **Specific Operations**.
2. Select **Include**.
3. Click **add operation** +.
4. In the **Operation to add** box, type the operation ID.
5. Click **confirm** ✔.
   The operation ID is added to the allow list.

Defining specific operations to exclude

The Exclude feature defines a deny list of operation IDs that should be excluded from the output.

To define a specific operation to exclude:

1. Select **Specific Operations**.
2. Select **Exclude**.
3. Click **add operation** +.
4. In the **Operation to add** box, type the operation ID.
5. Click **confirm** ✔.
   The operation ID is added to the deny list.

Editing specific operations

To edit a specific operation in the allow or deny list:

1. Do one of the following:
   - To edit an operation in the allow list, select **Include**.

- To edit an operation in the deny list, select **Exclude**.

2. Click the **edit** for the operation ID you want to edit.

Removing specific operations

To remove a specific operation from the allow or deny list:

1. Do one of the following:
   - To remove an operation from the allow list, select **Include**.
   - To remove an operation from the deny list, select **Exclude**.
2. Select the check box for each operation ID you want to remove.
3. Click **REMOVE**.

Defining parameter rules

Parameter rules define a default value to use for a parameter when the parameter name and type are encountered. You can also specify operations to determine whether a specific parameter rule should or should not apply to those operations.

Important! If you configure a parameter rule and then change the API definition type for which the parameter rule type becomes invalid, the invalid parameter rule type will be changed to **Any**. The invalid parameter rule will be highlighted in the Parameter Rules list, and a warning message will be displayed below the list.

To add a parameter rule:

1. Select **Parameter Rules**.
2. Click **Add**.
   The PARAMETER RULE dialog box appears.
3. In the **Parameter Rule Name** box, type a name for the rule.
4. In the **Parameter Rule Type** list, select a type. Available options depend on the API type and may include the following:
   - **Any**
   - **Boolean**
   - **Date**
   - **File**
   - **Guid**
   - **Number**
   - **String**

   For more information on the Parameter Rule Types and their equivalents based on

API type, see "Understanding parameter type matches" on page 193.

5. Continue according to the following table:

For this Rule Type...	Do this...
Any	In the **Value** box, type any value.
Boolean	In the **Boolean Value** list, select **true** or **false**.
Date	To enter any string value as the date: • Type the string in the **Date** box. **Note:** You may enter a duration, time span, formatted date, or formatted time in the **Date** box. To select a date/time format and use a calendar and clock to generate a formatted string: a. Click **GENERATE DATE**. The GENERATE DATE STRING dialog box opens. b. From the **Date Type** list, select a format. Options are **Date and time**, **Date**, and **Time**. c. In the **Date** box, enter a date using the preferred format defined in your Application Security. **Tip:** To select a date from the calendar, click the **Calendar** button. d. In the **Time** box, enter a time using the preferred format defined in your Application Security **Tip:** To select a time from a list, click the **Clock** button. e. Click **OK**.
File	a. Click **IMPORT** and browse to locate the file to add to the scan settings. b. Click **Open**.
Guid	In the **Value** box, enter a GUID.
Number	In the **Number Value** box, enter a numerical value.
String	In the **Value** box, type any value.

6. For Open API scans, in the **Parameter Rule Location** list, select a location where the parameter is found in the request. Options are:
   - **Any**
   - **Body**
   - **Header**
   - **Path**
   - **Query**
7. Optionally, select **Inject Parameter** to include the defined parameter in the request.

   Important! The **Inject Parameter** option does not work with schema-based APIs, such as SOAP, gRPC, and Postman. Those API types do not accept forced parameters. For GraphQL, **Inject Parameter** only works with the query operation if the property is in the query schema.
8. Optionally, to specify operations to which this parameter rule should or should not apply, select **Specific Operations** and perform steps 2-5 of "Defining specific operations to include" on page 404 or "Defining specific operations to exclude" on page 404.
9. Click **OK**.

   The rule is added to the Parameter Rules list.

Editing a parameter rule

To edit a rule in the Parameter Rules list:

- Select the check box for the rule to edit, and then click **EDIT**.

  The PARAMETER RULE dialog box appears. For more information about using this dialog box, see "Defining parameter rules" on page 405.

Removing a parameter rule

To remove a rule from the Parameter Rules list:

- Select the check box for the rule to remove, and then click **REMOVE**.

Adding and managing allowed hosts in base settings

Use the **Allowed Hosts** setting to add and manage domains to crawl and audit. If your Web application uses multiple domains, add those domains here. For example, if you were scanning "WIexample.com," you would need to add "WIexample2.com" and "WIexample3.com" here if those domains were part of your Web presence and you wanted to include them in the scan.

You can also use this feature to scan any domain whose name contains the text you specify. For example, suppose you specify www.myco.com as the scan target and you enter "myco" as an allowed host. As the sensor scans the target site, if it encounters a

link to any URL containing "myco," it will pursue that link and scan that site's server, repeating the process until all linked sites are scanned. For this hypothetical example, the sensor would scan the following domains:

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

Adding allowed hosts

To add allowed hosts:

1. Click **add allowed host** +.
2. Type a URL in the **Host name** box.

   Important! When you specify the URL, do not include the protocol designator (such as http:// or https://).
3. (Optional) To use a regular expression to represent a URL, select **Use Regular Expression**.
4. Do one of the following:
   - To save the allowed host to the list, click **confirm** ✔.

     The URL is added to the allowed hosts list. To add another allowed host, return to Step 1.
   - To clear the field and start over, click **discard** × and return to Step 1.

Editing or removing allowed hosts

To edit an allowed host:

1. In the **Allowed Hosts** list, click **edit** for the host you want to edit.
2. Edit the host as described in "Adding allowed hosts" above.

To remove an allowed host:

- In the **Allowed Hosts** list, click **delete** × for the host you want to delete.

Configuring scan priority in base settings

Scans are run using a priority ranking from 0 to 10, where 0 is the lowest priority and 10 is the highest. Before starting a scan, the Global Service determines if there is a higher-priority scan that needs to be started. If there is, the lower-priority scan will remain in the

queue. Additionally, a lower-priority scan that is running will be paused for a higher-priority scan if no other sensor is available.

If Advanced Scan Prioritization is enabled, the Global Service may move scans to other sensors, depending on scan priority and other settings. For more information about Advanced Scan Prioritization, see "Understanding advanced scan prioritization" on page 196.

Note: Applications are configured with a default priority level in the application settings. For more information, see "Understanding the Application Settings view" on page 419.

Changing the priority

To select a priority other than the default setting for the scan:

- Select a priority from 0 to 10 in the **Priority** list.

  Note: If you set a priority that differs from the Application Settings, the lower of the two settings will be used.

Tip: You cannot disable scan priority. However, you can set all applications and scans to the same priority to accomplish something similar.

Configuring data retention in base settings

If data retention is enabled for the application being scanned, then a default number of days for scan retention is configured in the application settings. In such cases, the default number of days for scan retention is displayed in the Details page. For more information, see "Working with application settings" on page 418.

To set a number of days other than the default setting for the scan:

- Enter the number of days in the **Data Retention** box.

Note: If you set a number of days that differs from the Application Settings, the lower of the two settings will be used.

Scanning single-page applications in base settings

This topic describes single-page application (SPA) support for crawling and auditing the Document Object Model (DOM) of an application.

The challenge of single-page applications

Developers use JavaScript frameworks such as Angular, Ext JS, and Ember.js to build SPAs. These frameworks make it easier for developers to build applications, but more difficult for security testers to scan those applications for security vulnerabilities.

Traditional sites use simple back-end server rendering, which involves constructing the complete HTML web page on the server side. SPAs and other Web 2.0 sites use front-end DOM rendering, or a mix of front-end and back-end DOM rendering. With SPAs, if the user selects a menu item, the entire page can be erased and recreated with new content. However, the event of selecting the menu item does not generate a request for a new page from the server. The content update occurs without reloading the page from the server.

With traditional vulnerability testing, the event that triggered the new content might destroy other events that were previously collected on the SPA for audit. Through its SPA support, the dynamic sensor offers a solution to the challenge of vulnerability testing on SPAs.

Configuring SPA support

When SPA support is enabled, the DOM script engine finds JavaScript includes, frame and iframe includes, CSS file includes, and AJAX calls during the crawl, and then audits all traffic generated by those events.

To configure SPA support:

- Under **Single-Page Applications** on the Details page, select one of the following options:
  - **Automatic** - If the sensor detects a SPA framework, it automatically switches to SPA-support mode.
  - **Disabled** - Indicates that SPA frameworks are not used in the target application.
  - **Enabled** - Indicates that SPA frameworks are used in the target application.

    Caution! Enable SPA support for single-page applications only. Enabling SPA support to scan a non-SPA website results in a slow scan.

Enabling traffic monitor in base settings

The site tree of a scan normally displays only the hierarchical structure of the website or web service, plus those sessions in which a vulnerability was discovered. If traffic monitor is enabled, then the Traffic Viewer tool and the Traffic table in the scan results allow you to view every HTTP request sent by the sensor and the associated HTTP response received from the web server.

Note: The Traffic Viewer tool is not included with ScanCentral DAST. However, if you have Fortify DAST installed locally, you can use the tool that is included with your local installation.

Option must be enabled

To see all traffic in the Traffic Viewer tool or in the Traffic table in the scan results, you must enable Traffic Monitor logging in the scan settings.

Note: The Traffic table is always available in the scan results in ScanCentral DAST. However, enabling Traffic Monitor logging includes all of the scan traffic.

Enabling traffic monitor logging

To enable traffic monitor logging:

- Under **Traffic Analysis** on the Details page, select **Enable Traffic Monitor**.

Creating and managing basic exclusions in base settings

You can exclude URLs and sessions—based on criteria in their requests or responses—from being crawled and audited. Excluding URLs means that the sensor will not examine the specified URL or host for links to other resources. Excluding sessions means that sensor will not process the sessions that meet the exclusion criteria.

To exclude these items from your scan, you must create a list of Basic Exclusions. Each exclusion in the list identifies one or more targets in which the criteria for exclusion is found.

Note: You can add multiple targets to each entry in the Basic Exclusions list.

Creating exclusions

To create one or more exclusions:

1. Under **Basic Exclusions** on the Details page, click **CREATE**.
   The MANAGE EXCLUSIONS dialog box opens.
2. Type a name for the exclusion in the **Name** box.
3. From the **Target** list, select one of the following target types to configure for exclusion:
   - **Extension** - Excludes file extensions that match the exclusion criteria
   - **Host** - Excludes hosts that match the exclusion criteria
   - **Post parameter** - Excludes sessions with a POST request parameter that matches the exclusion criteria
   - **Query parameter** - Excludes sessions with a query parameter in the URL that matches the exclusion criteria
   - **Request** – Excludes sessions with a request that matches the exclusion criteria
   - **Response** – Excludes sessions with a response that matches the exclusion criteria
   - **Response header** - Excludes sessions with a response header that matches the exclusion criteria
   - **Status code** - Excludes sessions with a response status code that match the

exclusion criteria

- **URL** – Excludes URLs that match the exclusion criteria

4. Type a name for the target in the **Name** box.
5. Select one of the following types of exclusion for the target from the **Type** list:
   - **Matches Regex** – Matches the regular expression you specify in the **String** box
   - **Matches Regex extension** – Matches the regular expression extension you specify in the **String** box
   - **Matches** - Matches the specified criteria in the **String** box
   - **Contains** – Contains the text string you specify in the **String** box
6. Type the string to match in the **String** box.
   For examples of Target, Type, and String settings, see "Exclusion examples" below.
7. Click **add** +.
   The exclusion is added to the exclusion list.
8. Optionally, to create another exclusion, return to Step 3. Otherwise, go to Step 9.
9. When the list of exclusions is complete, click **OK**.

Exclusion examples

The following table provides examples of exclusions.

To...	Create the following exclusion...
Ensure that you never send requests to any resource at Microsoft.com	URL contains `Microsoft.com`
Exclude the following directories: `http://www.test.com/W3SVC55/` `http://www.test.com/W3SVC5/` `http://www.test.com/W3SVC550/`	URL matches regex `/W3SVC[0-9]*/`
Ensure that you never process session responses with 404 Not Found	Response contains `Not Found`

For more information about creating exclusions, see "Understanding and creating inclusive exclusions" on page 201.

Editing or removing exclusions

To edit or remove an entry in the **Basic Exclusions** list:

1. Select an entry from the **Basic Exclusions** list.
2. Do one of the following:
   - To edit the exclusion settings, click **MANAGE**.

     The MANAGE EXCLUSIONS dialog box opens. For more information about using this dialog box, see "Creating exclusions" on page 411.
   - To remove the host from the allowed hosts list, click **REMOVE**.

Configuring redundant page detection in base settings

Highly dynamic sites could create an infinite number of resources (pages) that are virtually identical. If allowed to pursue each resource, the sensor would never be able to finish the scan. The **Perform redundant page detection** option compares page structure to determine the level of similarity, allowing the sensor to identify and exclude processing of redundant resources.

Important! Redundant page detection works in the crawl portion of the scan. If the audit introduces a session that would be redundant, the session will not be excluded from the scan.

To configure redundant page detection:

1. Select the **Perform redundant page detection** check box.
2. Configure settings as described in the following table.

Setting	Description
Page Similarity Threshold (%)	Indicates how similar two pages must be to be considered redundant. Enter a percentage from 1 to 100, where 100 is an exact match. The default setting is 95 percent.
Tag attributes to include	Identifies the tag attributes to include in the page structure. Typically, tag attributes and their values are dropped when determining structure. Identifying tag attributes in this list adds those attributes and their values in the page structure. By default, `id` and `class` tag attributes are included. To add tag attributes: a. Type the attribute name in the **Tag item** box. Do not include tag brackets (< and >).

Setting	Description
	b. Click **ADD**. The tag attribute is added to the **Tag attributes to include** list. **Tip:** Certain sites may be primarily composed of one type of tag, such as `<div>`. Including these attributes creates a more rigid page match. Excluding these attributes creates a less strict match.

Enabling SAST correlation in base settings

SAST correlation correlates the static and dynamic findings for your web application in Application Security. Correlation enables you to see the static findings that were also found in a dynamic scan. It can help you to prioritize which issues to fix and help verify that those issues are not false positives.

To enable SAST correlation:

- Select **Enable SAST Correlation**.

Applying base settings to applications

Base settings are applied at the application level. Therefore, when configuring base settings, you must select one or more applications to which the settings will apply.

To select applications on the **Applications** page:

- To assign the base settings to all existing and future applications, slide the toggle to **Grant all application access**.
- To assign the base settings to individual applications, slide the toggle to **Assign individual applications**, and then select individual application check boxes in the **APPLICATIONS** list.

  Note: Only selected applications will have access to the base settings.

What's next?

After you have selected applications, click **NEXT** and proceed with "Reviewing and saving base settings" below.

Reviewing and saving base settings

On the Review page, you can review a summary of the base settings that you configured and save the settings for others to use.

To save the base settings:

1. On the **Review** page, type a name for the base settings in the **Name** box.
2. Click **SAVE**.

   The base settings are added to the ScanCentral DAST database and appear in the base settings list. For more information, see "Understanding the Base Settings view" on page 374.

Working with Administration settings

Administration settings apply to the following areas of ScanCentral DAST:

- Metrics & Tracking.
- Templates
- Users
- Plugins
- Policies
- Configuration

Note: For more information on these settings, refer to the Open Text Application Security documentation.

Configuration

This section are used to configure the following ScanCentral DAST settings:

- AI Assistant
- AppSec Training
- BIRT Reports
- Core
- Customization
- Email
- Issue Audit
- JMS
- Kafka Stream
- LDAP Servers
- Maintenance
- Processing Rules
- Proxy
- SCIM

- SSO
- ScanCentral DAST
- ScanCentral SAST
- Scheduler
- Security
- Seed Bundles
- Webhooks

ScanCentral DAST

The ScanCentral DAST settings are used to turn on ScanCentral DAST and manage Service Credentials.

ScanCentral DAST

To turn on ScanCentral DAST:

1. Select the **Enable ScanCentral DAST** check box.
2. Enter the ScanCentral DAST server URL in the textbox.
3. Click **Save**.

Service credentials

Service credentials are used to give administrator users secure and controlled access to ScanCentral DAST credentials management. You can add service credentials, view sessions, edit existing credentials, reset the credential secret, and remove credentials.

To add service credentials:

1. Click **+ SERVICE CREDENTIALS**.
   The **CREATE NEW SERVICE CREDENTIALS** dialog box opens.
2. In the **CREATE NEW SERVICE CREDENTIALS** dialog box:
   a. Enter a **Name** for the new service credentials.
   b. Enter an optional **Description**.
   c. Enter an **Expiration** for the service credentials (in minutes).
   d. Select **Enabled**.
3. Click **OK** to continue or **CANCEL** to close the dialog box without saving.
4. In the **SERVICE CREDENTIALS CREATED** dialog box, copy the **Client ID** and the **Client secret**.

   Important! Copy and save the **Client ID** and the **Client secret** for future use; they will not be available after closing this dialog box.

5. Click OK to close the **SERVICE CREDENTIALS CREATED** dialog box.

To view sessions associated with service credentials:

1. Click **View sessions** for the selected service credentials.
   The **Sessions** dialog box opens.
2. Click **Refresh** to update the sessions list.
3. Select an option from the **Items per page** list to change the number of sessions displayed.
4. Click **OK** to close the **Sessions** dialog box.

To edit a service credentials:

1. Click **Edit**.
2. Change the **Name**, **Description**, or **Expiration** as needed.
3. Select **Enabled** to turn the credentials on or off.
4. Click **OK** to save your changes or **CANCEL** to revert to the previous settings.

To reset a service credentials secret:

1. Click Reset secret for the selected credentials.
   The **RESET SECRET** dialog box opens.
2. In the **RESET SECRET** dialog box, enter an optional reason for the reset in the Reset reason text box.
3. Click **OK** to continue or **CANCEL** to close the **RESET SECRET** dialog box without resetting the secret.
   New credentials are created and displayed.
4. In the **RESET SECRET** dialog box, copy the **Client ID** and the **Client secret**.
5. Click OK to close the **RESET SECRET** dialog box.

To remove service credentials:

1. Select the check box for the service credentials to be removed.
2. Click **DELETE**.
3. In the **DELETE SELECTED SERVICE CLIENT CREDENTIALS** dialog box, enter an optional reason for the deletion in the **Delete service credentials reason** text box.
4. Click **OK** to continue or **CANCEL** to close the **DELETE SELECTED SERVICE CLIENT CREDENTIALS** dialog box without deleting the selected credentials.
   The **SERVICE CREDENTIALS DELETED** dialog box opens.
5. Click **OK** to close the **SERVICE CREDENTIALS DELETED** dialog box.

Chapter 14: Working with application settings

Application settings apply to applications and generally override settings that are made in scan settings. Application settings such as scan priority, data retention, SAST correlation, domain restrictions, and private data settings are created and maintained by Application Security users who have permission to manage ScanCentral DAST deny intervals and other global settings.

Application settings are global settings

Global settings are those that apply or may apply to all of your applications, scans, scan schedules, sensors, or sensor pools.

Priority

Scans for an application are run using a priority ranking from 0 to 10, where 0 is the lowest priority and 10 is the highest. Applications are configured with a default priority level in the application settings. For more information, see "Configuring scan priority" on page 195 or "Configuring scan priority in base settings" on page 408.

Data retention

When a scan is run, it creates several artifacts, including scan logs, an FPR, a site tree, and a scan file. Configuring data retention settings for an application can aid in preventing your ScanCentral DAST database from becoming full. Purging the scan data from ScanCentral DAST does not delete the FPR from Application Security.

Applicable scans for domain restrictions

Domain restrictions allow the scanning of a specific IP address, range of IP addresses, or a domain or host. Application setting domain restrictions apply only to Standard scans or API scans that use a start URL.

Accessing the Application Settings view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with ScanCentral DAST application settings directly in Application Security.

To access the ScanCentral DAST Application Settings view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Application Settings**.
   The Application Settings view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Application Settings view

The Application Settings view displays in a table the settings for each of the applications in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each application.

Column	Description
Application	Identifies the application to which the settings apply.
Priority	Specifies the default priority of scans that are run for the application. For more information, see "Configuring scan priority" on page 195 or "Configuring scan priority in base settings" on page 408.
Data Retention	Indicates whether data retention is configured for scans of the application. Settings are **Enabled** and **Disabled**.
Retention	Specifies the number of days to retain scan data in the ScanCentral

Column	Description
Days	DAST database.
Sast Correlation	Indicates whether SAST correlation is configured for scans of the application. Settings are **Enabled** and **Disabled**.
Global Restrictions	Indicates whether global restrictions are configured for scans of the application. Settings are **Enabled** and **Disabled**. For more information, see "Working with global restrictions" on page 440.
Has Domain Restrictions	Indicates whether domain restrictions are configured for scans of the application. Settings are **Yes** and **No**.
Global Private Data Settings	Indicates whether global private data settings are configured for scans of the application. Settings are **Enabled** and **Disabled**. For more information, see "Working with private data settings" on page 443.
Has Private Data Settings	Indicates whether private data settings are configured for scans of the application. Settings are **Yes** and **No**.

Understanding the application setting detail panel

When you select an entry in the Application Settings view, the application settings detail panel appears. The detail panel displays the information from the Application Settings table for the selected application.

If global restrictions are enabled, the detail panel displays the list of allowed IP addresses or hosts or both. If specific domain restrictions are configured for the application, the detail panel displays the list of allowed IP addresses or hosts or both.

Important! For domain restrictions, ScanCentral DAST merges the global and application-level restrictions. If the URL passes either the global or application-level restrictions, the scan will run.

Additionally, the detail panel provides an option to edit the settings for the selected application.

Managing application settings

You can edit existing application settings and refresh the settings that are displayed in the Application Settings view.

Editing application settings

To edit application settings:

1. In the **Application Settings** view, select one or more check boxes for the application settings to edit.
2. Click **EDIT**.

   The APPLICATION SETTINGS wizard opens pre-populated with the selected application settings.

   Note: If you select multiple application settings to edit, then the APPLICATION SETTINGS wizard will display default settings rather than those of the selected applications.

3. On the **Getting Started** page, continue according to the following table.

To...	Then...
Edit scan priority	In the **Priority** drop-down list, select a new priority.
Enable data retention	a. Slide the **Data Retention Disabled** toggle to **Data Retention Enabled**. b. In the **Number of days for retention** box, select a number of days to retain scans in the database.
Disable data retention	Slide the **Data Retention Enabled** toggle to **Data Retention Disabled**.
Enable SAST correlation	Slide the **SAST Correlation Disabled** toggle to **SAST Correlation Enabled**.
Disable SAST correlation	Slide the **SAST Correlation Enabled** toggle to **SAST Correlation Disabled**.

4. On the **Domain Restrictions** page, continue according to the following table.

To...	Then...
Enable global restrictions	Slide the **Global Domain Restrictions Disabled** toggle to **Global Domain Restrictions Enabled**.
Disable global restrictions	Slide the **Global Domain Restrictions Enabled** toggle to **Global Domain Restrictions Disabled**.
Create an application domain restriction	a. Click **NEW**. b. Continue with the steps in "Creating or editing an application domain restriction" on the next page.
Edit an existing application domain restriction	a. In the **APPLICATION DOMAIN RESTRICTIONS** area, select the restriction to edit. b. Click **EDIT**. c. Continue with the steps in "Creating or editing an application domain restriction" on the next page.
Delete an application domain restriction	a. In the **APPLICATION DOMAIN RESTRICTIONS** area, select the restriction to delete. b. Click **DELETE**.

5. On the **Private Data Settings** page, continue according to the following table.

To...	Then...
Enable global private data settings	Slide the **Global Private Data Settings Disabled** toggle to **Global Private Data Settings Enabled**.
Disable global private data settings	Slide the **Global Private Data Settings Enabled** toggle to **Global Private Data Settings Disabled**.
Create an application private data setting	a. Click **NEW**. b. Continue with the steps in "Creating or editing an application private data setting" on page 424.

To...	Then...
Edit an existing application private data setting	a. In the **APPLICATION PRIVATE DATA SETTINGS** area, select the data setting to edit. b. Click **EDIT**. c. Continue with the steps in "Creating or editing an application private data setting" on the next page.
Delete an application private data setting	a. In the **APPLICATION PRIVATE DATA SETTINGS** area, select the data setting to delete. b. Click **DELETE**.

6. Click **OK**.

Refreshing the Application Settings view

Generally, the changes that you make to the application settings appear right away on the Application Settings view. However, if other users have access to the same applications, any changes they make will not be updated in your view. To see such changes, you can manually refresh the Application Settings view.

To refresh the Application Settings view:

- Click **REFRESH**.

Creating or editing an application domain restriction

You can create or edit an application domain restriction in the DOMAIN RESTRICTION dialog box of the APPLICATION SETTINGS wizard. For information about accessing this wizard, see "Managing application settings" on page 420.

To create or edit an application domain restriction in the DOMAIN RESTRICTION dialog box:

1. Optionally, in the **Restriction Name** box, type a name for the restriction.
2. Continue according to the following table.

To allow a...	Do this...
Specific IP address	a. In the **Domain Restriction Type** list box, select **IP address**. b. In the **IP Address** box, type the IP address to restrict.
Range of IP addresses	a. In the **Domain Restriction Type** list box, select **IP address range**. b. In the **From** box, type the first IP address in the range. c. In the **To** box, type the last IP address in the range.
Domain or host	a. In the **Domain Restriction Type** list box, select **Host**. b. In the **Host** box, type the domain or host name. **Note:** You can enter only one domain or host name. To allow additional hosts, you must create a domain restriction for each host.

3. Click **OK**.

Creating or editing an application private data setting

You can create or edit an application private data setting in the PRIVATE DATA CONFIGURATION dialog box of the APPLICATION SETTINGS wizard. For information about accessing this wizard, see "Managing application settings" on page 420.

To create or edit an application private data setting in the PRIVATE DATA CONFIGURATION dialog box:

1. In the **Type** list, select a type of data to use for matching on information in the scan and log files. Options are **Regex** or **Literal**.
2. In the **Match** box, do one of the following:
   - For **Regex** type matches, construct a regular expression as match criteria.
   - For **Literal** type matches, type the exact text to use as match criteria.
3. In the **Replace** box, type the value to use for masking private data that is found.
4. Click **OK**.

Chapter 15: Working with two-factor authentication

Two-factor authentication augments the standard password, which is defined as the "something you know" factor, with one of the following:

- Something you have, such as a one-time passcode (OTP) sent by SMS or email
- Something you are, such as your fingerprint, face, or retina

While this second factor of authentication improves security, it adds a layer of complexity when conducting an automated scan of web applications that implement it.

OpenText engineers have developed a method and process that enable Fortify DAST sensors and the Event-based Web Macro Recorder to automate the "something you have" factor of two-factor authentication.

How scanning with two-factor authentication works

ScanCentral DAST includes a 2FA Server Docker image that you configure for a control center to process the SMS and email responses coming from your application server. There is also a mobile application that forwards SMS responses to the control center. The control center queues the responses and forwards them to the appropriate TruClient browser when needed for authentication. For more information about the 2FA Server Docker image and container, see "ScanCentral DAST with two-factor authentication" on page 44.

Recommendation

OpenText strongly recommends that you use test phones and test email addresses only. For privacy concerns, do not use personal phones and email addresses.

Known limitations

The following known limitations apply to the two-factor authentication feature:

- IMAP and POP3 servers are supported. However, only POP3 servers that support unique ID listing (UIDL) are supported.

- Currently, login macros with two-factor authentication using email support only the Basic authentication method for IMAP or POP3.
- Currently, only Android mobile phones are supported.
- The mobile phone requires a Wi-Fi connection in the same subnet where the Fortify DAST sensor is installed.

Facts about Gmail accounts

Be aware of the following facts related to Gmail accounts:

- Gmail account settings include normal mode and recent mode. If you use a Gmail account and experience issues with new incoming emails, using recent mode might resolve this issue. To enable recent mode, configure the account name in your POP3 account settings using the following format:

  `recent:<email_address@gmail.com>`
- For security, Google uses "Sign in with Google" to connect Gmail to a user's Google account and does not accept user-created passwords. When using a Gmail account, you must create and use a Google app password. For more information, refer to Google account documentation for creating and using app passwords.

Configuring two-factor authentication in ScanCentral DAST

The scanner service Docker compose file and environment file for Linux containers includes settings that pull and start the 2FA Server container. For more information, see "Configuring the TLS environment file for the scanner service" on page 109 and "Configuring the mTLS environment file for the scanner service" on page 120.

Before you can conduct a scan using two-factor authentication, you must configure the 2FA server in ScanCentral DAST. For more information, see "Creating a 2FA Server" on page 429.

Conducting a scan using two-factor authentication

After you have configured two-factor authentication in ScanCentral DAST, you can conduct a scan using two-factor authentication. The following table describes the process for conducting such a scan.

Stage	Description
1.	In the Event-based Web Macro Recorder, record a login macro and modify it as follows: 1. Add and configure a **Two-factor authentication** group step. **Note:** You must configure the group step for SMS or email responses. The group step includes a **Wait for 2FA** step that you must also configure. 2. Optionally, create user name, password, phone number, email, and email password parameters. Using parameters for two-factor authentication enables you to conduct a multi-user login scan. 3. Configure the **Wait for 2FA** step. 4. Add a **Generic Object Action** step and configure it as a **Type** step. 5. Add a **Generic Object Action** step and configure it as a **Click** step. For more information, see the *OpenText™ Fortify DAST Tools Guide*.
2.	In the Web Macro Recorder, replay the login macro.
3.	In ScanCentral DAST, run a scan using the macro. For more information, see "Configuring a scan" on page 150.

Accessing the Two Factor Authentication view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can set up and manage two-factor authentication for your scans directly in Application Security. Two-factor authentication servers that are configured in ScanCentral DAST appear in the Two Factor Authentication view.

To access the Two Factor Authentication view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Two Factor Authentication**.
   The Two Factor Authentication view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules,

and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission.

Understanding the Two Factor Authentication view

The Two Factor Authentication view displays in a table the two-factor authentication servers that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each two-factor authentication server.

Column	Description
Name	Indicates the name of the two-factor authentication server.
Root URL	Indicates the hostname and port where the 2FA Server Docker container is running.
Status	Indicates the current status of the 2FA Server container. Possible statuses are: • **Online** – The server is running and capable of processing SMS or email responses or both. • **Offline** – The server is not running. • **Unknown** – The status of the server cannot be determined. • **InvalidAuthToken** – The access token is not valid. **Note:** This is *not* the master token used in the run command for the 2FA Server container. During 2FA Server configuration, ScanCentral DAST creates an access token to authenticate communication with the 2FA server. InvalidAuthToken refers to this access token.
Status Time	The date and time when the 2FA Server container entered its current status.
Access Token Created	The date and time when the access token was created by ScanCentral DAST for the 2FA Server.
Access Token	The date and time when the access token for the 2FA Server

Column	Description
Expiration	expires. **Important!** Upon expiration, ScanCentral DAST automatically creates a new token. After this date, however, you must generate a new QR code and scan it to update the settings on your mobile phone. For more information, see "Configuring a mobile device" on page 438.

Understanding the two-factor authentication detail panel

When you select a server in the Two Factor Authentication view, the two-factor authentication detail panel appears. The server name and root URL appear at the top of the panel, along with the information from the Two Factor Authentication table for the selected 2FA Server.

The detail panel also provides options to edit and delete the selected 2FA Server, as well as join a mobile device to the server.

Creating a 2FA Server

You can use the TWO FACTOR AUTHENTICATION wizard to create a 2FA Server that will process the SMS and email responses coming from your application server. During creation, you must assign the 2FA Server to sensor pools.

Important! If the 2FA Server Docker image has not been downloaded and started in a container, then you cannot verify the server configuration.

To create a 2FA Server:

1. On the **Two Factor Authentication** page, click **+ NEW 2FA SERVER**.
   The TWO FACTOR AUTHENTICATION wizard opens.
2. On the **Getting Started** page, enter the following information:
   - In the **2FA Server Name** box, enter a name for the server.
   - In the **Root URL** box, enter the URL and port number for the 2FA server.

     Tip: This is the URL for the host running the 2FA Server. The default port is 443.

     Important! For SMS two-factor authentication, you must enter the public network IP address of the Docker host. For email two-factor authentication, you may enter the Docker container's internal IP address.

- In the **Token** box, enter the master token GUID that you previously generated for the server. For more information, see "Configuring the TLS environment file for the scanner service" on page 109.

3. Click **VERIFY**.
   Connection to the 2FA Server is validated.

   Tip: If you are unable to validate a connection to the server, ensure that the 2FA Server Docker image has been downloaded and started in a container.

4. Click **NEXT**.
   The Sensor Pools page appears.
5. In the **SENSOR POOLS** list, select one or more check boxes to assign to the 2FA Server.

   Important! Only sensors in the selected pools will run scans that use two-factor authentication.

6. Click **NEXT**.
   The Review page appears.
7. Click **NEXT**.
   The Join mobile device page appears.
8. Do one of the following:
   - If your application server sends email responses only, then click **CANCEL**.
   - If your application server sends SMS responses, then proceed with "Configuring a mobile device" below.

Configuring a mobile device

If your application server sends SMS responses, then you must install the **Fortify2FA** mobile application on a mobile device and download your two-factor authentication settings to it. After configuration, the mobile application receives the SMS response and forwards it to the 2FA Server.

Note: Currently, the mobile application is available only for Android operating systems.

To configure the mobile application on the **Join mobile device** page:

1. Have you already downloaded and installed the **Fortify2FA** mobile application on the mobile device?
   - If *yes*, start the application on the mobile device, and then go to step 2.
   - If *no*, go to step 2.
2. In the **Mobile Phone** field, enter the phone number that will receive SMS responses.

3. Click **GENERATE QR CODE**.
   The 2FA Server generates a quick response (QR) code that includes the two-factor authentication settings and a link to download the mobile application.
4. Do one of the following:
   - To configure the application, use the mobile phone's camera to scan the QR code.
   - To install and configure the mobile application, proceed to "Installing and configuring the Fortify2FA mobile app" below.

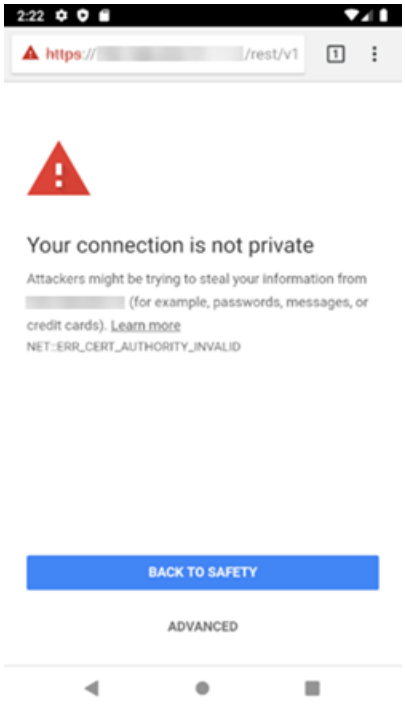
   Tip: If you use multiple threads in the scan, you might want to use more than one phone. Using the same phone number for multi-user scans can affect the scan time.

Installing and configuring the Fortify2FA mobile app

To install and configure the mobile application on a phone that will receive SMS responses:

1. Use the mobile phone's camera to scan the QR code on the **Join mobile device** page.
   A link appears.
2. Click the link (or **Open** button) to access the site for downloading the app.

A warning about the self-signed certificate appears.

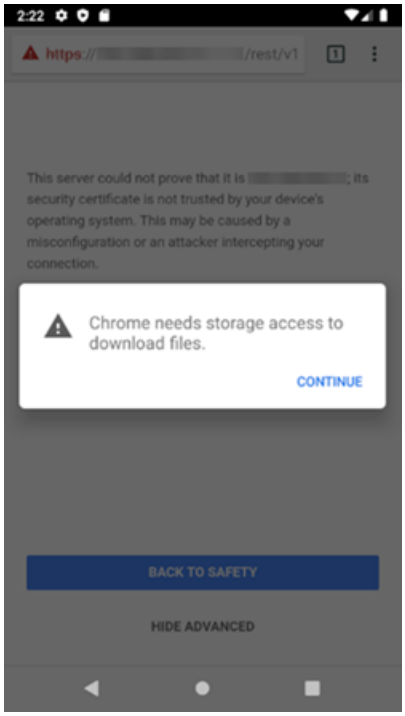


3. Click **ADVANCED**.
   Additional information is provided along with a link to proceed.

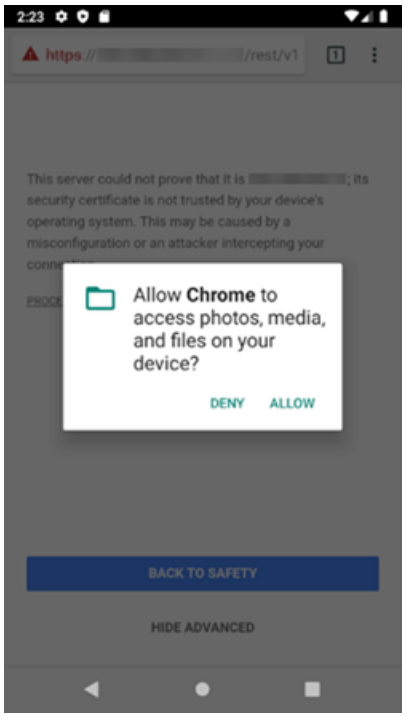


4. Click **PROCEED TO *<ip_address>* (UNSAFE)**.

A prompt requests storage access to download files.



5. Click **CONTINUE**.
   A prompt requests access to photos, media, and files on the device.

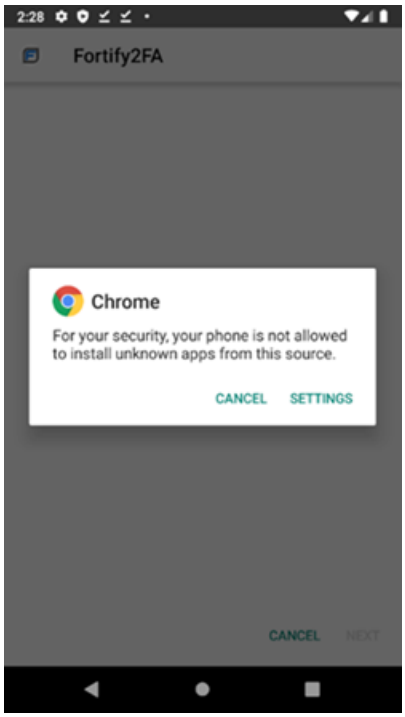


6. Click **ALLOW**.

The fortify-2fa.apk file is downloaded.

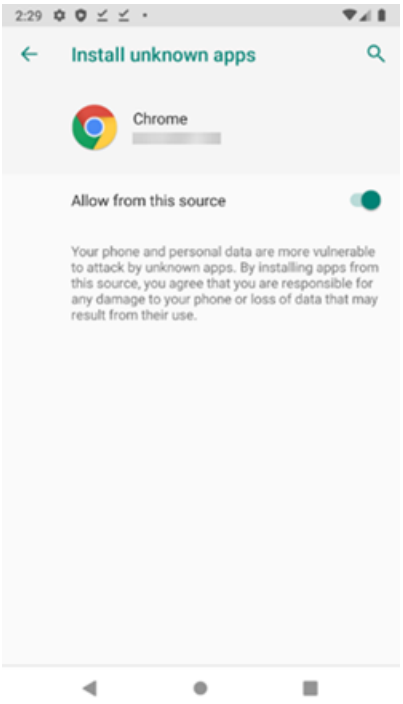


7. Click **OPEN**.
   A prompt advises about installing unknown apps.

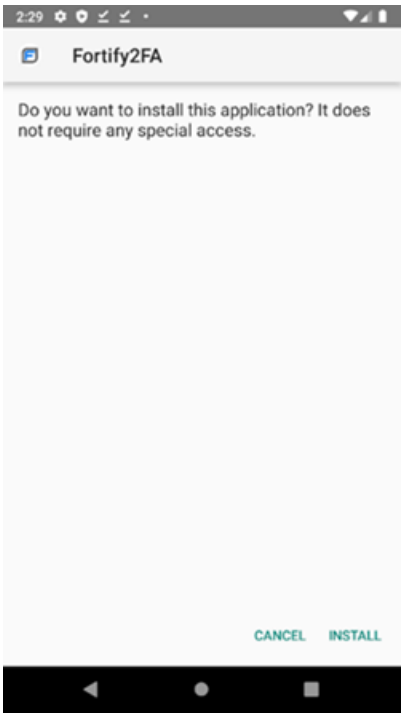


8. Click **SETTINGS**.

The Install unknown apps setting appears.

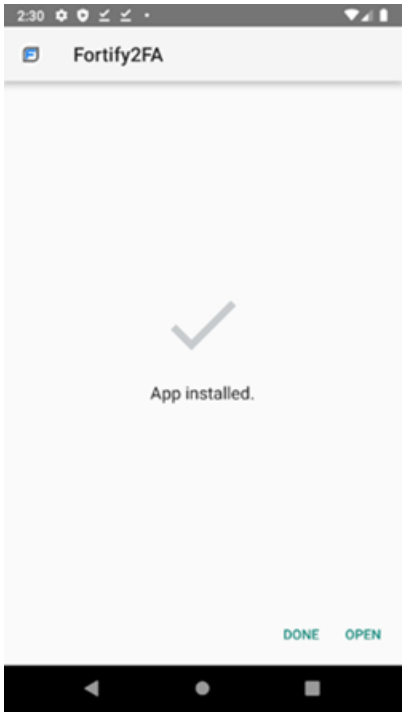


9. Enable **Allow from this source**.
   A prompt asks if you want to install the application.

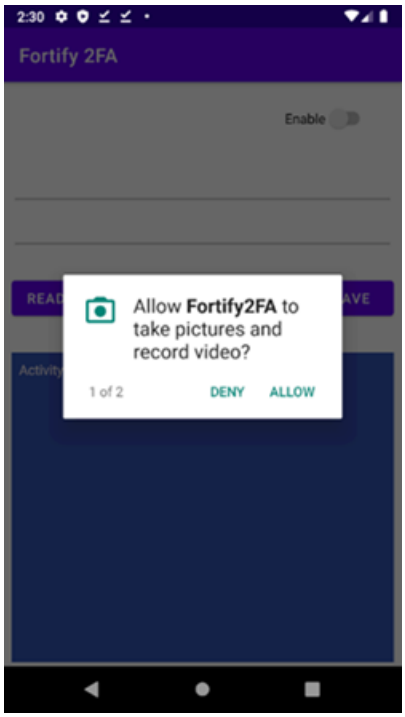


10. Click **INSTALL**.

A message indicates that the app is installed.

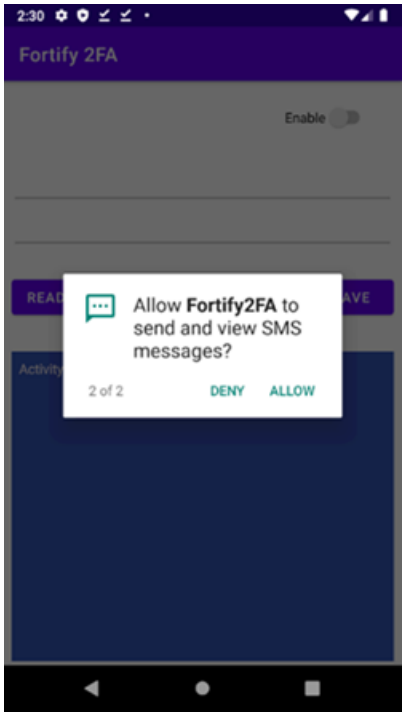


11. Click **OPEN**.
    A prompt requests permission to take pictures and record video.

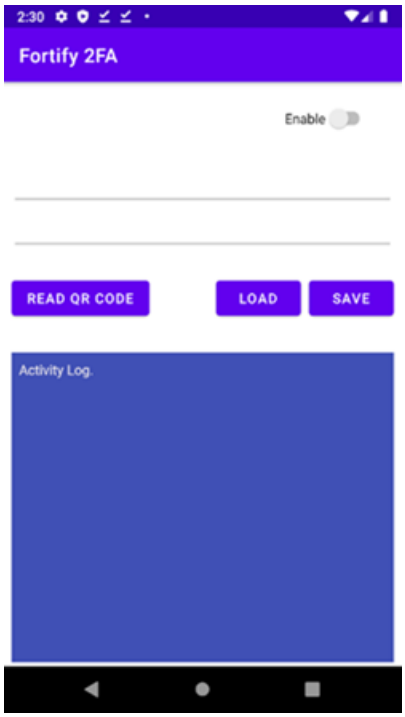


12. Click **ALLOW**.

A prompt requests permission to send and view SMS messages.



13. Click **ALLOW**.
    The app is ready to be configured.



14. Click **READ QR CODE** to scan the QR code on the **Join mobile device** page.
    The two-factor authentication settings are configured in the **Fortify2FA** mobile application.

Managing 2FA Servers

You can edit and delete 2FA Servers, and refresh the servers that are displayed on the Two Factor Authentication view. Additionally, you can configure a new mobile device or update settings for an existing device on the two-factor authentication detail panel.

Editing a 2FA Server

To edit a 2FA Server:

1. In the **Two Factor Authentication** view, select the 2FA Server to edit.
   The two-factor authentication detail panel appears.
2. Click **EDIT**.
   The TWO FACTOR AUTHENTICATION wizard opens with the settings visible for the selected 2FA Server.
3. To make edits, follow the procedure in "Creating a 2FA Server" on page 429.

Deleting a 2FA Server

To delete a 2FA Server, do one of the following:

- Select one or more check boxes for 2FA Servers in the **Two Factor Authentication** view, and then click **DELETE** at the bottom of the table.
- Select a 2FA Server to view the two-factor authentication details, and then click **DELETE** at the bottom of the two-factor authentication detail panel.

Refreshing the 2FA Server list

Generally, the changes that you make to 2FA Servers appear right away on the Two Factor Authentication view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Two Factor Authentication view:

- Click **REFRESH**.

Configuring a mobile device

If your application server sends SMS responses, then you must install the **Fortify2FA** mobile application on a mobile device and download your two-factor authentication settings to it. After configuration, the mobile application receives the SMS response and forwards it to the 2FA Server.

Note: Currently, the mobile application is available only for Android operating systems.

During 2FA Server configuration, ScanCentral DAST creates an access token to authenticate communication with the 2FA server. By default, the access token is valid for one year. Upon expiration, ScanCentral DAST automatically creates a new access token. When this occurs, you must generate a new QR code and scan it to update the existing settings on your mobile phone.

You can configure a new mobile device or update settings for an existing device on the two-factor authentication detail panel.

To configure the mobile application:

1. In the **Two Factor Authentication** view, select the 2FA Server to edit.
   The two-factor authentication detail panel appears.
2. Click **JOIN MOBILE DEVICE**.
   The JOIN MOBILE DEVICE dialog box appears.
3. Have you already downloaded and installed the **Fortify2FA** mobile application on the mobile device?
   - If *yes*, start the application on the mobile device, and then go to step 4.
   - If *no*, go to step 4.
4. Click **GENERATE QR CODE**.
   The 2FA Server generates a quick response (QR) code that includes the two-factor authentication settings and a link to download the mobile application.
5. Do one of the following:
   - To configure the mobile application, use the mobile phone's camera to scan the QR code.
   - To install and configure the mobile application, proceed to "Installing and configuring the Fortify2FA mobile app" on page 431.

Tip: If you use multiple threads in the scan, you might want to use more than one phone. Using the same phone number for multi-user scans can affect the scan time.

Chapter 16: Working with global restrictions and private data settings

You can configure global restrictions and private data settings that apply globally to all scans. You can disable the global aspect of these restrictions and settings, and apply them to individual applications in the Application Settings view. The following pages describe creating, viewing, and managing global restrictions and private data settings.

Working with global restrictions

You can configure global restrictions that limit a user's ability to scan by host, IP address, or range of IP addresses. Global restrictions *allow* scanning of the specified IP addresses or hosts. By default, global restrictions apply to all scans. However, you can disable global restrictions for individual applications in the Application Settings view. For more information, see "Managing application settings" on page 420.

Important! For domain restrictions, ScanCentral DAST merges the global and application-level restrictions. If the URL passes either the global or application-level restrictions, the scan will run.

Applicable scans

Global Restrictions apply only to Standard scans or API scans that use a start URL.

Accessing the Global Restrictions view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with global restrictions directly in Application Security.

To access the Global Restrictions view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Global Restrictions**.
   The Global Restrictions view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules,

and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to global restrictions may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Understanding the Global Restrictions view

The Global Restrictions view displays in a table the global domain restrictions that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each domain restriction.

Column	Description
Name	Optionally, indicates the name given to the restriction upon creation.
Restriction Type	Indicates the type of restriction. Options are: • **Single** – A single IP address is allowed. • **Range** – A range of IP addresses is allowed. • **Host** – A single domain or host name is allowed.
Restriction	Specifies the restriction value—an IP address, a range of IP addresses, or a host name.

Creating a global restriction

You can create a global restriction for an IP address, range of IP addresses, or host name. Restrictions for IP addresses support Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6).

Tip: You can use an asterisk (*) as a wild card character at the beginning of a domain name, such as *.webappsecurity.com, or at the end of an IP address, such as 172.16.*.*.

To create a global restriction:

1. On the **Global Restrictions** view, click **+ RESTRICTION**.
   The DOMAIN RESTRICTION dialog box opens.
2. Optionally, in the **Restriction Name** box, type a name for the restriction.
3. Continue according to the following table.

To allow a...	Do this...
Specific IP address	a. In the **Domain Restriction Type** list box, select **IP address**. b. In the **IP Address** box, type the IP address to restrict.
Range of IP addresses	a. In the **Domain Restriction Type** list box, select **IP address range**. b. In the **From** box, type the first IP address in the range. c. In the **To** box, type the last IP address in the range.
Domain or host	a. In the **Domain Restriction Type** list box, select **Host**. b. In the **Host** box, type the domain or host name. **Note:** You can enter only one domain or host name. To allow additional hosts, you must create a domain restriction for each host.

4. Click **OK**.
   The restriction is added to the Global Restrictions view and applied to all applications that have Global Domain Restrictions enabled.

Managing global restrictions

You can edit and delete global restrictions, and refresh the Global Restrictions view.

Editing a global restriction

To edit a global restriction:

1. In the **Global Restrictions** view, select the global restriction to edit.
2. Click **EDIT**.
   The DOMAIN RESTRICTION dialog box opens.
3. Edit the fields as needed.

   Note: For a description of the fields, see "Creating a global restriction" on the previous page.

4. Click **OK**.
   The changes are saved in the ScanCentral DAST database.

Deleting a global restriction

To delete a global restriction:

- Select one or more check boxes for global restrictions in the **Global Restrictions** view, and then click **DELETE** at the bottom of the table.

Refreshing the Global Restrictions view

Generally, the changes that you make to global restrictions appear right away on the Global Restrictions view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Global Restrictions view:

- Click **REFRESH**.

Working with private data settings

You can configure private data settings that remove personally identifiable information from the scan and log data upon scan completion. By default, private data settings apply to all scans. However, you can disable private data settings for individual applications in the Application Settings view. For more information, see "Managing application settings" on page 420.

Accessing the Private Data Settings view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with private data settings directly in Application Security.

To access the Private Data Settings view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Private Data Settings**.
   The Private Data Settings view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to private data settings may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Understanding the Private Data Settings view

The Private Data Settings view displays in a table the private data settings that are available in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each private data setting.

Column	Description
Private Data Type	Indicates the type of data used for matching on information in the scan. Possible values are **Regex** and **Literal**.
Match	Specifies the regular expression or literal text used as match criteria to identify private data.
Replace	Specifies the value used for masking the private data in scans and log files.

Default Private Data Settings

There are three default private data settings:

- Credit or debit card number
- IP address
- Social Security Number

You can delete these default settings. However, in the case of accidental deletion, you must recreate them. There is no way to restore private data settings.

Creating private data settings

You can create a private data setting that applies to all applications that have Global Private Data Settings enabled.

To create a private data setting:

1. On the **Private Data Settings** view, click **+ PRIVATE DATA SETTING**.
   The PRIVATE DATA CONFIGURATION dialog box opens.
2. In the **Type** list, select a type of data to use for matching on information in the scan and log files. Options are **Regex** or **Literal**.
3. In the **Match** box, do one of the following:

- For **Regex** type matches, construct a regular expression as match criteria.
- For **Literal** type matches, type the exact text to use as match criteria.

4. In the **Replace** box, type the value to use for masking private data that is found.
5. Click **OK**.

The private data setting is added to the Private Data Settings view and applied to all applications that have Global Private Data Settings enabled.

Managing private data settings

You can edit and delete private data settings, and refresh the Private Data Settings view.

Editing a private data setting

To edit a private data setting:

1. In the **Private Data Settings** view, select the private data setting to edit.
2. Click **EDIT**.
   The PRIVATE DATA CONFIGURATION dialog box opens.
3. Edit the fields as needed.

   Note: For a description of the fields, see "Creating private data settings" on the previous page.

4. Click **OK**.
   The changes are saved in the ScanCentral DAST database.

Deleting a private data setting

To delete a private data setting:

- Select one or more check boxes for private data settings in the view, and then click **DELETE** at the bottom of the table.

Refreshing the Private Data Setting view

Generally, the changes that you make to private data settings appear right away on the Private Data Setting view. However, if other users have access to the same view, any changes they make will not be updated in your view. To see such changes, you can manually refresh the view.

To refresh the Private Data Settings view:

- Click **REFRESH**.

Chapter 17: Working with key stores and artifacts repositories

Key stores and artifacts repositories help you streamline the management of values in scan settings and the files used in settings, such as workflow macros, login macros, and client certificates. The following pages describe key stores and artifacts repositories.

Understanding key stores

Key stores provide a way to create variables that you can use in scan settings, base settings, and macro parameters. Creating a key store generates placeholder text that you can use in settings fields that accept string data. Values for the placeholder text are stored in key store entries. When a scan starts in ScanCentral DAST using the settings file, the placeholder text is replaced with the latest values from the key store.

When you save scan settings that use key store placeholder text, a background process generates an OpenText DAST (Fortify WebInspect) composite settings file that you can download. This settings file includes the latest values from the key store entries. However, the key store references are removed and the values in this file are static.

When you edit a key store, a background process uses the latest values to generate new Fortify DAST composite settings files for any scan settings that use the updated key store. When the settings are regenerated, the Modified date for the settings is updated. For more information, see "Understanding the Settings List view" on page 348.

Benefit of using key stores

Key stores allow you to manage scan settings values in a single location. For example, if scan settings use an API token that changes frequently, you can use a key store to store the token value. Scan settings can reference the key store entry by using the placeholder text instead of the API token. When the token changes, a single change to the key store entry is all that is needed.

Key store placeholder format

The format for key store entry placeholder text is as follows:

```
${DAST_KS_KeyStoreName_KeyStoreEntryName}
```

Any entry in a field that includes the format `${DAST_KS_KeystoreName_KeyStoreEntryName}` is identified by ScanCentral DAST as a key store placeholder. If you manually edit this placeholder to include two sequential underscore characters, such as

${DAST_KS_KeystoreName__KeyStoreEntryName}, or any other change that alters the format, it will no longer be identified by ScanCentral DAST as a key store placeholder.

Placeholder text in exported/imported settings

When you export scan settings that use key store placeholder text from ScanCentral DAST, the placeholder text is replaced with the actual values from the key store. Importing the scan settings back into ScanCentral DAST uses the key store values at the time the settings were created, rather than the key store placeholder text.

Types of key store entries and their usage

There are three types of key store entries:

- **Text** – for use in any field that accepts string input, except for the Policy ID field.
- **URL** – for use in fields that accept URLs only.
- **Password** – for use with data that should be treated as a password. The entry is masked and is not visible in the UI.

You cannot use key store entries in the names of base settings or scan settings.

URL key store entry validation

URL fields require key store entry values to be valid URLs. Therefore, URL fields are validated against the value of the selected key store entry rather than the placeholder text.

Key stores in login macros

To use a key store in a login macro, you must first create a parameterized login macro and import it when creating a scan. For more information, see the "Working with Parameters" topic in the Event-based Web Macro Recorder chapter of the *OpenText™ Fortify DAST Tools Guide*.

Accessing the Key Stores view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with key stores directly in Application Security.

To access the Key Stores view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.

2. In the left panel, select **Key Stores**.
   The Key Stores view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to key stores may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Understanding the Key Stores view

The Key Stores view displays in a table the key stores that are in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each key store.

Column	Description
Name	Identifies the name of the key store.
Description	Provides a description of the key store.
Is Hidden	Indicates whether the key store and its entries are visible for selection in the user interface. Options are **Yes** and **No**.
All Application Access	Indicates whether all applications have access to the values in key store entries. Options are **Yes** and **No**.

Understanding the key store detail panel

When you select a key store in the Key Stores view, the key store detail panel appears.

The detail panel displays the same information that is displayed in the Key Stores view for the selected key store, as well as the list of applications to which the key store is assigned.

Understanding the key store usage tab

The detail panel includes a usage tab that shows the usage data for the selected key store. The usage data is categorized into the following groups:

- **Scan Settings** – a list of scan settings that use values from the key store
- **Base Scan Settings** – a list of base scan settings that use values from the key store
- **Scans** – a list of scans that use values from the key store

A group is displayed only if there is usage associated with the group.

The following table describes the data that is provided in each group.

Data	Description
Name	Identifies the name of the settings file or scan.
Settings ID or **Scan ID**	Indicates the integer ID in the ScanCentral DAST database for the settings file or scan.
Property	Identifies the settings property, such as `ScanSettings.StartUrls` or `ScanSettings.ProxyPACUrl`, that uses the key store entry.
Entry Name	Identifies the name of the key store entry.

Creating a key store

When you create a key store, you can assign it to individual applications or to all applications. These assignments determine which applications can use the key store placeholders in their scan settings.

To create a key store:

1. On the **Key Stores** view, select **+ KEY STORE**.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. Configure the GENERAL settings as follows:
   a. To make the key store visible so that it can be selected when configuring scan settings, slide the toggle to **Key Store Visible**.

      Tip: You cannot delete a key store after it has been created. However, you can hide it so that it is not visible to users when configuring scan settings. To hide the key store, slide the toggle to **Key Store Hidden**.

   b. In the **Key Store Name** box, type a name that will become part of the placeholder text used in settings.

      Important! This field is required and cannot be the same as any existing key store. After the key store is created, you cannot change the key store name.

   c. Optionally, in the **Key Store Description** box, type a useful description.
3. Click **NEXT**.

The Application Selection page appears.

4. Do one of the following:
   - To assign the key store to all existing and future applications, slide the toggle to **Grant all application access**.
   - To assign the key store to individual applications, slide the toggle to **Assign individual applications**, and then select individual application check boxes in the **APPLICATIONS** list.

     Note: Only selected applications will have access to the key store. The key store must have at least one assigned application.

5. Click **NEXT**.

   The Key Store Values page appears.

   Note: The key store must have at least one key store entry.

   Tip: To view updated key store entries that other administrators may be creating in the same key store, click **REFRESH** to update the list of key store entries.

6. To add a key store entry, select **+ KEY STORE ENTRY**.

   The KEY STORE ENTRY dialog box opens.

7. Continue as follows:
   a. To make the key store entry visible so that it can be selected when configuring scan settings, slide the toggle to **Key Store Entry Visible**.

      Tip: You cannot delete a key store entry. However, you can hide it so that it is not visible to users when configuring scan settings. To hide the key store entry, slide the toggle to **Key Store Entry Hidden**.

   b. In the **Key Store Entry Name** box, type a name that will become part of the placeholder text used in settings.

      Important! The name cannot contain underscores or spaces, exceed 255 characters, or match any existing key store entry names. After the entry is saved, you cannot change the key store entry name.

   c. Optionally, in the **Key Store Entry Description** box, type a useful description.
   d. From the **Type** list, select one of the following:
      - **Text** – for use in any field that accepts string input, except for the Policy ID field.
      - **URL** – for use in fields that accept URLs only.
      - **Password** – for use with data that should be treated as a password. The entry is masked and is not visible in the UI.

      Note: URL type entries are available only for settings fields that require a URL as input. Password type entries are available only for settings fields that require a password as input. Text type entries are not available for settings

fields that require a URL or password.

e. In the **Key Store Entry Value** box, type the value that will replace the placeholder text in the scan settings.

Note: The maximum length is 4,000 characters.

f. Click **OK**.

The new entry is added to the KEY STORE ENTRIES list.

Tip: To make the entry values in the list visible, click **REVEAL VALUES**. This option is not available for Password type key store entries.

You cannot sort on the **Entry Value** column because these values are encrypted.

Note: You cannot delete a key store entry that has been saved. However, you can remove one that has not yet been saved by clicking **remove** × for the entry. Only unsaved entries have the remove icon.

g. Optionally, to add another key store entry, select **+ KEY STORE ENTRY** and return to Step a.

8. Click **NEXT**.

The Review page appears.

9. Click **SAVE**.

Managing key stores

You can edit a key store, hide a key store, and view hidden key stores.

Editing a key store

To edit a key store:

1. In the **Key Stores** view, click **edit** for the key store you want to edit.

The KEY STORE CONFIGURATION wizard opens to the Getting Started page.

2. To make edits, follow the procedure listed in "Creating a key store" on page 449.

Hiding a key store

You cannot delete a key store, but you can hide it from view in the user interface. Placeholders in a hidden key store are not available for selection in the scan settings and base settings user interfaces.

Note: Although a hidden placeholder is not available for selection in the user interface, you can manually enter the placeholder in a relevant field. If the placeholder is formatted correctly, ScanCentral DAST will accept it without further validation. Ensure that manually entered placeholders are valid. Otherwise, the scan settings might not be valid. For more information, see "Key store placeholder format" on page 446.

To hide a key store:

1. In the **Key Stores** view, click **edit** for the key store you want to hide.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. To hide the key store so that it cannot be selected when configuring scan settings, slide the toggle to **Key Store Hidden**.
3. In the left navigation, select **Review**.
   The Review page appears.
4. Click **SAVE**.

Viewing hidden key stores

By default, hidden key stores are not visible in the Key Stores view. However, you can view them if needed.

To view hidden key stores:

- On the **Key Stores** view, select the **Show hidden** check box.
  All key stores become visible in the Key Stores view.

Managing key store entries

You cannot delete a key store entry that has been saved. However, you can edit or hide a key store entry.

Editing a key store entry

To edit a key store entry:

1. In the **Key Stores** view, click **edit** for the key store whose entries you want to edit.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. In the left navigation, select **Key Store Values**.
   The Key Store Values page appears.
3. Click **edit** for the entry you want to edit.
   The KEY STORE ENTRY dialog box opens.

Tip: To make the value visible, click **REVEAL VALUE**. This option is not available for Password type key store entries.

4. Edit the values as described in Step 7 of "Creating a key store" on page 449.

Hiding a key store entry

You cannot delete a key store entry, but you can hide it from view in the user interface.

To hide a key store entry:

1. In the **Key Stores** view, click **edit** for the key store whose entries you want to hide.
   The KEY STORE CONFIGURATION wizard opens to the Getting Started page.
2. In the left navigation, select **Key Store Values**.
   The Key Store Values page appears.
3. Click **edit** for the entry you want to hide.
   The KEY STORE ENTRY dialog box opens.
4. Slide the toggle to **Key Store Entry Hidden**.

Understanding artifacts repositories

Artifacts repositories provide a way to specify repositories where scan artifacts reside. When a scan is run that references an artifact in a repository, either a tagged version or the latest copy of the artifact is pulled and used to configure and run the scan.

Benefits of using artifacts repositories

When artifacts are stored in the ScanCentral DAST database and updated frequently, such as Postman collections, you must manually reconfigure scan settings after each update. Creating a reference to artifacts in a repository eliminates the need to manually update scan settings. The latest version of the artifacts are automatically pulled from the repository and used to run the scan each time the settings are used.

Supported artifacts

Any file that you can import into ScanCentral DAST to configure settings or start a scan can be placed in a repository and referenced. Such artifacts include client certificates, login macros, workflow macros, HAR files, Burp files, Postman collections, and so forth.

Supported repositories

Supported repositories are as follows:

- GitHub
- GitHub Enterprise
- GitLab
- JFrog Artifactory

Using a proxy with the repository

If a proxy is required for communication with the repository, the ScanCentral DAST API will use the proxy that is configured in ScanCentral DAST.

Artifacts in XML settings files

Artifacts from the repository will be included in Fortify DAST composite settings files that are downloaded from ScanCentral DAST.

Accessing the Artifacts Repositories view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with artifacts repositories directly in Application Security.

To access the Artifacts Repositories view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Artifacts Repositories**.
   The Artifacts Repositories view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to artifacts repositories may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Understanding the Artifacts Repositories view

The Artifacts Repositories view displays in a table the repositories that are in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each repository.

Column	Description
Repository Name	Identifies the name of the repository.
Description	Provides a description of the repository.
Repository Type	Indicates the type of repository. Possible values are: • **GitHub** • **GitHub Enterprise** • **GitLab** • **JFrog Artifactory**
Root Api Url	Indicates the URL for the location of the repository.
All Application Access	Indicates whether all applications have access to the artifacts in the repository. Options are **Yes** and **No**.
Repository Status	Indicates the current status of the repository, including the migration status during the deletion process. Possible statuses are: • **Active** – The repository is currently active and usable in the UI. • **Migrate Artifacts Queued** – A user deleted the repository and chose to migrate artifacts that are being used from the selected repository to the ScanCentral DAST database. • **Migrating Artifacts** – Artifacts are currently migrating from the repository during the deletion process. • **Migrating Artifacts Failed** – Artifact migration failed. You can retry a delete with migration or delete without migration. • **Canceling Migration** – A user canceled the migration and the migration process is currently being stopped. • **Migration Canceled** – A user canceled the migration, stopping the migration and deletion process. The artifacts that were migrated remain in the ScanCentral DAST database. The artifacts repository remains active and usable in the UI.

Understanding the artifacts repositories detail panel

When you select a repository in the Artifacts Repositories view, the artifacts repository detail panel appears.

The detail panel displays the same information that is displayed in the Artifacts Repositories view for the selected repository, as well as the list of applications to which the repository is assigned.

Understanding the artifacts repositories USAGE tab

The detail panel includes a USAGE tab that shows the usage data for the selected repository. The usage data is categorized into the following groups:

- **Scan Settings** – a list of scan settings that use artifacts from the repository
- **Base Scan Settings** – a list of base scan settings that use artifacts from the repository
- **Scans** – a list of scans that use artifacts from the repository

A group is displayed only if there is usage associated with the group.

The following table describes the data that is provided in each group.

Data	Description
Name	Identifies the name of the settings file or scan.
Settings ID or **Scan ID**	Indicates the integer ID in the ScanCentral DAST database for the settings file or scan.
Property	Identifies the settings property, such as `ScanSettings.LoginMacroBinaryField` or `ScanSettings.TruClientMacroParameters.MacroBinaryField`, that uses the artifact.
Artifact Path	Indicates the path to the artifact in the repository.

Understanding the artifacts repositories LOGS tab

ScanCentral DAST records Fortify DAST sensor logs that are displayed in the LOGS tab of the detail panel. The sensor logs are chronologically ordered lists of recorded events that may be of use in troubleshooting issues with artifacts repositories.

To update the entries, click **REFRESH**.

Creating an artifacts repository

When you create an artifacts repository, you can assign it to individual applications or to all applications. These assignments determine which applications can use artifacts from the repository.

Before you begin

You must generate an access token for your repository to configure access to the repository in ScanCentral DAST. The token must have read access at minimum. If additional requirements are needed, refer to your GitHub, GitHub Enterprise, GitLab, or JFrog Artifactory documentation.

Tip: Both classic and fine-grained personal access tokens from GitHub are supported. For fine-grained tokens, select Contents and Metadata permissions.

Additionally, when configuring a GitLab repository, you must copy the project ID from GitLab and paste it in the ARTIFACTS REPOSITORY CONFIGURATION wizard. For more information, refer to your GitLab documentation.

Creating an artifacts repository

To create an artifacts repository:

1. On the **Artifacts Repositories** view, select **+ ARTIFACTS REPOSITORY**.
   The ARTIFACTS REPOSITORY CONFIGURATION wizard opens to the Getting Started page.
2. Configure the GENERAL settings as follows:
   a. In the **Repository Name** box, type a name for the repository. For example, in `https://github.com/scdast/HelloWorld`, the repository name is "`HelloWorld`."
   b. Optionally, in the **Repository Description** box, type a useful description.
3. Click **NEXT**.
   The DETAILS page appears.
4. Continue as follows:
   a. From the **Repository Type** list, select the type of repository to configure. Options are:
      - **GitHub**
      - **GitHub Enterprise**

        Important! Be sure to select the correct GitHub type for your repository. ScanCentral DAST will validate connection to the root API URL regardless of the selected type. However, if the wrong type is selected, ScanCentral DAST will not be able to retrieve artifacts from the repository when configuring settings.

      - **GitLab**
      - **JFrog Artifactory**
   b. In the **Root API URL** box, type the URL for the location of the repository. For example, the root API URL for GitHub is `https://api.github.com/`.

c. In the **Access Token** box, enter the access token that you created for the repository.

5. Continue according to the following table.

For this repository type...	Then...
GitHub GitHub Enterprise	a. In the **Owner** box, type the name of the owner or organization for the repository. For example, in `https://github.com/scdast/HelloWorld`, the owner is "`scdast`." **Tip:** The Github UI and API use different terms, so owner and organization can refer to the same thing. b. In the **Branch** box, type the name of the repository branch that you want to access. The default branch in GitHub is usually "master" or "main" but might be different depending on your environment.
GitLab	a. In the **Project ID** box, paste the project ID that you copied from GitLab. b. In the **Branch** box, type the name of the repository branch that you want to access.

Important! If you create a connection to a specific branch and then create a new branch from your original branch, you must edit the previous connection to use the new branch or create a new repository using the new branch.

6. Optionally, click **VALIDATE** to validate the connection using the configuration settings.

   A dialog displays whether the connection to the repository succeeded or failed.

7. Click **NEXT**.

   The Application Selection page appears.

8. Do one of the following:
   - To assign the repository to all existing and future applications, slide the toggle to **Grant all application access**.
   - To assign the repository to individual applications, slide the toggle to **Assign individual applications**, and then select individual application check boxes in the **APPLICATIONS** list.

Note: Only selected applications will have access to the repository. The repository must have at least one assigned application.

9. Click **NEXT**.
   The Review page appears.
10. Click **SAVE**.

Managing artifacts repositories

You can edit an existing repository, validate the repository connection, and delete the repository.

Editing a repository

To edit a repository:

1. In the **Artifacts Repositories** view, click **edit** for the repository you want to edit.
   The ARTIFACTS REPOSITORY CONFIGURATION wizard opens to the Getting Started page.
2. To make edits, follow the procedure listed in "Creating an artifacts repository" on page 456.

Validating a repository connection

You can validate the connection to an existing repository from the artifacts repository details panel.

To validate a repository connection:

1. In the **Artifacts Repositories** view, select the repository whose connection you want to validate.
   The artifacts repository details panel opens.
2. In the details panel, click **VALIDATE**.
   A dialog displays whether the connection to the repository succeeded or failed.

Deleting a repository

If you delete a repository, ScanCentral DAST prompts you to migrate the artifacts that are referenced in scan settings and base settings from the repository to the ScanCentral DAST database. If you select this option, ScanCentral DAST will migrate only the referenced artifacts from the repository. During migration, ScanCentral DAST validates the files. Depending on your environment and network, it might take some time to migrate.

Caution! When you delete a repository and do not migrate the artifacts, all scan settings and base settings that reference the repository become invalid. Additionally, you cannot restore a deleted repository. You must recreate the artifact repository.

To delete a repository:

1. In the **Artifacts Repositories** view, select the repository to delete.
   The artifacts repository details panel opens.
2. In the details panel, click **DELETE**.
   The DELETE REPOSITORY dialog box opens.
3. Optionally, to see which scan settings, base settings, and scans reference artifacts in the repository, click **See Usage**.
   The information displayed here is the same as in the USAGE tab on the repository details panel. For more information, see "Understanding the artifacts repositories USAGE tab" on page 456.
4. By default, the **Migrate artifacts** check box is selected. Do one of the following:
   - Leave the check box selected so that all artifacts specified in the usage list will be downloaded to the ScanCentral DAST database before the repository is deleted. With this option, all scan settings and base settings that reference the repository remain valid.
   - Clear the check box so that referenced artifacts will *not* be downloaded to the ScanCentral DAST database before the repository is deleted. With this option, all scan settings and base settings that reference the repository become invalid upon deletion.
5. Click **OK**.
   If **Migrate artifacts** is enabled, the migration process will start, followed by the deletion of the repository configuration. For more information, see "Migrating artifacts" below.

Migrating artifacts

During the artifacts migration process, a **Cancel Migration** button is displayed in the details panel. Clicking this button cancels the migration, but any artifacts that have been downloaded to the ScanCentral DAST database will remain there. The **Delete** button is not available while artifacts are being migrated. If the migration fails or is canceled, the **Delete** button will become available again. If the migration fails, you can retry migrating artifacts or deleting the repository.

Chapter 18: Working with scan compliance and health policies

Scan compliance and health policies identify which applications or application versions are not running successful scans. You can configure check definitions in the policies to send alerts to the scan compliance and health Overview page.

Facts about scan compliance and health policies

You should understand the following facts about scan compliance and health policies:

- A policy does not need to have any application versions assigned. This fact allows administrative users to create a policy, have others review the policy, and then decide which applications and versions should use the policy.
- You can set only one policy as the default policy for each ScanCentral DAST environment.
- The default policy is set at the policy level (in the General settings of the policy), not at the application level.
- If a policy is set as the default at the policy level (in the General settings of the policy), then any application or application version that has not explicitly been assigned to a different policy will use the default policy.
- If a policy is set as the default at the application level, then any application version that belongs to that application will use the policy if it is not explicitly assigned to another policy.
- Any application or application version that is explicitly assigned to another policy will continue to use the policy to which it is assigned.

  Important! An exception to this fact occurs when **SET POLICY AS DEFAULT** is enabled and **Reassign all applications versions** is selected. This combination of settings reassigns every application and application version to the new default policy.

Accessing the Scan Compliance and Health view

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with scan compliance

and health policies directly in Application Security.

To access the Scan Compliance and Health view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Scan Compliance and Health** .
   The Scan Compliance and Health view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. For more information, see "Permissions in Application Security" on page 45.

Understanding the Scan Compliance and Health view

The Scan Compliance and Health view displays in a table the scan health policies that are stored in the ScanCentral DAST database.

You can select the information you want to display, as well as customize other aspects of the table. For more information, see "Working with tables" on page 136.

The following table describes the columns of information provided for each scan health policy.

Column	Description
Id	Indicates the integer ID in the ScanCentral DAST database for the policy.
Name	Identifies the name of the compliance and health policy. This name appears in the scan health Overview page.
Description	Displays the description that was specified in the COMPLIANCE AND HEALTH POLICY wizard when the policy was created.
Enabled	Indicates whether the policy is enabled.
Is Default	Indicates whether the policy is the default compliance and health policy for all application versions. Only one policy can be set as the default at any given time.

Creating a compliance and health policy

When you create a ScanCentral DAST compliance and health policy, you may assign it to one or more applications or you may leave it unassigned to any application. You create the policy and assign applications to it in the COMPLIANCE AND HEALTH POLICY wizard.

To create a policy:

1. On the **Scan Compliance and Health** view, click **+ COMPLIANCE AND HEALTH POLICY**.

   The COMPLIANCE AND HEALTH POLICY wizard opens.
2. On the **General** page, do the following:
   a. By default, the policy is enabled upon creation. To disable the policy, slide the toggle to **Compliance and Health Policy Disabled**.

      Important! If you disable the policy on the **General** page, you will not be able to configure check definitions for the policy on the **Check Definitions** page.

   b. In the **Policy Name** box, type a name for the policy.

      Note: When naming the policy, be aware that you can save a policy with the same name as another policy. However, the Policy ID that is assigned by ScanCentral DAST for each policy is unique.

   c. Optionally, in the **Policy Description** box, type a useful description.
   d. To set the policy as the default policy for all application versions, slide the **SET POLICY AS DEFAULT** toggle to enabled. Optionally, to reassign all application versions to this policy, select the **Reassign all application versions** check box.
3. Click **NEXT**.

   The Check Definitions page appears.
4. On the **Check Definitions** page, review and optionally configure check definitions according to the following table. For more information, see "Configuring check definition alert priorities" on page 465.

   Tip: If you disabled the policy on the **General** page, you will not be able to configure check definitions. To enable check definition configuration, slide the toggle to **Policy enabled** at the top of the **Check Definitions** page.

Check Definition	Description / Configurable Alert Priorities
Scan has not completed or forced	The application has not completed a scan—nor has a scan been forcibly completed—within the past *<number*

Check Definition	Description / Configurable Alert Priorities
completed	*of>* days. The configurable check definition alert priorities represent days.
Scan Has Been Running Longer Than Expected	The application has initiated a scan that has been running continuously for more than *<number of>* minutes without completion or forced termination. The configurable check definition alert priorities represent days (d), hours (h), and minutes (m).
Scan has completed or force completed	The application has completed a scan—or the scan was forcibly terminated—in less than *<number of>* minutes. The configurable check definition alert priorities represent days (d), hours (h), and minutes (m)
Scan total requests	The scan contains fewer than *<number of>* requests. The configurable check definition alert priorities represent the number of requests sent by the Fortify DAST sensor.
Login Macro Failed or Not Executed	The application encountered a scan where the login macro either failed to execute successfully or was not triggered at all. There are no configurable check definition alert priorities.
Macro Playback	Macro(s) have executed *<number of>* times in the scan. The configurable check definition alert priorities represent how many times the Fortify DAST sensor encountered a logout condition and had to execute the login macro.
Scan Failed or Interrupted	The application encountered a scan that either failed to complete or was unexpectedly interrupted. There are no configurable check definition alert priorities.

5. Click **NEXT**.
   The Application Selection page appears.

Note: If you enabled the **SET POLICY AS DEFAULT** toggle on the General page, then you cannot apply the policy to specific applications on the Application Selection page.

6. Continue as follows:
   a. In the **APPLICATIONS** list, select an application to which you want the policy to apply.
   b. In the **VERSIONS** list, select the version(s) to which you want the policy to apply.
      The version(s) are added to the SELECTED ITEMS list.

      Tip: Click **Select All** to select all versions in the application. Click **Set as default** make the policy the default policy for all selected application versions.

   c. Do one of the following:
      - Repeat steps a and b to add application versions.
      - Click **NEXT**.
        The Review page appears.
7. Click **SAVE**.

Configuring check definition alert priorities

Scan health policies include predefined check definitions that are enabled by default. You can disable checks when creating or modifying a policy.

Some check definitions can only be set to either "enabled" or "disabled." Other check definitions, however, offer a configurable control to set threshold values for three alert priorities: Information, Important, and Urgent. When creating or editing a policy, you can configure these priorities to suite your needs. For example, if you know your scan typically takes over 24 hours to complete and it finishes in under 12 hours, then that may be an urgent alert for your environment.

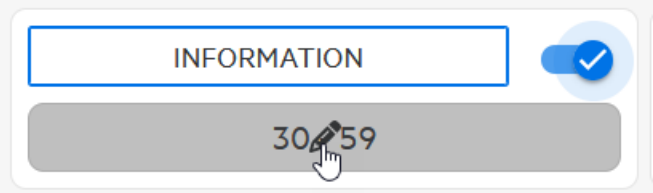
This topic describes how to use features in the COMPLIANCE AND HEALTH POLICY wizard to configure check definition alert priorities. For more information about the wizard, see "Creating a compliance and health policy" on page 463.

Using input boxes

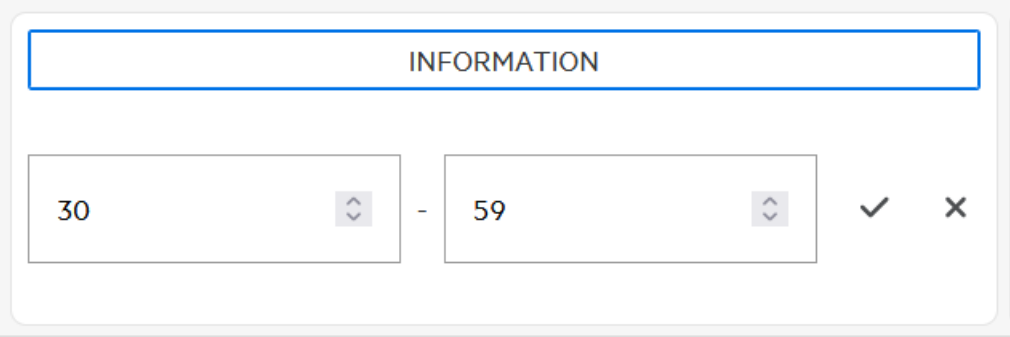
You can configure specific ranges for check definition alert priorities using input boxes in the COMPLIANCE AND HEALTH POLICY wizard.

To configure the alert priorities using input boxes:

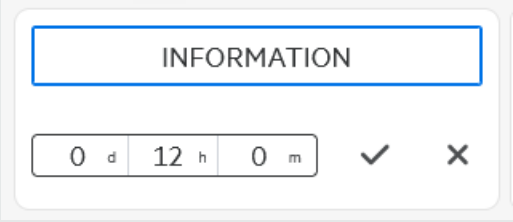
1. Click the number range below the alert priority.



2. Do one of the following:
   - Click the up or down arrows in the beginning and ending range boxes until the desired number appears in each box.
   - Type the desired number in the beginning and ending range boxes.



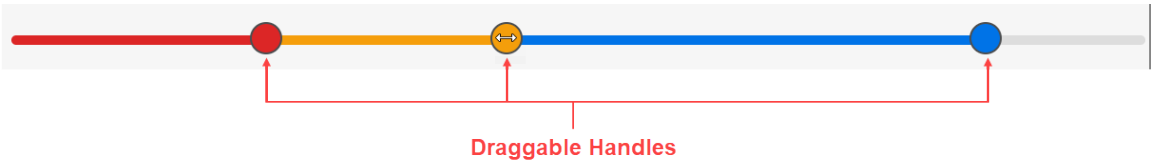
Note: Check definitions that use time ranges for alert priorities provide input boxes for days (d), hours(h), and minutes (m). Type the desired number in each input box.



3. To save your changes, click **confirm** ✓.

Using sliders

Alternatively, you can use the multi-point range sliders in the COMPLIANCE AND HEALTH POLICY wizard to select a range of values along a continuum, defined by three draggable handles.



To configure the alert priorities using sliders:

- Click a handle and drag it left or right to adjust the range values.
  The affected alert priority range values change as you drag the handle.

Managing compliance and health policies

You can edit and delete compliance and health policies, and refresh the Scan Compliance and Health view.

Facts about deleting policies

You can delete a policy in the Scan Compliance and Health view. Before doing so, however, consider the following facts about default policy settings when deleting a policy that is directly assigned to an application version:

- If the application has a default policy, then the fallback will be to the default policy for the application.
- If there is a global default policy, then the fallback will be to the global default policy.
- If the application has a default policy and there is also a global default policy, then the fallback will be to the default policy for the application.
- If there is no application default policy or global default policy, then there will be no fallback policy.

Editing a policy

To edit a policy:

1. In the **Scan Compliance and Health** view, select the policy to edit.
2. Click **EDIT**.
   The COMPLIANCE AND HEALTH POLICY wizard opens.
3. Edit the policy settings as needed.

   Note: For more information about the COMPLIANCE AND HEALTH POLICY wizard, see "Creating a compliance and health policy" on page 463.
4. On the **Review** page, click **SAVE**.
   The changes are saved in the ScanCentral DAST database.

Deleting a policy

To delete a policy:

- Select the check box for the policy in the **Scan Compliance and Health** view, and then click **DELETE** at the bottom of the table.

Refreshing the Scan Compliance and Health view

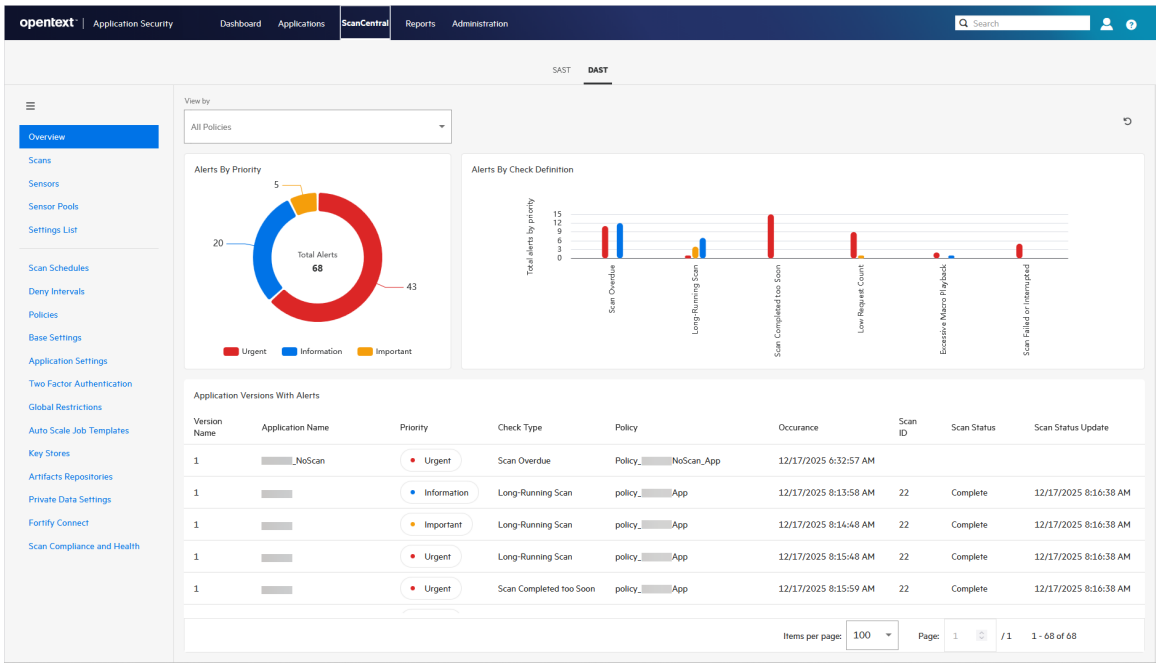
Changes to policies may take some time to process and appear on the Scan Compliance and Health view, depending on the complexity of changes. To see if your changes have been processed, you can manually refresh the view.

To refresh the Scan Compliance and Health view:

- Click **REFRESH**.

Understanding the scan health Overview

The landing page for ScanCentral DAST in Application Security is the scan health Overview.



The Overview provides a comprehensive snapshot of the current status of all configured and enabled scan health policy check definitions. This centralized interface enables you to quickly assess your ScanCentral DAST system health, identify threshold breaches, and monitor key metrics at a glance.

For information about filtering alerts, alerts by priority, and alerts by check definition, see Working with alerts on the scan health Overview

Application Versions With Alerts

The **Application Versions With Alerts** area provides a tabular view of the alerts for all application versions. You can sort the data by any column in the table. For more

information, see "Sorting data in columns" on page 145.

The following table describes the columns of information that are available for each scan.

Column	Description
Version Name	Identifies the application version for which the alert occurred.
Application Name	Identifies the application for which the alert occurred.
Priority	Indicates the color-coded alert priority that was configured for the check definition in the compliance and health policy. Possible priorities are: • Urgent • Important • Information **Note:** The **Login Macro Failed or Not Executed** and **Scan Failed or Interrupted** check definitions have no configurable alert priorities. These alerts default to the Urgent priority.
Check Type	Identifies the check definition name.
Policy	Identifies the name of the compliance and health policy in which the check is configured and to which the application version is assigned.
Occurrence Timestamp	Indicates the date and time when the alert occurred.
Scan ID	Indicates the integer ID in the ScanCentral DAST database for the scan.
Scan Status	Indicates the current status of the scan. For more information on scan statuses, see "Understanding the Scans view" on page 285.
Scan Status Update	Indicates the date and time when the scan status changed.

Note: The **Application Versions With Alerts** table does not currently include the table preferences panel.

Facts about alerts on scan health Overview and Scans view

Be aware of the following facts about the alerts you may see on the scan health Overview and on the Scans view:

- Only the last completed and currently running scans for an application version will have active compliance and health alerts in both the Scans view and the scan health Overview.
- When creating, editing, or deleting a policy, the alerts for the last completed scan and currently running scan for the assigned application versions will be recalculated by the ScanCentral DAST Global Service. Recalculation may take some time to process, depending on data and load.

Working with alerts on the scan health Overview

Delete this text and replace it with your own content.

Filtering by policy

By default, the Overview displays statistics for all enabled policies. You can filter the content for one or more specific policies.

To filter by one or more policies:

1. In the **View by** listbox, click the drop-down arrow.
   A list of enabled compliance and health policies appears.
2. Select the check box for each policy to include in the Overview.
   The content changes with each policy selected.
3. Click anywhere outside the list to close the list.

To view statistics for all policies again:

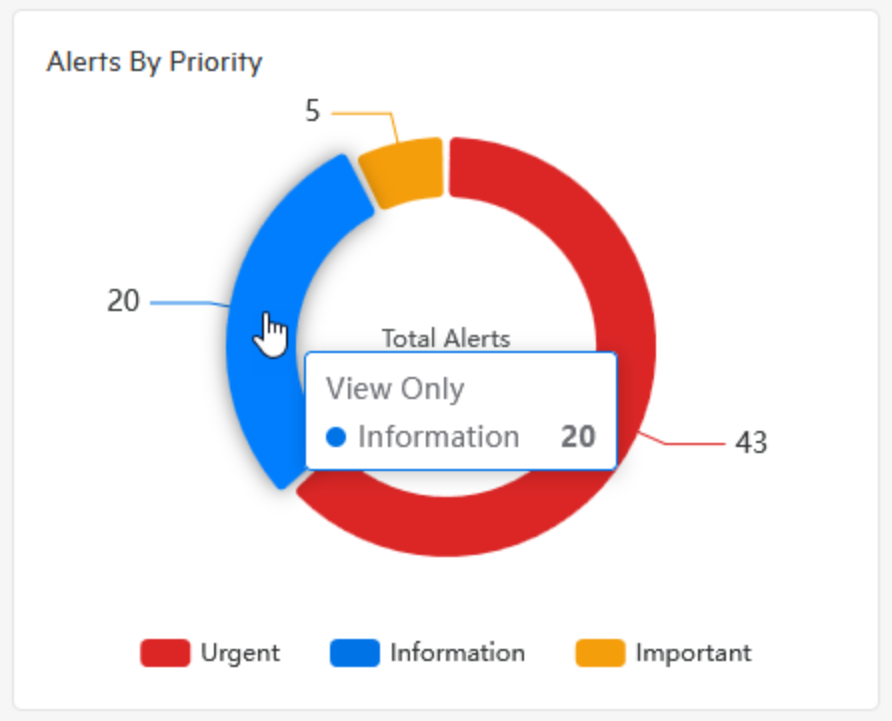
1. In the **View by** listbox, click the drop-down arrow.
   A list of enabled compliance and health policies appears.
2. Clear the check boxes for the selected policies.
3. Click anywhere outside the list to close the list.

Alerts By Priority

The **Alerts By Priority** area includes a doughnut chart that identifies the number of alerts by priority. Each segment in the chart corresponds to a priority.

To filter the content for a specific priority:

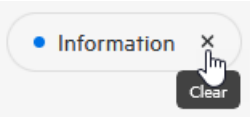
- Click the priority segment in the chart.



The Overview shows only content for the selected priority and a filter badge appears to the right of the **View by** listbox.

To remove the priority filter:

- Click **Clear** ✕ on the filter badge.

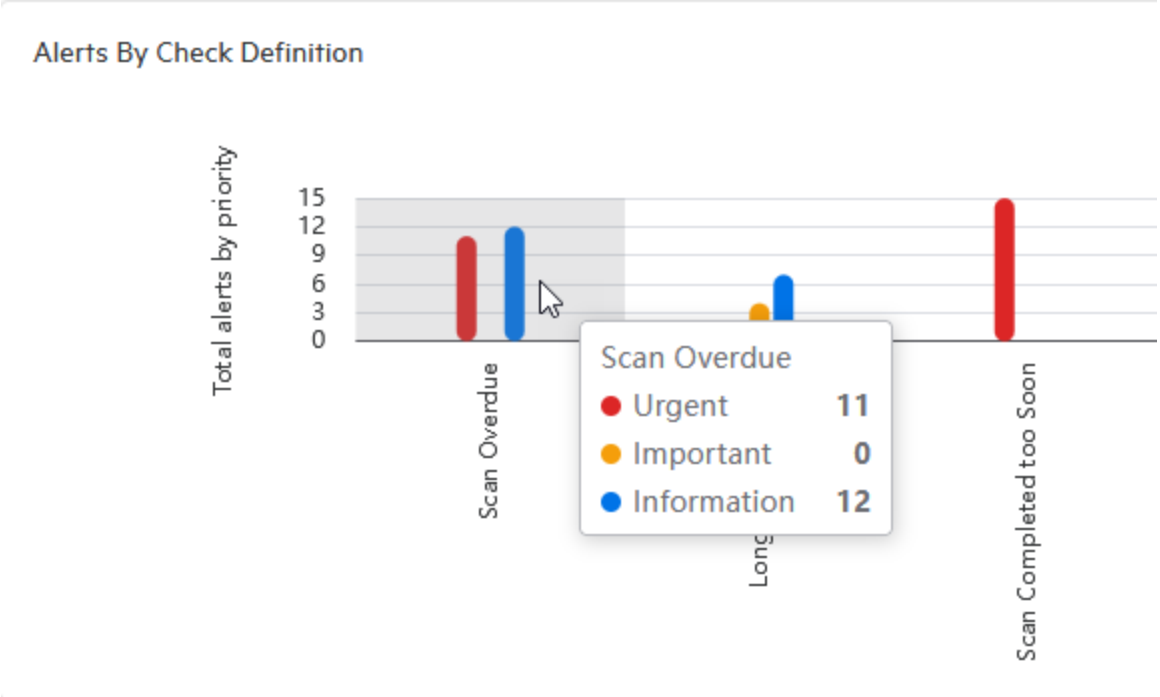


Alerts By Check Definition

The **Alerts By Check Definition** area includes a bar chart that shows alert counts per check type across different priorities. For more information about check definitions, see "Corrective actions for scan health alerts" on page 473.

To view the number of each priority for a specific check definition:

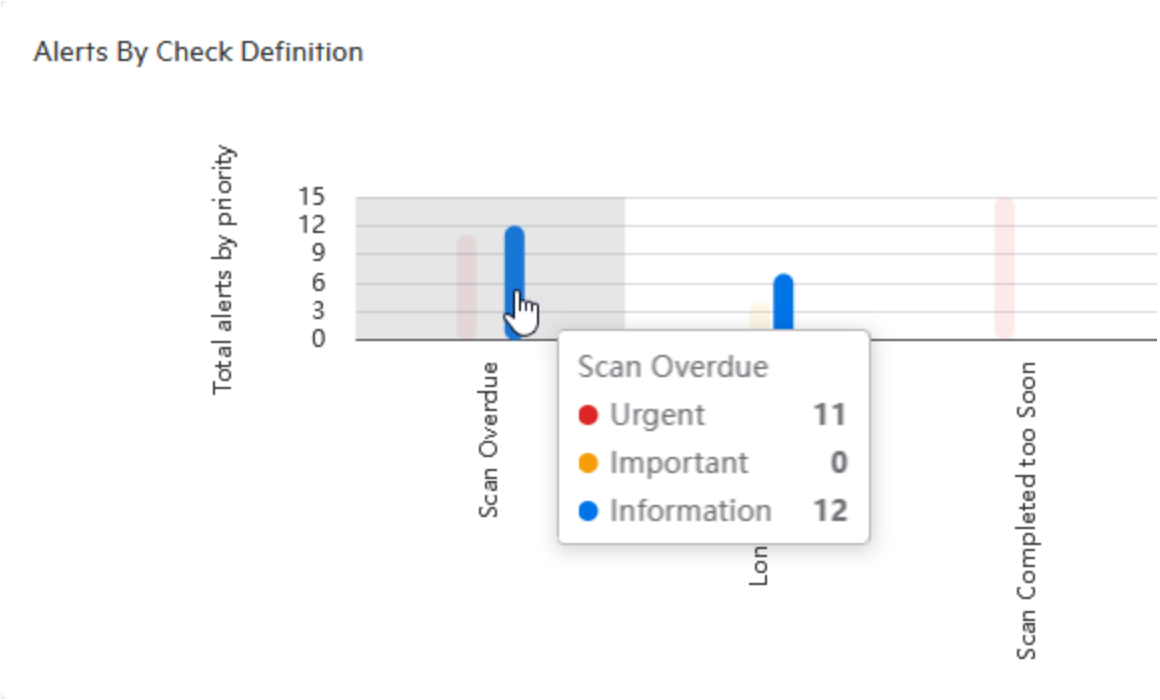
- Hover over the check definition in the chart.
  A pop up displays the number of each priority for the check.



You can also filter the alerts for a specific priority from within the bar chart.

To filter the content for a specific priority:

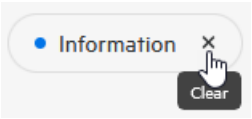
- Click the priority bar in the chart.



The Overview shows only content for the selected priority and a filter badge appears to the right of the **View by** listbox.

To remove the priority filter:

- Click **Clear** × on the filter badge.



Corrective actions for scan health alerts

The following table describes the scan health alerts that may appear on the scan health Overview and provides corrective action for each.

Alert / Description	Corrective Action(s)
Scan Overdue The application version has not completed a scan nor forcibly completed a scan within the past *<number of>* days.	Start a new scan for the application version.

Alert / Description	Corrective Action(s)
Long-Running Scan The application version has initiated a scan that has been running continuously for more than *<number of>* minutes without completion or forced completion. This does not include scans that are paused due to higher priority, user paused, or deny interval.	Force complete the affected scan.
Scan Completed too Soon The application version has completed a scan or forcibly completed in less than *<number of>* minutes.	1. Download the log files. 2. Start a new scan for the application version.
Low Request Count The scan contains fewer than *<number of>* requests.	1. Download the log files. 2. Start a new scan for the application version.
Login Macro Failed The login macro either failed to login successfully or was not executed during the scan.	1. Modify the macro. 2. Start a new scan for the application version.
Excessive Macro Playback Macro(s) have played *<number of>* times during the scan. This indicates excessive logins which is triggered only by login macros.	1. Download the log files. 2. Start a new scan for the application version.
Scan Failed or Interrupted The scan either failed to complete or was unexpectedly interrupted.	1. Download the log files. 2. Start a new scan for the application version.

Chapter 19: Working with Aviator auto-generated macros

You can configure ScanCentral DAST to integrate with OpenText™ Application Security Aviator to leverage Large Language Model (LLM) technology to automatically generate a login macro. If you have purchased entitlements to Application Security Aviator, and have configured access to Application Security Aviator using the SC DAST Aviator management UI, then you can select the Aviator Autogen Macro option, enter credentials, and have the macro automatically generated. You may also provide a time-based one-time password (TOTP) or upload a QR code image.

When macros are generated

Macro generation occurs only when new scan settings are applied or when existing scan settings are modified and the option to re-generate the macro is explicitly selected. A macro is not created when running a scan using existing scan settings with an auto-generated macro. However, in this scenario, updated credentials are used.

Macro generation process

The following table describes the components and activities involved in the automated macro generation process.

Stage	Component	Activity
1.	ScanCentral DAST	1. Logs into Application Security Aviator with stored configuration (URL, tenant, and private key). 2. Pulls the user email address.
2.	Application Security Aviator	1. Validates the tenant. 2. Creates a JWT with supplied email. 3. Sends JWT back to ScanCentral DAST.
3.	ScanCentral DAST	Passes the JWT, URL, username, password, and TOTP (optional) to ScanCentral DAST API.
4.	ScanCentral DAST API	Requests Application Security Aviator create

Stage	Component	Activity
		login macro using the JWT.
5.	Application Security Aviator	Validates the JWT and entitlements.
6.	ScanCentral DAST Utility Service	Creates the login macro using the JWT, URL, username, password, and TOTP (optional).

Enabling Aviator

After you configure your ScanCentral DAST environment and enable ScanCentral DAST in the Administration view in Application Security, you can work with Aviator directly in Application Security.

Accessing the Aviator view

To access the Aviator view in Application Security:

1. Select **SCANCENTRAL** > **DAST**.
   The Overview page appears.
2. In the left panel, select **Aviator**.
   The Aviator view appears.

User role determines capabilities

Your user role and permissions in Application Security determine which tasks you can perform on ScanCentral DAST scans, sensors, sensor pools, settings, scan schedules, and other features. Access to Aviator is restricted to users with the Manage DAST Aviator permission. Access to Aviator may also be restricted. For more information, see "Permissions in Application Security" on page 45.

Aviator configuration

The Aviator service is disabled by default.

Important! Upon first navigation to the Aviator view, an Aviator Service Disclaimer message is displayed. You must accept the terms of the disclaimer to continue. Select the **I acknowledge and agree to the terms above** check box and click **ACKNOWLEDGE**.

The Aviator Configuration Settings dialog box opens.

To enable and configure the service:

1. In the Aviator Configuration Settings dialog box, slide the **Aviator Service Disabled** toggle to **Aviator Service Enabled**.
2. In the **Aviator URL** box, enter the URL for the Aviator service provided by the Aviator team.

   Note: This entry must be in a valid URL format.
3. In the **Tenant Name** box, enter the tenant name provided by the Aviator team.
4. In the **Private Key** area, upload or drag and drop the certificate (`.pem` format).
5. Click **Save**.

   A summary of the Aviator configuration settings appears.

Understanding the Aviator view

The Aviator view has three areas: Aviator Configuration Settings, Credits Summary, and Aviator Entitlements. After Aviator has generated login macros, the Aviator Entitlements table displays in a table all Aviator macro generation jobs.

Aviator Configuration Settings

This area displays the Aviator settings. During initial setup of Aviator, complete the fields and add a Private key. For more on initial setup, see "Enabling Aviator" on the previous page

Setting	Description
Aviator Service switch	• **Aviator Service Disabled**: Aviator is not turned on. • **Aviator Service Enabled**: Aviator is turned on.
Aviator URL	The URL for the Aviator service provided by the Aviator team.
Tenant Name	The tenant name provided by the Aviator team
Private Key	The private key. After a key has been provided, the **REMOVE** button is displayed.

Credits Summary

This area displays your current Aviator credits usage as a percentage graph, with summary details.

Item	Description
Usage graph	A bar graph showing the percentage of Aviator credits that have been used n the current period. The expiration date of the credits is also indicated on the bar graph.
Total	The number Aviator credits purchased across all active Aviator job entitlements.
Consumed	The number Aviator credits consumed from successful jobs across all entitlements.
Reserved	The number of Aviator credits currently reserved for in-progress jobs.
Remaining	The number of Aviator credits available for new Aviator jobs.
Adjustments	The number of Aviator credit adjustments across all entitlements.

Aviator Entitlements

The following table describes the columns in the Aviator Entitlements list:

Column	Description
id	The Aviator entitlement identification number.
Start date	The date the entitlement started.
End date	The date the entitlement ends.
Created on	The creation date of the entitlement.
Number of units	The sum of credits consumed and credits remaining.
Credits consumed	The number of credits used by the entitlement.
Credits reserved	The number of credits reserved for use by the entitlement.
Credit adjustments	The number of credit adjustments for the entitlement.
Credits remaining	The number of credits remaining for the entitlement.
Contract id	An identifier for the entitlement contract.
Is valid	True or false, whether the entitlement is currently valid.

Managing Aviator jobs

You can retry macro generation, view macro generation, or cancel macro generation, depending on the current state of the macro generation job.

Tip: You can manage pending Aviator jobs from the Aviator view, Scans view, Settings List view, or Base Settings view. Selecting an item that has a pending Aviator job in any of these views opens the detail panel where Aviator-specific actions are available.

Retrying generation

If the macro generation job failed, you can retry the generation.

To retry generation from the Aviator view table:

- Click **retry** for the job you want to retry generation.

To retry generation from the detail panel:

- Click **RETRY MACRO GENERATION**.

Viewing generation

You can view macro generation or you may continue to use ScanCentral DAST while the macro is generating. Viewing macro generation is optional, but it may be useful in debugging issues.

To view generation from any view that includes the **Aviator Macro Autogen** icon ( ):

1. Select the item in the view table.
   The detail panel opens.
2. Click **VIEW PROGRESS**.

For more information, see "Understanding Aviator macro generation progress views" on page 481.

Canceling generation

To cancel the current Aviator macro auto-generation job from any view that includes the **Aviator Macro Autogen** icon ( ):

1. Select the item in the view table.
   The detail panel opens.
2. Click **CANCEL MACRO GENERATION**.

Downloading auto-generated macros

When an Aviator job has completed, a download icon appears for the job in the Aviator view table. At that point, you can download the auto-generated macro from the Aviator view. After the macro has been selected for use in scan settings, you can download the macro from the Settings List view. After the macro has been used in a scan, you can download the macro from the Scans list view.

To download the macro from the...	Do this...
Aviator view table	Click **Download Login Macro**. The macro is downloaded.
Settings List view	Click **Download**. A settings ZIP file, including the login macro, is downloaded.
Scans view	Click **Download**. A settings ZIP file, including the login macro, is downloaded.

Understanding Aviator Jobs

The **Aviator Jobs** list is in a new location as of ScanCentral DAST 26.4.

To access the Aviator jobs list:

1. Select **SCANCENTRAL** > **DAST**.
   The **Overview** page appears.
2. In the menu, select **Aviator Jobs**.
   The **Aviator jobs** list opens.

The following table describes the columns of information that are available for each job.

Column	Description
ID	Indicates the unique identifier assigned to the Aviator job. This corresponds to the SC DAST ID.
Start URL	Indicates the URL used to begin macro generation. Generally,

Column	Description
	this is the application under test.
Created	Indicates the time the job was initiated.
Job Status	Indicates the current status of the Aviator job. Possible statuses are: • New • Running • Completed • Failed • Pending Cancellation • Canceling • Canceled • Pending Retry
Status Update	Indicates the time of the most recent status change.
Source ID	Indicates the identifier of the originating source.
Source Type	Identifies the origin of the Aviator job. Possible origins are: • Application Version Scan Settings • Base Scan Settings • Scan
Source Name	Identifies the name of the entity that initiated the Aviator job.
Priority	Indicates the priority level assigned to the originating source.
Download login macro	Click to download the login macro for the job (if available).

Understanding Aviator macro generation progress views

Aviator macro generation progress consists of five views:

- Startup
- Intermediate

- Full
- Compact
- Bubble

Each view provides different levels of detail and available user actions during the macro generation process.

Startup view

The startup view is a simple status view that is displayed when macro generation begins.

From the startup view, you can cancel the macro generation or close the view.

Intermediate view

The intermediate view shows the current state of the macro generation process. This view includes screenshots sent from the Aviator service of the macro steps as they are recorded in the TruClient sidebar window and the target site in the TruClient browser window. The bottom portion displays the steps taken to generate the macro.

From the intermediate view, you can cancel the macro generation or close the view.

When you hover over the intermediate view, icons enable the following actions:

- Click **Minimize** – to display the compact view.
- Click **Full history** to display the full view.
- Click **View sidebar** to show or hide the sidebar image.

Full view

The full view shows an expanded version of the intermediate view with additional historical context. The History panel lists all recorded steps in the generation process with the most recent step appearing at the top. Selecting a step in the History panel displays its details in the bottom portion of the view.

From the full view, you can cancel the macro generation or close the view.

When you hover over the full view, icons enable the following actions:

- Click **Minimize** – to display the compact view.
- Click **Intermediate view** to display the intermediate view.
- Click **View sidebar** to show or hide the sidebar image.

Compact view

The compact view is a smaller, movable visualization displaying simplified progress updates. The view displays a thumbnail screenshot of the application and current status messages with live updates. You can click and drag this view to any location on the screen. If you navigate to another view in ScanCentral DAST, however, the compact view closes.

On the compact view, you can do the following:

- Click **Compact view** to display the bubble view.
- Click **Intermediate view** to display the intermediate view.
- Click **Full history** to display the full view.
- Click **Trash** to cancel macro generation.
- Click **Close** to close the visualization.

Bubble view

The bubble view is a single bubble showing the thumbnail screenshot of the application. It is the smallest visualization footprint. Like the compact view, you can click and drag the bubble view to any location on the screen.

You can click the bubble to open the compact view.

Appendix A: Troubleshooting ScanCentral DAST

If you encounter issues when setting up your ScanCentral DAST environment or with using it after a successful set up, the following pages might help determine possible causes and solutions.

Locating log files

This topic provides information about log files generated by the various ScanCentral DAST components, including where to find logs for each component and how to extract log files if necessary.

Event log files in the UI

You can view event log files for scans, settings, scan schedules, and artifacts repositories in their respective detail panels. For more information, see the following:

- "Understanding the scan detail panel" on page 290
- "Understanding the scan settings detail panel" on page 350
- "Understanding the schedule detail panel" on page 357
- "Understanding the Artifacts Repositories view" on page 454

Log file names

The log file name is in the format of `YYYY-MM-DD.log`, such as `2025-05-04.log`. There is one log file per day. If you run the Configuration Tool CLI more than once during a single day, the file is appended with new entries for each successive run.

ScanCentral DAST keeps a maximum of seven log files per service. A new log file is created daily or when a log file reaches 100 MB. The 100 MB limit prevents log files from becoming too large.

Locating log files inside the Docker Windows containers

The following table describes where to find log files within the Microsoft Windows® containers.

Container	Location
Global Service	`C:\app\logs`
ScanCentral DAST API	`C:\app\logs`
Sensor	Scan Logs and ScanData using SQLExpress `C:\ProgramData\HP\HP WebInspect\Schedule\logs\` `C:\ProgramData\HP\HP WebInspect\Schedule\ScanData\`
ScanCentral DAST Scanner Worker Service	`C:\Program Files\Fortify\DAST-ScannerService\logs`
Utility Worker Service	`C:\Program Files\Fortify\DAST-UtilityService\logs`
WIRCServer (OpenText DAST (Fortify WebInspect) API)	`%SystemRoot%\System32\Winevt\Logs\WebInspect API.evtx`

Locating log files inside the Docker Linux containers

The following table describes where to find log files within the Linux® containers.

Container	Location
Global Service	`/app/logs`
ScanCentral DAST API	`/app/logs`
Sensor	`/etc/wi/.widata/user/Logs` `/etc/wi/.widata/shared/logs`
ScanCentral DAST Scanner Worker Service	`/etc/wi/dast/logs`
Utility Worker Service	`/etc/wi/dast/logs`
WIRCServer (OpenText DAST (Fortify WebInspect)	`/etc/wi/.widata/user/Logs/WIRCServer` **Tip:** To enable DEBUG mode, edit the following files:

Container	Location
API)	• `/etc/wi/.widata/user/Logs/WIRCServer/WIRCServer_LogConfig.xml` • `/etc/wi/wircargs.txt`

Exporting log files

You can export log files from Docker containers using the Docker `logs` command using the following syntax:

```
docker logs <name of container> > <name_of_container>-log.txt
```

Examples:

```
docker logs 23g > scdast-api-log.txt
docker logs 7b6 > scdast-gs-log.txt
docker logs p9t > scdast-util-log.txt
```

Troubleshooting the Configuration Tool CLI

If the ScanCentral DAST Configuration Tool CLI fails to create and seed the database or fails at any other point, review the tool log file for errors.

CLI return codes

When the Configuration Tool CLI finishes, it provides the return codes described in the following table.

Return Code	Description
0	The command completed normally.
-1 or another negative number	An error occurred. Check the log file for specific error messages.

Troubleshooting tips

The following table describes possible causes and solutions related to the Configuration Tool CLI.

Error or Symptom	Possible Cause	Possible Solution
You configured a proxy in the Configuration Tool CLI, but do not want to access Application Security through the proxy. Now the Configuration Tool CLI cannot validate a connection to Application Security using the host name, machine name, or container name.	The Application Security host name, machine name, or container name is not in the `proxyBypassList` parameter.	Do the following: 1. Add the Application Security host name, machine name, or container name to the `proxyBypassList` parameter in the JSON or YML settings file. For more information, see "Environment settings" on page 80. 2. If your OS has an `HTTP_PROXY` or `HTTPS_PROXY` environment variable or both, then add the Application Security host name, machine name, or container name in a comma-separated list to the `NO_PROXY` variable. For example, if the Application Security URL is `http://MySSCMachine:8080/ssc`, then the comma-separated list in the `NO_PROXY` variable would be as follows: `localhost,MySSCMachine` If the previous steps do not correct the issue, then use the Application Security IP address instead of the host name, machine name, or container name as follows: • In the `proxyBypassList` parameter in the JSON or YML settings file • In the `sscRootUrl` in the JSON or YML settings file
You configured a proxy in the Configuration Tool CLI, but do not want to access the LIM	A known issue prevents using the host name, machine name, or container name in the `proxyBypassList`	When configuring ScanCentral DAST settings, do one of the following: • Use the LIM IP address in the `proxyBypassList` parameter in the

Error or Symptom	Possible Cause	Possible Solution
through the proxy. Now the Configuration Tool CLI cannot validate a connection to the LIM using the host name, machine name, or container name.	parameter.	JSON or YML settings file. • Set the `useProxy` parameter to `false` in the JSON or YML settings file, and configure `HTTP_PROXY` and `NO_PROXY` environment variables instead. For more information, see "Environment settings" on page 80.

Troubleshooting upgrade issues

If you perform an incomplete upgrade, you may encounter compatibility issues when attempting to use ScanCentral DAST. The following table describes possible causes and solutions related to upgrade issues.

Important! When upgrading your ScanCentral DAST environment, follow these requirements:

- Use the ScanCentral DAST Configuration Tool CLI that is packaged with the version of ScanCentral DAST software that you downloaded. Do *not* use a previous version of the tool.
- Upgrade your Application Security to the current compatible version. For version compatibility, see "Software integrations for ScanCentral DAST" in the *OpenText™ Application Security Software System Requirements*.
- Upgrade all ScanCentral DAST components, including the database, API container, Global Service container, Utility Service container, and the Fortify DAST on Docker image or the classic Fortify DAST installation with the ScanCentral DAST sensor service.

Error or Symptom	Possible Cause	Possible Solution
The following error appears in the Global Service log file: `IsVersionCompatible failed. ProcessName = DAST.GlobalWorkerService, Version = <DAST Version>, Type = DAST`	The Global Service attempted to start, but it is not compatible with the database. The ScanCentral DAST database was updated, but the Global Service container was not.	Use the `docker-compose.yml` file that you used when you upgraded your ScanCentral DAST database to upgrade all containers to the same version as your ScanCentral

Error or Symptom	Possible Cause	Possible Solution
		DAST database. For more information, see "Using the TLS compose file for core components" on page 123.
One of the following errors appears in the Utility Service log file: `IsVersionCompatible failed. ProcessName = DAST.UtilityWorkerService, Version = <DAST Version>, Type = DAST` `IsVersionCompatible failed. ProcessName = DAST.Web.API, Version = <DAST Version>, Type = DAST`	The Utility Service attempted to start, but it is not compatible with the database. The ScanCentral DAST database was updated, but the Utility Service was not.	
The following warning appears in the scanner service log file: `Scanner application version is not compatible and will have limited functionality. Version = <dastVersion>`	The scanner service started, but it is not compatible with the database. The ScanCentral DAST database was updated, but the scanner service was not. The service cannot start new scans or create scan settings.	Use the `docker-compose.yml` file to pull and run a compatible version of the scanner service (or sensor) container image. For more information, see "Using the TLS compose file for the sensor" on page 124.
The following error appears in the scanner service log file: `IsVersionCompatible failed. ProcessName = DAST.ScannerWorkerService, Version = <webInspectVersion>, Type = WebInspect`	The scanner service attempted to start, but it is not compatible with the database. The ScanCentral DAST database was updated, but the scanner service was not.	

Troubleshooting the ScanCentral DAST API

The following table describes possible causes and solutions when you cannot connect to the ScanCentral DAST API from Application Security.

Error or Symptom	Possible Cause	Possible Solution
In Application Security, you receive the following error on the ScanCentral DAST page: "UNABLE TO CONNECT TO SCANCENTRAL DAST API"	ScanCentral DAST might be using an untrusted or self-signed certificate.	To resolve this issue, do one of the following: • Ask your administrator to redeploy using a trusted certificate. • Navigate to the *<ScanCentral DAST API Swagger>*, export the certificate, and add it to your trusted certificate store.
	The ScanCentral DAST API URL may be configured improperly.	Do the following: 1. Navigate to **Administration** > **Configuration** > **ScanCentral DAST**. 2. Update the URL.
	The ScanCentral DAST API might be inaccessible from the current browser.	Verify the following: • The *<ScanCentral DAST API Swagger>* is not blocked by firewall rules. • The host is resolvable by way of DNS. • The ScanCentral DASTAPI service is running properly.
	Application Security's content security policy (CSP) might be too restrictive.	Ask your administrator to navigate to **Administration** > **Configuration** > **Security** to adjust the CSP policy.
	Cross-origin resource sharing (CORS) might have been misconfigured when ScanCentral DAST was deployed.	Ask your administrator to run the ScanCentral DAST Configuration Tool CLI to validate CORS is configured properly, and to

Error or Symptom	Possible Cause	Possible Solution
		adjust if necessary. For more information, see "ScanCentral DAST API settings" on page 76.

Troubleshooting Fortify Connect

The following table describes possible causes and solutions for issues involving the Fortify Connect client.

Error or Symptom	Possible Cause	Possible Solution
When trying to run the Fortify Connect client, you receive the error: `Bad remote forwarding specification 'port'`	You may be using an unsupported version of OpenSSH.	Verify that you are using a supported version of OpenSSH as specified in the system requirements. For more information, refer to the *OpenText™ Application Security Software System Requirements*.

Troubleshooting Kafka

ScanCentral DAST uses the Kafka messaging system that is configured in Application Security to sync audit history changes in Application Security with ScanCentral DAST. If problems arise with syncing audit history changes, use the following tips to troubleshoot Kafka settings and the Kafka messaging system:

- Ensure that the `SSCSettings` > `KafkaSettings` > `FindingAuditTopic` value that is configured for ScanCentral DAST matches the `stream.kafka.topics.customTagEvent` value in Application Security.
- Ensure that the `SSCSettings` > `KafkaSettings` > `Brokers` value that is configured for ScanCentral DAST matches the `stream.kafka.bootstrapServers` value in Application Security.
- Ensure that Kafka is running on a different machine than the ScanCentral DAST components and that Kafka is properly configured for external listening.
- Check the ScanCentral DAST Global Service logs for any errors.

Troubleshooting artifacts repositories

The following table describes possible causes and solutions for issues involving artifacts repositories.

Error or Symptom	Possible Cause	Possible Solution
When trying to access an artifacts repository in GitHub, you receive the error: `StatusCode = Forbidden, Content = {"message":"Resource not accessible by personal access token"...`	You are using a fine-grained personal access token with improper permissions.	Be sure to select Contents and Metadata permissions for the token.

Troubleshooting ScanCentral DAST scans

The following table describes possible causes and solutions when a ScanCentral DAST scan fails to start or fails to complete.

Error or Symptom	Possible Cause	Possible Solution
A scan is stuck in one of the following transitional states: • Queued • Resume Scan Queued • Resume Scan Queued Deny Interval	If the transitional state persists, it could be due to network errors or the scanner service being down. In such cases, the command to resume the scan will not have been sent or the scanner service will not have acknowledged receiving the resume command.	You may see network-related errors in the scanner service log files. Also check the ScanCentral DAST Global Service log files for any errors. For more information, see "Locating log files" on page 484.
		To determine if the scanner service is down: 1. Check the sensor status in the Sensors list. If the

Error or Symptom	Possible Cause	Possible Solution
		status is **Offline**, then correct this issue first. For more information, see "Understanding the Sensors view" on page 333. 2. Ensure that the OpenText DAST (Fortify WebInspect) API service is running. 3. Restart the sensor service.
A scheduled scan fails to start, and the following entry appears in the global service log file: `Failed to process scan schedule. The scanner assigned is no longer active. ScanScheduleId = <Id>, ScannerId = <ScannerId>`	The scheduled scan was configured with the **Use this sensor only** option, but the original sensor container that was assigned to the scheduled scan no longer exists due to upgrading the ScanCentral DAST components.	Edit the scheduled scan settings to use the new sensor container. For more information, see "Editing a schedule" on page 360.
A scan using a client certificate fails upon startup.	The certificate must be a valid CER, PEM, or PFX format.	Update the scan settings with a valid client certificate.
	The certificate might not be installed on the machine where the sensor service is running or the private key might not be exportable.	Do one of the following: • Install the certificate on the machine where the sensor service is running. • Verify that the certificate's private key is exportable.
	If the certificate is password protected, the password provided might be incorrect.	Update the scan settings with the correct certificate password.

Troubleshooting sensors and the sensor service

The following table describes possible causes and solutions when the sensor service fails to start or sensors do not appear in the ScanCentral DAST UI.

Error or Symptom	Possible Cause	Possible Solution
The sensor service fails to start, and the following entry appears in the scanner service log file: `The remote certificate is invalid because of errors in the certificate chain: UntrustedRoot`	Encrypted communication is used for the ScanCentral DAST API service, but the API SSL certificate is not installed in the Trusted Store on the ScanCentral DAST sensor service machine.	1. Copy the API SSL certificate from the Configuration Tool artifacts. 2. Add the certificate to the Trusted Store on the machine where the ScanCentral DAST sensor service will run.
Sensors are not appearing in the ScanCentral DAST UI.	The ScanCentral DAST Global Service may not be running.	1. Verify that there are no errors in the scanner service log files. For more information, see "Locating log files" on page 484. 2. Ensure that the ScanCentral DAST Global Service container is running and communicating with the ScanCentral DAST API container. For more information, see "ScanCentral DAST Global Service" on page 42.

You can check to see whether the sensor service is running, and then stop and/or restart the service if needed, as described in the following paragraphs.

Tip: If you need to restart both the Fortify DAST API and the sensor service, restarting the container restarts both.

Checking the sensor service status in a classic Fortify WebInspect installation

To check the service status:

1. Open Windows Services Manager (`services.msc`). For more information, refer to your Windows documentation.
2. In Windows Services Manager, look for the service named **ScannerWorkerService**.
3. Check the **Status** column.

Restarting the sensor service in a classic Fortify WebInspect installation

If the service is currently running, but you need to stop it:

- In Windows Services Manager, right-click the service named **ScannerWorkerService**, and then select **Stop**.

To restart the service:

- In Windows Services Manager, right-click the service named **ScannerWorkerService**, and then select **Start**.

Checking the sensor service status in ScanCentral DAST sensor in Windows

To check the service status in Microsoft Windows®:

- In PowerShell, enter the following commands:

  ```
  docker exec -it containerID powershell
  get-process -Name "DAST.ScannerWorkerService"
  ```

  If the service is running, you will see statistics for a process named "DAST.ScannerWorkerService." If the service is not running, you will receive an error.

  ```
  get-process : Cannot find a process with the name "WebInspect". Verify the
  process name and call the cmdlet again.
  ```

Checking the sensor service status in ScanCentral DAST sensor in Linux

To check the service status in Linux®:

- At the command prompt, enter the following command:

  ```
  ps -C DAST.ScannerWorkerService
  ```

  If the service is running, you will see statistics for a process named "DAST.ScannerWorkerService." If the service is not running, you will receive an error.

Restarting the sensor service in ScanCentral DAST sensor in Windows

If the service is currently running, but you need to stop it in Microsoft Windows®:

- In PowerShell, enter the following command:

  ```
  stop-process -Name "DAST.ScannerWorkerService.exe"
  ```

To start the service again in Microsoft Windows®:

- In PowerShell, enter the following command:

  ```
  start-process -Name "DAST.ScannerWorkerService.exe"
  ```

Restarting the sensor service in ScanCentral DAST sensor in Linux

If the service is currently running, but you need to stop it in Linux®:

- At the command prompt, enter the following command:

  ```
  pkill DAST.ScannerWorkerService.exe
  ```

To start the service again in Linux®:

- At the command prompt, enter the following:

  ```
  DAST.ScannerWorkerService.exe
  ```

Troubleshooting alerts

Alerts do not always indicate that there is a scan quality issue. Some alerts may be false positive. However, alerts may provide insight into issues that could adversely affect the scan.

Disabling alerts

You cannot currently disable alerts in the ScanCentral DAST user interface. For assistance in disabling individual alerts, contact Customer Support. For more information, see "Preface" on page 30.

Alerts troubleshooting table

Important! Any solutions involving changes to scan settings must be made for a future scan. You cannot change the scan settings for the current scan.

The following table describes possible causes and solutions for alerts.

Alert	Possible Cause	Possible Solution
EXCESSIVE LOGIN	The login macro has been played an excessive number of times for the number of requests made. The login credentials may be incorrect or the logout signature may be invalid.	Do one of the following: • Perform troubleshooting procedures on the macro. • Record a new login macro. For more information, see the *OpenText™ Fortify DAST Tools Guide*.
REDUNDANT CONTENT	Redundant content has been detected.	You might be able to improve performance in a future scan by enabling redundant page detection. For more information, see "Configuring redundant page detection" on page 204 or "Configuring redundant page detection in base settings" on page 413.
RESPONSE TIME	Responses coming from the web server are taking longer than average or longer than expected. A longer response time may result in a slower scan.	Check your network connectivity or the performance of the application under test (AUT).

Alert	Possible Cause	Possible Solution
WAF DETECTED	A web application firewall (WAF) signature has been detected.	Disable the WAF that is protecting the AUT.

Testing login macros

The Fortify DAST sensor performs tests on the login macro in the following instances:

- When an auto-generated macro, newly-recorded macro, or pre-existing macro is tested during scan configuration
- At the start of the scan with any login macro if **Enable macro validation** is selected in the scan settings

Note: Macro testing is not supported for macros containing two-factor authentication.

Validation tests performed

The following table describes the tests that the Fortify DAST sensor performs.

Test	Result of Failure
Determine if the validation step is missing.	The scan continues, but a warning is written to the scan log.
Monitor the behavior when incorrect credentials are used.	
Determine whether the landing page is accessible with a login state.	
Determine whether the landing page is accessible without a login state.	
Determine if the site can handle multiple logins concurrently. The default number of concurrent logins tested is 5.	
Verify that the auto-generated macro logs into the application.	The scan stops and an error is written to the scan log.

Test	Result of Failure
Verify that the replay of the macro logs into the application.	

If a scan stops after failing a test, it may be possible to examine the specific error message in the scan log to determine and resolve the issue. Use the error message and the troubleshooting tips in this topic to help resolve the issue.

Troubleshooting tips

In all cases of macro failure, it is possible that an invalid macro was recorded. However, a previously good macro that fails is almost always due to site changes or credentials.

The following table provides possible causes and solutions for each error message.

Note: This table does not include all possible causes and solutions for each error message. Additional troubleshooting may be necessary.

Error Message	Possible Cause	Possible Solution
Automatic login generation failed	The login macro could not be created because the user credentials provided are not valid.	Try the Auto-gen Login Macro option again using credentials that are known to be valid.
Execution Failed	An HTML element, such as a verification element, username, or password, was not located.	Record a new macro in the Web Macro Recorder to identify the login input elements.
	The username has been deactivated (removed from the database) and/or the password has changed.	Record a new macro in the Web Macro Recorder using credentials that are known to be valid.
Logged in verification step not found	The login macro does not contain a verification step.	Edit the macro in the Web Macro Recorder to add a verification step to indicate a successful login.
Verification step did not fail after invalid login	The verification step succeeded after an invalid login attempt. A valid	Edit the macro in the Web Macro Recorder to select another object for the verification step.

Error Message	Possible Cause	Possible Solution
	verification step should only succeed upon successful login. This indicates that an incorrect login verification object was selected.	

For specific information about using the Web Macro Recorder, see the *OpenText™ Fortify DAST Tools Guide*.

Checking and restarting the OpenText DAST (Fortify WebInspect) REST API service

You can check to see whether the Fortify DAST REST API service is running, and then stop and/or restart the service if needed.

Checking the Fortify DAST REST API service status in a classic Fortify DAST installation

To check the service status:

- Right-click the **Fortify DAST Monitor** icon.
  If the service is running, you will see the "Stop DAST API" option in the menu.

Restarting the service in a classic Fortify DAST installation

If the service is currently running, but you need to stop it:

- Right-click the **Fortify DAST Monitor** icon, and then click **Stop DAST API**.

To restart the service:

- Right-click the **Fortify DAST Monitor** icon, and then click **Start DAST API**.

  Note: The start option may not be available until the service has fully stopped.

Checking the Fortify DAST REST API service status

To check the service status:

- In Windows PowerShell, enter the following command:

```
Get-Service -Name "WebInspect API"
```

Restarting the service for Fortify DAST

Tip: If you need to restart both the Fortify DAST API and the sensor service, restarting the container restarts both.

If the service is currently running, but you need to stop it:

- In Windows PowerShell, enter the following command:

```
net stop "WebInspect API"
```

To start the service again:

- In Windows PowerShell, enter the following command:

```
net start "WebInspect API"
```

Appendix B: Scanning with a Postman collection

You can use your existing Postman automation test scripts, also known as collections, to conduct scans of REST API applications. This section provides general information about Postman, tips for creating a good Postman collection, and instructions for manually configuring dynamic tokens for authentication.

For information about configuring a Postman scan, see "Configuring an API scan" on page 167.

What is Postman?

Postman is an API development environment that allows you to design, collaborate on, and test APIs. Postman lets you create collections for your API calls, where each collection can be organized into subfolders and multiple requests. You can import and export collections, making it easy to share files across your development and testing environment. Using a Collection Runner such as Newman, tests can be run in multiple iterations, saving time on repetitive tests.

Benefits of a Postman collection

A REST API application does not expose all the endpoints in a format that a human with a browser or an automated tool can consume. It is often simply a collection of endpoints that accepts various posts, puts, and gets with a specific set of request data. To successfully audit these endpoints, the ScanCentral DAST sensor needs to understand key details about the API. A well-defined Postman collection can expose these endpoints so that the sensor can audit the API application.

Known limitations with Postman variables

ScanCentral DAST does not support Global variables or Data variables in Postman. However, it does support Environment and Collection variables, as well as Local variables in a collection.

As a workaround, you can specify Global variables and Data variables in an Environment, which is a set of variables that you can use in your Postman requests.

Postman prerequisites

A Postman collection version 2.0 or 2.1 is required for conducting scans in ScanCentral DAST. The remaining prerequisite software is installed on the OpenText DAST (Fortify WebInspect) image.

Tips for preparing a Postman collection

This topic provides tips for creating a good Postman collection.

Ensure valid responses

To get valid responses, the collection must be complete and executable. Requests must include:

- A valid request URL
- The correct HTTP method (POST, GET, PUT, PATCH, or DELETE)
- Valid parameter data that allows proper exercising of the API

  For example, if you have a “name” parameter, then you must provide actual sample data such as "King Lear" or "Hamlet," rather than the default data type “string.”

Order of requests

Remember that the order of operations or requests is important. For example, you must create (or POST) sample data to a parameter before you can do a GET or a DELETE operation on the data.

Tip: To avoid URL errors while running the collection in the ScanCentral DAST sensor, after bundling the API requests in the correct order in your collection, save each request individually by clicking the request and then clicking **Save**.

Handling authentication

If your API requires authentication, you must configure it in the Postman collection. Follow these guidelines when configuring authentication:

- The user credentials must be current and not expired.
- If you use an environment to specify authentication information, select the type of authentication environment in the Postman collection.
- It is possible that not all requests in the collection require authentication or not all requests require the same type of authentication. If this is the case in your collection,

be sure to specify the appropriate authentication type for each request in the collection.

Important! If session state is lost while using various authentication types in a scan, it will not be restored correctly. For proper restoration of session state, use a login macro or Postman login collection with a single type of authentication.

Using static authentication

When using static authentication, you must hard-code user credentials as a name/value pair in the Postman collection. When the ScanCentral DAST sensor parses the collection file, it determines the type of authentication being used and retrieves the key name and value from the collection. These values are then added to the scan settings.

The ScanCentral DAST sensor supports the following types of static authentication:

- API Key
- Basic
- Bearer Token
- Digest
- NTLM
- Oauth 1.0
- Oauth 2.0

Using dynamic authentication

When using dynamic authentication, you must store the Bearer token or API key authentication variables in either a Postman environment file or a collection file. For example, a Bearer Token may use a variable such as `{{bearerToken}}`.

You must use regular expressions in a response state rule to dynamically supply the Bearer token or API key during the scan. The response state rule provides search and replace options that enable the token or key to be retrieved from a response and then used in future sessions.

Using a Postman login macro

You can provide a login macro and a workflow macro in the form of Postman collection files when configuring scan settings. For example, you can specify a login macro file such as `LoginBearer.json`. When using a login macro, however, you must also specify a logout condition, such as the regular expression `The\stoken\sis\snot\svalid`.

Postman auto-configuration

Auto-configuration for static authentication is supported when the authentication values are known, such as when the username and password are hard-coded in the authentication section of the collection. If auto-configuration is not disabled, ScanCentral DAST checks the authentication portion of the collection file for valid values that are then applied to the scan settings.

Auto-configuration for dynamic authentication attempts to automatically provide a login macro and response state rule. It is useful when the Bearer token or API key is stored in a variable. If successfully validated, the authentication sessions are added to the sessions table. If a Bearer token was detected but a stable configuration was not created, then no authentication sessions are added to the sessions table.

Important! Auto-configuration for dynamic authentication works only for simple cases using Bearer token authentication.

If auto-configuration fails, you must manually configure authentication. For more information, see "Manually configuring Postman login for dynamic tokens" below.

Sample Postman scripts

Sample code for leveraging the Postman API can be found at https://github.com/fortify/WebInspectAutomation.

A sample Postman collection is available for download on the Fortify repository on GitHub at https://github.com/fortify/WebInspectAutomation/tree/master/PostmanSamples.

Manually configuring Postman login for dynamic tokens

This topic describes how to configure dynamic authentication manually if auto-configuration fails for a Postman scan. Dynamic authentication uses dynamic tokens.

What are dynamic tokens?

Dynamic tokens are authentication tokens that are generated by software and are unique for each instance of authentication. Tokens can be created for a short period of time, and each instance is renewed individually.

Before you begin

You must know the following to configure manual login:

- The type of authentication used in your application (such as Bearer, API key, OAuth1.0, OAuth 2.0, Cookie)
- How to create regular expression search arguments

Process overview

The process to manually configure login is described in the following table.

Stage	Description
1.	Identify and isolate the login request or requests in a separate Postman collection. For more information, see "Identifying and isolating the login request" below.
2.	Create a logout condition regular expression. For more information, see "Creating a logout condition with regular expressions" on the next page
3.	Create a response state rule. For more information, see: • "Creating a response state rule for a bearer token" on the next page • "Creating a response state rule for an API key" on page 508 **Note:** A response state rule is not needed for cookie session management.

Identifying and isolating the login request

To identify and isolate the login request:

1. Examine the Postman collection contents to identify the login request.

   Tip: Typically, the login request is the first request in the Postman collection that obtains an authentication token. However, authentication could involve several requests.

2. Copy this request or multiple requests.
3. Paste the request(s) in a separate file.
4. Save the file as a Postman collection.

Creating a logout condition with regular expressions

To create a logout condition:

1. Find several requests that require authentication.
2. Do one of the following:
   - For a bearer token, replace the auth token with an incorrect value and send it to the application.
   - For an API key, send an incorrect APIKey value to the application.
3. Use the reply from these requests to create a regular expression that matches these responses and does not match a valid session.

   For example, if you see the word “unauthorized” in most cases, then it is the best word to use in the regular expression, such as:

   ```
   [STATUSCODE]200 AND [BODY]unauthorized
   ```

   If an incorrect APIKey value gets a reply of “{"status": "Access Deny"}”, then the best regular expression would be:

   ```
   [BODY]Access\sDeny
   ```

Creating a response state rule for a bearer token

To create a response state rule for a bearer token, you must create two regular expressions.

The first regular expression searches all responses for an authentication token update. Typically, this token will be in response to the login request that was identified in Stage 1 of the process.

For example, in the following response, we see a reference to "token."

```
"{"success":true,"message":"Authentication
      successful!","token":"eyJhbGciOiJIUzI1NiIs
      InR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluI
      iwiaWF0IjoxNTg1NzQzNzkzLCJleHAiOjE1ODU3NDc
      zOTN9.i8uXa20JQt00tlOjd1twRD76jTnsG-0xiU97
      QWy6jkg"}"
```

For this response, we can create the following regular expression:

```
"token":"(?<Token>[-a-zA-Z0-9._~+/]+?=*)"}$
```

In this regular expression, the `(?<Token>[-a-zA-Z0-9._~+/]+?=*)` identifies the value of the token.

Note: XML uses character escaping. When you use regular expressions that include < and > symbols in XML format, the < symbol escapes with `<` and the > symbol escapes with `>`.

The second regular expression indicates where to store this token. For a bearer token, it will be in the “Authorization: Bearer ….” header.

The following is an example for a bearer token:

```
"Authorization:\sBearer\s(?<Token>[^\r\n]*)\r\n"
```

In this second regular expression, the `(?<Token>[^\r\n]*)` identifies the value that should be replaced with the value from the first regular expression.

Creating a response state rule for an API key

To create a response state rule for an API key, you must create two regular expressions.

The first regular expression searches all responses for an authentication token update. Typically, this token will be in response to the login request that was identified in Stage 1 of the process.

For example, assume that you have a header API key type of auth. A request sends the username and password to the path “/Login” and returns a response similar to the following:

```
"{"success":true,"APIToken":
      "tp8989ieupgrjynsfbnfgh9ysdopfghsprohjo"}"
```

All protected requests send an “APIKey: ….” header to authorize access.

For this response, we can create the following regular expression:

```
"APIToken":"(?<APIToken>[a-zA-Z0-9]+?)"}$
```

Note: XML uses character escaping. When you use regular expressions that include < and > symbols in XML format, the < symbol escapes with `<` and the > symbol escapes with `>`.

The second regular expression indicates where to store this token. For an APIKey, it could be a custom header name and value or a custom query parameter name and value.

```
APIKey:\s(?<APIToken>[^\r\n]*)\r\n
```

Appendix C: Working with the Regex Editor

A regular expression is a pattern that describes a set of strings. Regular expressions are constructed similarly to mathematical expressions by using various operators to combine smaller expressions. The Regex Editor enables you to construct and test regular expressions.

Accessing the Regex Editor in ScanCentral DAST

You can access the Regex Editor from the Tools menu of any input box in the user interface that accepts regular expressions.

To access the Regex Editor:

1. Click **Tools menu** ⋮.

   Note: For some input boxes, the Tools menu icon is visible only after you have selected a checkbox indicating that a regular expression will be used or selected an entry type of Regex.

2. Select **Regex Editor**.

   The Regex Editor opens. If the input box contains a value, then the regular expression value in the Regex Editor is populated with the value from the input box.

Finding matching text

You can use the Regex Editor to search text for matches to a regular expression. For example, you may want to find a string of text in an HTTP request or response message.

To find matching text:

1. In the **Regex Select Type** list, select **Match**.
2. In the **Regular Expression** box, construct or paste a regular expression that you think will match the target text.

   For information about available regular expression options, see "Using regular expression options" on page 511.

   For assistance in constructing a regular expression with snippets, see "Working with sample snippets" on page 512.

Note: If you open the Regex Editor from an input box that includes a regular expression, the regular expression is populated in the Regular Expression box in the Regex Editor.

3. In the **TEST STRING** box, paste the text that you want to search.

   Note: If you open the Regex Editor from the HTTP REQUEST or RESPONSE area in scan visualization in ScanCentral DAST, the TEST STRING box is populated with the request or response.

4. Click **TEST**.

   Matches found in the TEST STRING box are highlighted, and all match details are displayed in the MATCHES area.

5. Click **OK** to copy the regular expression into the input box in ScanCentral DAST.

Replacing text

You can use regular expressions for pattern matching of sensitive personally identifiable information (PII). The Regex Editor includes a replace feature that enables you to view how PII that is detected using regular expressions will look after being scrubbed or redacted.

To replace text:

1. In the **Regex Select Type** list, select **Replace**.
2. In the **Regular Expression** box, construct or paste a regular expression that you think will match the target text.

   For information about available regular expression options, see "Using regular expression options" on the next page.

   For assistance in constructing a regular expression with snippets, see "Working with sample snippets" on page 512.

   Note: If you open the Regex Editor from an input box that includes a regular expression, the regular expression is populated in the Regular Expression box in the Regex Editor.

3. In the **TEST STRING** box, paste the text that you want to search.

   Note: If you open the Regex Editor from the HTTP REQUEST or RESPONSE area in scan visualization in ScanCentral DAST, the TEST STRING box is populated with the request or response.

4. In the **Replacement** box, type or paste the replacement text.
5. Click **TEST**.

   Matches found in the TEST STRING box are highlighted and redacted, and each match is listed separately in the MATCHES area.

Using regular expression options

You can use regular expression options to control how the regular expression pattern is interpreted.

To use an option:

1. Click the **Set Regex Options** icon (🏴).
   The REGEX OPTIONS list opens.
2. Select the option or options to use.
   Each selected option is prepended to the start of the regular expression.

Understanding the options

The following table describes the available regular expression options.

Option	Description	Inline Character
insensitive	Uses case-insensitive matching.	`i`
multi line	Uses multi-line mode, where the `^` and `$` characters match the start and end of a line, instead of the start and end of a string.	`m`
single line	Uses single-line mode, where the input string is treated as if it consists of a single line. The `.` character matches every character, instead of every character except `\n`.	`s`
explicit capture	Captures only explicitly named or numbered groups. The following examples show the groups named `Dir` and `page`: `/(?<Dir>.*)/?` `/(?<page>[^\/]*.[^/]*)$`	`n`
ignore white space	Ignores unescaped white space in the regular expression pattern.	`x`

Working with sample snippets

The QUICK REFERENCE area provides sample snippets of popular regular expression functionality and operators. You can use these snippets to build a regular expression pattern.

Filtering sample snippets

By default, all sample snippets are available for use in the QUICK REFERENCE area. However, you can filter by category to aid in locating a specific snippet.

To filter snippets for a specific category:

- In the **QUICK REFERENCE** area, select the category whose samples you want to view. Categories are as follows:
  - **Common** – snippets that match on many common alphanumeric patterns, such as any character between a and z or any digit. For more information see "Understanding common sample snippets" on the next page.
  - **Web Helpers** – snippets that match on common web application components, such as URLs and parameters. For more information see "Understanding web helper sample snippets" on page 515.
  - **Extensions** – extensions that enable pattern matching in specific parts of requests and responses. For more information see "Understanding the regular expression extensions" on page 516.
  - **Operators** – operators that enable you to combine snippets to build complex regular expression patterns. For more information see "Understanding the regular expression operators" on page 517.

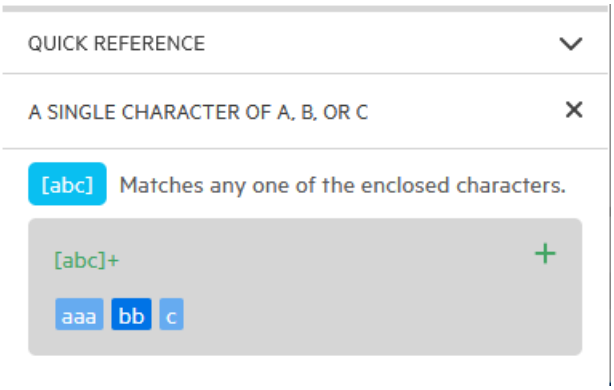
Viewing sample snippet details

All of the sample snippets include a brief description of its purpose, but some all common and some web helper snippets include a more detailed explanation and examples.

To view the snippet details:

- Click **See example** .

  The snippet syntax, description, and an example match are displayed.



To hide the snippet details:

- Click **Close regex example** ×.

Adding a snippet to your regular expression

You can add a snippet to your regular expression from the snippet list or from the regex example.

To add a snippet:

- Click **Add to regex** +.
  The snippet is added to the Regular Expression box.

Understanding common sample snippets

The common sample snippets include regular expression syntax for matching on character groups, word characters, non-word characters, digits, white-space characters, and non-white-space characters.

The following table describes the common sample snippets.

Match Target	Description / Regex Syntax
A single character of a, b, or c	Matches any one of the enclosed characters. `[abc]`
A character except a, b, or c	Matches any character not in the enclosed characters. `[^abc]`
A character in the range of a-z	Matches any characters between a and z, including a and z.

Match Target	Description / Regex Syntax
	`[a-z]`
A character not in the range of a-z	Matches any characters except those in the range of a-z. `[^a-z]`
A character in the range of a-z or A-Z	Matches any characters between a-z or A-Z. `[a-zA-Z]`
Any single character	Matches any single character except a newline character. `.`
Zero or more	Matches the preceding character zero or more times. `*`
One or more	Matches the preceding character one or more times. `+`
Or	Matches either what is before the | or what is after it. `|`
Any whitespace character	Matches any space, tab, or newline character. `\s`
Any non-whitespace character	Matches anything other than space, tab, or newline character. `\S`
Any digit	Matches any digit. Equivalent to [0-9]. `\d`
Any non-digit	Matches anything other than a digit. `\D`
Any word character	Matches any letter, digit, or underscore. `\w`
Any non-word character	Matches anything other than a letter, digit, or

Match Target	Description / Regex Syntax
	underscore. \W

Understanding web helper sample snippets

The web helper sample snippets include regular expression syntax with explicitly named groups for matching on common web application components.

The following table describes the web helper sample snippets.

Match Target	Description / Regex Syntax
IPv4 address	Matches an IPv4 IP address. (?<First>2[0-4]\d|25[0-5]|[01]?\d\d?) \.(?<Second>2[0-4]\d|25[0-5]|[01]?\d\d?) \.(?<Third>2[0-4]\d|25[0-5]|[01]?\d\d?) \.(?<Fourth>2[0-4]\d|25[0-5]|[01]?\d\d?)
URL	Matches a URL. (?<Protocol>\w+)://(?<Domain>[\w.]+)\S*
Directory	Matches a directory. /(?<Dir>.*)/?
Page	Matches a page. /(?<page>[^\/]*.[^/]*)$
Parameter	Matches a parameter name. (?<Param_paramname>[^;/?#]+)?
Matrix Parameter	Matches a matrix parameter. (?<matrixparamlocation>;(?<paramname>[^=\/?#;]+) =(?<Param_paramname>[^/?#;]+))

Understanding the regular expression extensions

OpenText engineers have developed and implemented extensions to the normal regular expression syntax. When building a regular expression pattern, you can use these extensions to specify in which element of the request or response to search for a match.

The following table describes the extensions.

Extension	Element
[ALL]	All elements of the request or response
[BODY]	Request Body Response Body
[COOKIES]	Cookie in the Request
[HEADERS]	Request Headers Response Headers
[METHOD]	Request Method
[POSTDATA]	Post Data
[REQUESTLINE]	Request Line (the start line of an HTTP request)
[SETCOOKIES]	Set-Cookie Response Header **Note:** This extension does not work in the Regex Editor. However, regular expressions using this extension will work outside of the editor.
[STATUSCODE]	Status Code
[STATUSDESCRIPTION]	Status Description (a string that describes the status of the HTTP output returned to the client)
[STATUSLINE]	Status Line (the start line of an HTTP response)
[URI]	The request target (a URI)
[VERSION]	HTTP Version

Examples of extension usage

The following examples demonstrate the use of the regular expression extensions:

- The following regular expression finds "200" in the status code:
  `[STATUSCODE]200`
- The following regular expression finds the string "password admin" in the response body:
  `[BODY]password\sadmin`
- The following regular expression finds a response containing the string "Please Authenticate" in the status description:
  `[STATUSDESCRIPTION]Please\sAuthenticate`

Understanding the regular expression operators

OpenText engineers have developed regular expression operators that you can use to construct complex regular expression patterns. The operators are:

- `AND`
- `OR`
- `NOT`
- `[]`
- `()`

Important! The operators must be separated from the regular expression syntax with spaces.

Examples of operator usage

The following examples demonstrate the use of the regular expression extensions:

- The following regular expression finds "200" in the status code or "OK" in the status description:
  `[STATUSCODE]200 OR [STATUSDESCRIPTION]OK`
- The following regular expression detects a response indicating that the requested resource resides temporarily under a different URI (redirection) and has a reference to the path "/Login.asp" anywhere in the response:
  `[STATUSCODE]302 AND [ALL]Login.asp`
- The following regular expression detects a response containing either (a) a status code of "200" and the phrase "logged out" or "session expired" anywhere in the body, or (b) a status code of "302" and a reference to the path "/Login.asp" anywhere in the response:

```
 ( [STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired ) OR (
[STATUSCODE]302 AND [ALL]Login.asp )
```

Tip: You must include a space before and after an "open" or "close" parenthesis. Otherwise, the parenthesis will be erroneously considered as part of the regular expression.

Appendix D: Reference lists

The following pages provide a list of policies that are available for use in ScanCentral DAST, as well as HTTP status codes for reference.

Policies

A policy is a collection of vulnerability checks and attack methodologies that the OpenText DAST (Fortify WebInspect) sensor deploys against a web application. Each policy is kept current through SmartUpdate functionality, ensuring that scans are accurate and capable of detecting the most recently discovered threats.

ScanCentral DAST contains the following packaged policies that you can use to determine the vulnerability of your web application.

Note: This list might not match the policies that you see in your product. SmartUpdate might have added or deprecated policies since this document was produced.

About OAST-related checks

For networks that have Internet access, the Fortify DAST sensor uses a public DNS service when running OAST-related checks. Ensure that your firewall does not block access to **fortify-oast.net**. For networks lacking Internet access, the Fortify OAST on Docker image is available. For more information, see the *OpenText™ Dynamic Application Security Testing and OAST on Docker User Guide*.

Best Practices

The Best Practices group contains policies designed to test applications for the most pervasive and problematic web application security vulnerabilities.

- **API**: This policy contains checks that target various issues relevant to an API security assessment. This includes various injection attacks, transport layer security, and privacy violation, but does not include checks to detect client-side issues and attack surface discovery such as directory enumeration or backup file search checks. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy is not intended for scanning applications that consume Web APIs.
- **CWE Top 25 *<version>***: The Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25) is a list created by MITRE. The list demonstrates the most widespread and critical software weaknesses that can lead to vulnerabilities in software.

- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **Best Practices** group.
- **General Data Protection Regulation (GDPR)**: The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and provides a framework for organizations on how to handle personal data. The GDPR articles that pertain to application security and require businesses to protect personal data during design and development of their products and services are as follows:
  - Article 25, data protection by design and by default, which requires businesses to implement appropriate technical and organizational measures for ensuring that, by default, only personal data that is necessary for each specific purpose of the processing is processed.
  - Article 32, security of processing, which requires businesses to protect their systems and applications from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data.

  This policy contains a selection of checks to help identify and protect personal data specifically related to application security for the GDPR.
- **NIST-SP80053R5**: NIST Special Publication 800-53 Revision 5 - (NIST SP 800-53 Rev.5) provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. This policy contains a selection of checks that must be audited to meet the guidelines and standards of NIST SP 800-53 Rev.5.
- **OWASP API Top 10 *<year>***: The OWASP API Top 10 *<year>* provides a list of the top security risks affecting APIs for the year specified. It aims to raise awareness around API security weaknesses and to educate those involved in API development and maintenance, such as developers, designers, architects, managers and/or organizations in general who need to secure Web APIs. The OWASP API Top 10 focuses on weaknesses affecting Web APIs and it is not intended to be used only by itself, instead it is intended to be used in combination with other standards and best practices to thoroughly capture all relevant risks. For example, it should be used in combination with the OWASP Top 10 to identify issues related to input validation such as injections.
- **OWASP Application Security Verification Standard (ASVS)**: The Application Security Verification Standard (ASVS) is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test, and verify secure applications.

  This policy uses OWASP ASVS suggested CWE mapping for each category of SecureBase checks to include. Because CWE is a hierarchical taxonomy, this policy also includes checks that map to additional CWEs that are implied from OWASP ASVS suggested CWE using a "ParentOf" relationship.

- **OWASP Top 10 *<year>***: This policy provides a minimum standard for web application security. The OWASP Top 10 represents a broad consensus about the most critical web application security flaws. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code. Multiple releases of the OWASP Top Ten policy may be available. For more information, consult the OWASP Top Ten Project.
- **SANS Top 25 *<year>***: The SANS Top 25 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software. These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to take over the software completely, steal data, or prevent the software from working altogether.
- **Standard**: A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities such as SQL Injection and Cross-Site Scripting as well as poor error handling and weak SSL configuration at the web server, web application server, and web application layers.

By Type

The By Type group contains policies designed with a specific application layer, type of vulnerability, or generic function as its focus. For instance, the Application policy contains all checks designed to test an application, as opposed to the operating system.

- **Aggressive SQL Injection**: This policy performs a comprehensive security assessment of your web application for SQL Injection vulnerabilities. SQL Injection is an attack technique that takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database. This policy performs a more accurate and decisive job, but has a longer scan time.
- **Apache Struts**: This policy detects supported known advisories against the Apache Struts framework.
- **Blank**: This policy is a template that you can use to build your own policy. It includes an automated crawl of the server and no vulnerability checks. Edit this policy to create custom policies that only scan for specific vulnerabilities.
- **Client-side**: This policy intends to detect all issues that require an attacker to perform phishing in order to deliver an attack. These issues are typically manifested on the client, thus enforcing the phishing requirement. This includes Reflected Cross-site Scripting and various HTML5 checks. This policy may be used in conjunction with the Server-side policy to provide coverage across both the client and the server.
- **Criticals and Highs**: Use the Criticals and Highs policy to quickly scan your web applications for the most urgent and pressing vulnerabilities while not endangering production servers. This policy checks for SQL Injection, Cross-Site Scripting, and other critical and high severity vulnerabilities. It does not contain checks that may write data to databases or create denial-of-service conditions, and is safe to run against

production servers.

- **Cross-Site Scripting**: This policy performs a security scan of your web application for cross-site scripting (XSS) vulnerabilities. XSS is an attack technique that forces a website to echo attacker-supplied executable code, such as HTML code or client-side script, which then loads in a user's browser. Such an attack can be used to bypass access controls or conduct phishing expeditions.
- **DISA STIG *<version>***: The Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) provides security guidance for use throughout the application development lifecycle. This policy contains a selection of checks to help the application meet the secure coding requirements of the DISA STIG *<version>*. Multiple versions of the DISA STIG policy may be available in the **By Type** group.
- **Mobile**: A mobile scan detects security flaws based on the communication observed between a mobile application and the supporting backend services.
- **NoSQL and Node.js**: This policy includes an automated crawl of the server and performs checks for known and unknown vulnerabilities targeting databases based on NoSQL, such as MongoDB, and server side infrastructures based on JavaScript, such as Node.js.
- **OAST**: This policy includes all checks that use Out-of-band Application Security Testing (OAST) technology in scanning logic.
- **Passive Scan**: The Passive Scan policy scans an application for vulnerabilities detectable without active exploitation, making it safe to run against production servers. Vulnerabilities detected by this policy include issues of path disclosure, error messages, and others of a similar nature.
- **PCI DSS 4.0**: The Payment Card Industry Data Security Standard 4.0 (PCI DSS 4.0) provides a baseline of technical and operational requirements designed to protect account data. This policy contains a selection of checks that need to be audited to meet the secure coding requirements of PCI DSS 4.0.
- **PCI Software Security Framework *<version>* (PCI SSF *<version>*)**: The PCI SSF provides a baseline of requirements and guidance for building secure payment systems and software that handle payment transactions. This policy contains a selection of checks that must be audited to meet the secure coding requirements of PCI SSF.
- **Privilege Escalation**: The Privilege Escalation policy scans your web application for programming errors or design flaws that allow an attacker to gain elevated access to data and applications. The policy uses checks that compare responses of identical requests with different privilege levels.
- **Server-side**: This policy contains checks that target various issues on the server-side of an application. This includes various injection attacks, transport layer security, and privacy violation, but does not include attack surface discovery such as directory enumeration or backup file search. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy may be used in conjunction with the Client-side policy to provide coverage across both the client and the server.
- **SQL Injection**: The SQL Injection policy performs a security scan of your web application for SQL injection vulnerabilities. SQL injection is an attack technique that

takes advantage of non-validated input vulnerabilities to pass arbitrary SQL queries and/or commands through the web application for execution by a backend database.

- **Transport Layer Security**: This policy performs a security assessment of your web application for insecure SSL/TLS configurations and critical transport layer security vulnerabilities, such as Heartbleed, Poodle, and SSL Renegotiation attacks.
- **WebSocket**: This policy detects vulnerabilities related to WebSocket implementation in your application.

Custom

The Custom group contains all user-created policies and any custom policies modified by a user.

Hazardous

The Hazardous group contains a policy with potentially dangerous checks, such as a denial-of-service attack, that could cause production servers to fail. Use this policy against non-production servers and systems only.

- **All Checks**: An All Checks scan includes an automated crawl of the server and performs all active checks from SecureBase, the database. This scan includes all checks that are listed in the compliance reports that are available in Fortify web application and web services vulnerability scan products. This includes checks for known and unknown vulnerabilities at the web server, web application server, and web application layers.

  Caution! An All Checks scan includes checks that may write data to databases, submit forms, and create denial-of-service conditions. OpenText strongly recommends using the All Checks policy only in test environments.

Deprecated checks and policies

The following policies and checks are deprecated and are no longer maintained.

- **Aggressive Log4Shell (Deprecated)**: This policy performs a comprehensive security assessment of your web application for JNDI Reference injections in vulnerable versions of Apache Log4j libraries. In vulnerable versions, Log4j does not restrict JNDI features. This allows an attacker who can control log messages to inject JNDI references that point to an attacker-controlled server. This can lead to remote code execution on the vulnerable target. Compared with other policies that include Log4Shell agent, this policy performs a more accurate and decisive job, but produces a significant number of requests and has a longer scan time.
- **Application (Deprecated)**: The Application policy performs a security scan of your web application by submitting known and unknown web application attacks, and only submits specific attacks that assess the application layer. When performing scans of

enterprise level web applications, use the Application Only policy in conjunction with the Platform Only policy to optimize your scan in terms of speed and memory usage.

- **Assault (Deprecated)**: An assault scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web server, web application server, and web application layers. An assault scan includes checks that can create denial-of-service conditions. It is strongly recommended that assault scans only be used in test environments.
- **Deprecated Checks**: As technologies go end of life and fade out of the technical landscape it is necessary to prune the policy from time to time to remove checks that are no longer technically necessary. Deprecated checks policy includes checks that are either deemed end of life based on current technological landscape or have been re-implemented using smart and efficient audit algorithms that leverage latest enhancements of core Fortify DAST framework.
- **Dev (Deprecated)**: A Developer scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web application layer only. The policy does not execute checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **OpenSSL Heartbleed (Deprecated)**: This policy performs a security assessment of your web application for the critical TLS Heartbeat read overrun vulnerability. This vulnerability could potentially disclose critical server and web application data residing in the server memory at the time a malicious user sends a malformed Heartbeat request to the server hosting the site.
- **OWASP Top 10 Application Security Risks - 2010 (Deprecated)**: This policy provides a minimum standard for web application security. The OWASP Top 10 represents a broad consensus about what the most critical web application security flaws are. Adopting the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code. This policy includes elements specific to the 2010 Top Ten list. For more information, consult the OWASP Top Ten Project.
- **Platform (Deprecated)**: The Platform policy performs a security scan of your web application platform by submitting attacks specifically against the web server and known web applications. When performing scans of enterprise-level web applications, use the Platform Only policy in conjunction with the Application Only policy to optimize your scan in terms of speed and memory usage.
- **QA (Deprecated)**: The QA policy is designed to help QA professionals make project release decisions in terms of web application security. It performs checks for both known and unknown web application vulnerabilities. However, it does not submit potentially hazardous checks, making it safe to run on production systems.
- **Quick (Deprecated)**: A Quick scan includes an automated crawl of the server and performs checks for known vulnerabilities in major packages and unknown vulnerabilities at the web server, web application server and web application layers. A quick scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.
- **Safe (Deprecated)**: A Safe scan includes an automated crawl of the server and performs checks for most known vulnerabilities in major packages and some unknown

vulnerabilities at the web server, web application server and web application layers. A safe scan does not run any checks that could potentially trigger a denial-of-service condition, even on sensitive systems.

- **Standard (Deprecated)**: Standard (Deprecated) policy is copy of the original standard policy before it was revamped in R1 2015 release. A standard scan includes an automated crawl of the server and performs checks for known and unknown vulnerabilities at the web server, web application server and web application layers. A standard scan does not run checks that are likely to create denial-of-service conditions, so it is safe to run on production systems.

HTTP status codes

The following list of status codes was extracted from the Hypertext Transfer Protocol version 1.1 standard (RFC 2616). You can find more information at http://www.w3.org/Protocols/.

Code	Definition
100	Continue
101	Switching Protocols
200 OK	Request has succeeded
201 Created	Request fulfilled and new resource being created
202 Accepted	Request accepted for processing, but processing not completed.
203 Non-Authoritative Information	The returned metainformation in the entity-header is not the definitive set as available from the origin server, but is gathered from a local or a third-party copy.
204 No Content	The server has fulfilled the request but does not need to return an entity-body, and might want to return updated metainformation.
205 Reset Content	The server has fulfilled the request and the user agent should reset the document view which caused the request to be sent.
206 Partial Content	The server has fulfilled the partial GET request for the resource.
300 Multiple Choices	The requested resource corresponds to any one of a set of representations, each with its own specific location, and agent-driven negotiation information (section 12) is being provided so

Code	Definition
	that the user (or user agent) can select a preferred representation and redirect its request to that location.
301 Moved Permanently	The requested resource has been assigned a new permanent URI and any future references to this resource should use one of the returned URIs.
302 Found	The requested resource resides temporarily under a different URI.
303 See Other	The response to the request can be found under a different URI and should be retrieved using a GET method on that resource.
304 Not Modified	If the client has performed a conditional GET request and access is allowed, but the document has not been modified, the server should respond with this status code.
305 Use Proxy	The requested resource MUST be accessed through the proxy given by the Location field.
306 Unused	Unused.
307 Temporary Redirect	The requested resource resides temporarily under a different URI.
400 Bad Request	The request could not be understood by the server due to malformed syntax.
401 Unauthorized	The request requires user authentication. The response MUST include a WWW-Authenticate header field (section 14.47) containing a challenge applicable to the requested resource.
402 Payment Required	This code is reserved for future use.
403 Forbidden	The server understood the request, but is refusing to fulfill it.
404 Not Found	The server has not found anything matching the Request-URI.
405 Method Not Allowed	The method specified in the Request-Line is not allowed for the resource identified by the Request-URI.
406 Not Acceptable	The resource identified by the request is only capable of generating response entities which have content characteristics

Code	Definition
	not acceptable according to the accept headers sent in the request.
407 Proxy Authentication Required	This code is similar to 401 (Unauthorized), but indicates that the client must first authenticate itself with the proxy.
408 Request Timeout	The client did not produce a request within the time that the server was prepared to wait.
409 Conflict	The request could not be completed due to a conflict with the current state of the resource.
410 Gone	The requested resource is no longer available at the server and no forwarding address is known.
411 Length Required	The server refuses to accept the request without a defined Content-Length.
412 Precondition Failed	The precondition given in one or more of the request-header fields evaluated to false when it was tested on the server.
413 Request Entity Too Large	The server is refusing to process a request because the request entity is larger than the server is willing or able to process.
414 Request-URI Too Long	The server is refusing to service the request because the Request-URI is longer than the server is willing to interpret.
415 Unsupported Media Type	The server is refusing to service the request because the entity of the request is in a format not supported by the requested resource for the requested method.
416 Requested Range Not Satisfiable	A server should return a response with this status code if a request included a Range request-header field (section 14.35), and none of the range-specifier values in this field overlap the current extent of the selected resource, and the request did not include an If-Range request-header field.
417 Expectation Failed	The expectation given in an Expect request-header field (see section 14.20) could not be met by this server, or, if the server is a proxy, the server has unambiguous evidence that the request could not be met by the next-hop server.
500 Internal Server	The server encountered an unexpected condition which

Code	Definition
Error	prevented it from fulfilling the request.
501 Not Implemented	The server does not support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting it for any resource.
502 Bad Gateway	The server, while acting as a gateway or proxy, received an invalid response from the upstream server it accessed in attempting to fulfill the request.
503 Service Unavailable	The server is currently unable to handle the request due to a temporary overloading or maintenance of the server.
504 Gateway Timeout	The server, while acting as a gateway or proxy, did not receive a timely response from the upstream server specified by the URI (e.g., HTTP, FTP, LDAP) or some other auxiliary server (e.g., DNS) it needed to access in attempting to complete the request.
505 HTTP Version Not Supported	The server does not support, or refuses to support, the HTTP protocol version that was used in the request message.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Customer Support at https://www.microfocus.com/support so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on Configuration and Usage Guide (ScanCentral DAST 26.4.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to fortifydocteam@opentext.com.

We appreciate your feedback!