opentext™

ArcSight SIEM as a Service

Software Version: 23.9.1

Quick Start for Administrators

Document Release Date: September 2023
Software Release Date: September 2023

Legal Notices

Open Text Corporation

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

Copyright Notice

Trademark Notices

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Quick Start for Administrators

This *Quick Start* enables you to get an overview of ArcSight SIEM as a Service (ArcSight or ArcSight SaaS), set up your credentials and those of your users, and start collecting data.

- "Understanding ArcSight SIEM as a Service" on page 5
- "Getting Started" on page 11
- "Checklist for Getting Started" on page 12
- "Managing and Maintaining ArcSight " on page 72
- "Appendix - Installation Files" on page 92

Intended Audience

This guide provides information for the Administrator who will manage the users and groups in your organization who will access ArcSight SaaS, as well as the individuals responsible for configuring and maintaining data ingested by the product.

Additional Documentation

- *ArcSight SIEM as a Service - Release Notes*, which provides an overview of the products deployed in this suite and their latest features or updates

For the most recent version of this guide and other ArcSight documentation resources, visit the documentation site for ArcSight SaaS.

Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@microfocus.com. We value your input and look forward to hearing from you.

For specific product issues, contact OpenText SaaS Customer Success Support team or email us at cyberressupport@microfocus.com. For outages, call +1 (855) 982-2261 (US).

For general corporate and product information, see the OpenText Website.

For interactive conversations with your peers and OpenText experts, become an active member of our community. The OpenText online community provides product information, useful links to helpful resources, blogs, podcasts and other social media channels.

Understanding ArcSight SIEM as a Service

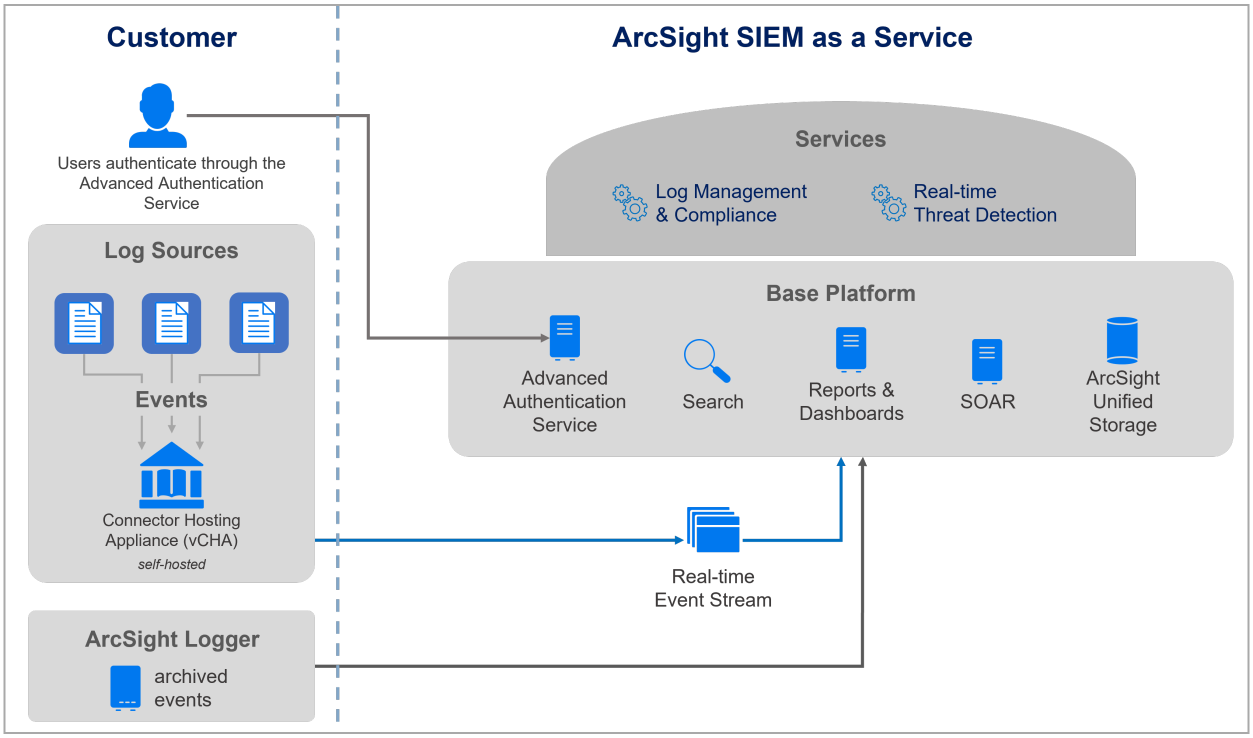
OpenText ArcSight SIEM as a Service (ArcSight) is deployed, configured, and maintained by OpenText. ArcSight ingests data from customer environments, making the data available for searches, reports, and other service-based activities. Customers can choose to use any combination of the available ArcSight Services.

Understanding the Architecture of ArcSight

ArcSight is a combination of security, user, and entity behavior analytics solutions integrated together so that you get the required benefits quickly without having to host or deploy the solutions yourself. However, you as the customer must host some data-collection components to ensure that data sources within your environment send data to ArcSight. To collect data, your local environment uses SmartConnectors.

For environments with only the Log Management and Compliance service, the SmartConnectors connect to an Amazon S3 destination through an AWS Identity and Access Management (IAM) user. If your environment includes the Real-time Threat Detection service, then the SmartConnectors connect to an ArcSight SaaS destination using credentials that OpenText provides. The SmartConnectors must have internet connectivity directly or through a proxy. By configuring the connectors to connect directly or through a proxy to the Amazon S3 bucket or ArcSight SaaS destination, you avoid the need to open specific firewall ports or establish a VPN connection for each connector. When you configure the SmartConnectors, you specify the Amazon S3 bucket or ArcSight SaaS destination as the destination for the collected data.

ArcSight is powered by a unified datastore that delivers high-speed query response and short-term archival storage across all of the ArcSight product components, as well as long-term archival storage for the Log Management and Compliance service. You can use the Search and reporting features in ArcSight SaaS to hunt for undetected threats, check data compliance, and create charts and dashboards to analyze filtered data. To improve efficiency in responding to cyberattacks, ArcSight SaaS includes SOAR as a part of its base platform. Use SOAR to ingest security events, triage, investigate cases, and automate your responses to incidents with playbooks automation. To have users access the service, you create user accounts in ArcSight. Note that, in the OpenText SIEM as a Service (SaaS) environment, all services use a limited version of Advanced Authentication Service to authenticate users that log in to all of the services.


Customer
ArcSight SIEM as a Service
Users authenticate through the Advanced Authentication Service
Log Sources
Events
Connector Hosting Appliance (vCHA)
self-hosted
ArcSight Logger
archived events
Services
Log Management & Compliance
Real-time Threat Detection
Base Platform
Advanced Authentication Service
Search
Reports & Dashboards
SOAR
ArcSight Unified Storage
Real-time Event Stream

Understanding the Base Platform

Understanding the ArcSight Services

Understanding Data Ingestion from Your Environment

Understanding the Base Platform

The base platform for ArcSight SIEM as a Service includes the following features:

- Advanced Authentication Service
- ArcSight Unified Storage
- Fusion
- Reports and Dashboards
- Search
- SOAR

For more information about using reports and dashboards, Search, SOAR, or other common features, see the Help in the product or the *User Guide for Fusion* on the documentation site for ArcSight.

Advanced Authentication Service

The Advanced Authentication component comes from the NetIQ suite of access products and services. Advanced Authentication delivers a full complement of security capabilities such as password enforcement and multi-factor authentication, including biometrics and SAML capabilities for federated integrations.

To have users access the service, you create user accounts in ArcSight. In the OpenText SIEM as a Service (SaaS) environment, all services use a limited version of Advanced Authentication Service to authenticate the users that log in to all of the services. When the ArcSight users log in, Advanced Authentication Service authenticates the users with their credentials.

ArcSight Unified Storage

A central part of the ArcSight SIEM is its integrated unified data storage. This datastore is used with each of the potential plug-in technologies. The data storage is a columnar datastore by design and delivers high-speed query response and long-term archival storage.

Fusion

Fusion manages the core services for ArcSight such as user, role, and group management; Search; SOAR; and the Reports Portal.

Reports and Dashboards

The Reports Portal provides built-in reports and dashboards, such as OWASP content, across the ArcSight technologies with one implementation. Use the portal to create charts and dashboards to visualize filtered data with tables, charts, and gauges. ArcSight reports and dashboards support all of the potential plug-in technologies within its modular architecture.

Search

The Search feature helps you investigate security issues by viewing search results and identifying outlier events.

SOAR (Respond)

ArcSight SOAR is a Security Orchestration, Automation, and Response (SOAR) tool that combines orchestration of both technology and people, automation, and incident management into a seamless experience. SOAR helps your security teams improve their efficiency in responding to cyberattacks in security operations. You can use SOAR to perform the following tasks:

- Ingest security events from multiple resources
- Case Creation and Management
- Triage, investigate cases, and track incidents in a unified user interface
- Automate your responses to incidents with playbooks automation

SOAR has over 100 integration points that allow for many different types of enrichment capabilities such as threat intelligence platforms, ticketing systems, and endpoint security tools.

Understanding the ArcSight Services

Your ArcSight SIEM as a Service environment can include the following plug-in services:

- ArcSight Log Management and Compliance
- Real-time Threat Detection

ArcSight Log Management and Compliance service

ArcSight Log Management and Compliance provides a modern log search and hunt solution powered by a high-performance, column-oriented, clustered database. With the Outlier Analytics feature you can identify anomalous behavior by comparing incoming event values to typical values for your environment. For more information, see the Help in the product or the *User's Guide for ArcSight SIEM as Service* on the documentation site for ArcSight.

Real-time Threat Detection service

Real-time Threat Detection analyzes and correlates every event that occurs across the organization to deliver accurate prioritization of security risks and compliance violations. Real-time Threat Detection provides a Big Data analytics approach to enterprise security, transforming Big Data into actionable intelligence.

Real-time Threat Detection combines traditional security event monitoring with network intelligence, context correlation, anomaly detection, historical analysis tools, and automated remediation. Real-time Threat Detection is a multi-level solution that provides tools for network security analysts, system administrators, and business users.

Understanding Data Ingestion from Your Environment

Your environment has the capabilities to ingest both live data (from SmartConnectors) or archived data (from Logger).

- " Ingesting Data from SmartConnectors" below
- " Ingesting Data from ArcSight Logger" on the next page

Ingesting Data from SmartConnectors

To collect data, your local environment uses SmartConnectors. These **SmartConnectors** intelligently collect a large amount of heterogeneous raw event data from devices in an enterprise network, process the data into ArcSight events, then compress and transport data to **destination** devices. SmartConnectors also automate the process of ingesting and managing logs from any device and in any format through normalization and categorization of logs into a unified format. They can parse individual events and normalize event values into the common event schema for log consumers.

You as the customer must host SmartConnectors to ensure that data sources within your environment send data to ArcSight. You can install or run these SmartConnectors from:

- Servers
- Local devices
- The cloud

Depending on how you configure the installed SmartConnectors, they will send data in batches to an Amazon S3 bucket destination as a temporary storage for collected events) or to an ArcSight SaaS destination as a live stream. ArcSight then consumes the data. When you receive the ArcSight SIEM as a Service account, OpenText provisions the destination for you to use and store the collected data. If you use just the Log Management & Compliance service, you will configure the Amazon S3 bucket and create an AWS IAM user account to properly configure the SmartConnectors. The SmartConnectors will connect to the S3 bucket as the AWS IAM user. However, if you use the Real-time Threat Detection service with or without Log Management service, you will configure the SmartConnector to send data to the ArcSight SaaS destination. You will need the host name of the MSK cluster and the user name and password that OpenText provides for SmartConnector configuration. The SmartConnectors will connect to the ArcSight SaaS destination using the provided credentials. For more information about configuring SmartConnectors to connect to MSK, see the *Installation Guide for SmartConnectors*.

The SmartConnectors must have internet connectivity directly or through a proxy. Configuring the connectors to connect directly or through a proxy to the configured destination avoids the need to open specific firewall ports or establish a VPN connection for each connector.

> **Note:** Although you might configure SmartConnectors to use the ArcSight SaaS destination, you will still need to create the AWS IAM user account. You need the account to access the Amazon S3 bucket to download the files for installing and upgrading the ArcSight components that your environment needs.

To help you effectively monitor and manage a large deployment of SmartConnectors, use the centralized management interface in **ArcSight Management Center (ArcMC)**.

You can install a standalone instance of ArcMC to manage multiple SmartConnectors. To use the full capabilities of ArcSight, review SmartConnector Installation Overview in the *Installation Guide for ArcSight SmartConnectors*.

Ingesting Data from ArcSight Logger

ArcSight SaaS can import archived data from all available Loggers, thus eliminating the need to continue managing them in your environment. The system stores the imported data in the ArcSight Database, making it available for Search and Reporting activities once the migration has completed successfully.

To perform the migration process, see "Setting Up Data Ingestion" on page 27 and Importing Logger Data to the ArcSight Database (SaaS).

Getting Started

OpenText manages and maintains ArcSight for your organization’s use, making it easier for you to use ArcSight capabilities with minimal effort on your part. However, to start using this service, there are some procedures that you will need to complete.

Checklist for Getting Started

Use this checklist to get started using ArcSight. Complete the tasks in the following order:

	Task	See
❑	1. Understand the components that comprise ArcSight	• "Understanding the ArcSight Services " on page 8 • "Understanding Data Ingestion from Your Environment" on page 9
❑	2. Review the technical requirements for installing the components in your environment	"Technical Requirements for Your Environment" on page 14
❑	3. Verify that you have the following items: • The information for the two tenant administrator accounts • Unique URL for accessing ArcSight	An email or package from OpenText that confirms your purchase of ArcSight
❑	4. Log in for the first time as the ArcSight Tenant Administrator for your organization	"Setting Up Credentials for Your ArcSight Tenant Administrator Account" on page 18
❑	5. Log in for the first time as the Advanced Authentication Tenant Administrator for your organization	"Setting Up Credentials for Your Advanced Authentication Tenant Administrator Account" on page 19
❑	6. (Optional) Configure your SaaS environment to use a form of advanced authentication	"Configuring SAML Authentication" on page 23 OR "Configuring Multi-factor Authentication" on page 21
❑	7. Understand how ArcSight can ingest data from your environment	"Understanding Data Ingestion" on page 27
❑	8. Prepare for data ingestion: a. Create a data ingestion account in AWS b. Give the Amazon Resource Name (ARN) of your AWS IAM user to the OpenText SaaS team c. Assign a policy to your AWS IAM user	"Preparing for Data Ingestion" on page 28
❑	9. (Optional) Import data from ArcSight Logger	"Importing Copied Logger Data to the SaaS Database" on page 39

□	10. (Conditional) For the Real-time Threat Detection service, install the console	"Setting Up the Real-time Threat Detection Console " on page 65
□	11. To install the data ingestion components: • For installing standalone SmartConnectors in specific locations OR • To use a standalone instance of ArcMC for installing and managing SmartConnectors	• "Installing Standalone SmartConnectors" on page 33 OR • "Installing a Standalone Instance of ArcMC" on page 34
□	12. To manage SmartConnectors using ArcMC: • Add already installed standalone SmartConnectors to ArcMC's management	• "Adding Standalone SmartConnectors to be Managed by ArcMC " on page 36
□	13. Add accounts for individuals in your environment who will use ArcSight	"Creating Additional User Accounts" on page 72
□	14. Notify your users of the process for logging in the first time	"First-time Login for New Users" on page 72

Technical Requirements for Your Environment

This section lists the hardware and software needed to run the data ingestion components and for users to access ArcSight, as well as requirements for the Real-time Threat Detection Console.

Browser Requirements

Your users can access ArcSight from one of the following browsers:

- Google Chrome
- Mozilla Firefox

Technical Requirements for Data Ingestion

These technical requirements represent what we determined to be necessary for handling the specified workload for a typical customer environment, as verified in our testing labs. The requirements for your environment might vary according to your needs.

For more information about available fresh or upgrade installers, see Appendix - Installation Files.

Category	Minimum Requirement
SmartConnectors* (ingest events)	Using only the Log Management service • 8.2.0 Patch 2 or later Using all available services • 8.4 or later **Note:** We recommend that you upgrade to SmartConnector 8.4 to take advantage of security and other defect fixes.
ArcSight Logger (migrate events)	Logger 7.2 (8372) or greater

*Applies when using the standalone ArcMC/SmartConnectors

Requirements for a Standalone ArcMC

For more information about technical requirements for ArcMC, see Technical Requirements for ArcMC in the *Release Notes for ArcMC*.

To install ArcMC, see Installing a Standalone Instance of ArcMC.

Requirements for Standalone SmartConnectors

For more information about the technical requirements for SmartConnectors, see *Technical Specifications for SmartConnectors*.

To install SmartConnectors, see Installing Standalone SmartConnectors.

Technical Requirements for Real-time Threat Detection Console

This section provides information about the technical requirements for the Real-time Threat Detection Console.

- Supported Platforms
- Supported Operating Systems
- Required Libraries for RHEL (64 bit)

Console Supported Platforms

The hardware requirements for the console are as follows:

	Minimum
Processor	Intel Core i5 2.4 GHz processor
Memory	8 GB RAM (16 preferred)

Console Supported Operating Systems

You can install the Real-time Threat Detection console on the following operating systems:

- Red Hat Enterprise Linux (RHEL) or Community Enterprise Operating System (CentOS) 7.9
- RHEL 8.6 or 8.4
- SUSE Linux Enterprise Desktop (SLES) 15 Service Pack 3
- macOS Big Sur
- Windows Server 2019
- Windows 10 Enterprise (including patches)

Required Libraries for RHEL and CentOS (64 Bit)

On RHEL and CentOS 64-bit workstations, the console requires the latest versions of the following libraries:

```
pam-1.1.1-10.el6.x86_64.rpm
```

```
pam-1.1.1-10.el6.i686.rpm
```

```
libXtst-1.0.99.2-3.el6.x86_64.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXp-1.0.0-15.1.el6.x86_64.rpm

libXp-1.0.0-15.1.el6.i686.rpm

libXmu-1.0.5-1.el6.x86_64.rpm

libXmu-1.0.5-1.el6.i686.rpm

libXft-2.1.13-4.1.el6.x86_64.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXext-1.1-3.el6.x86_64.rpm

libXext-1.1-3.el6.i686.rpm libXrender-0.9.7-2.el6.i686.rpm

gtk2-engines-2.18.4-5.el6.x86_64.rpm

gtk2-2.18.9-6.el6.x86_64.rpm

compat-libstdc++-33-3.2.3-69.el6.x86_64.rpm

compat-libstdc++-33-3.2.3-69.el6.i686.rpm

compat-db-4.6.21-15.el6.x86_64.rpm

compat-db-4.6.21-15.el6.i686.rpm
```

Setting Up and Managing Administrator Accounts

ArcSight uses a role-based access control model, which allows users to perform their role-based tasks. You can create new roles or modify the existing ones to suit your environment. Then assign users to those roles. The context-sensitive Help in ArcSight provides guidance for user and group management.

Understanding User Authentication

To authenticate users, ArcSight uses Advanced Authentication as a Service (the authentication service). In general, user credentials tend to be the combination of a valid email address (the username) and a password. The first time that a user logs in, they enter their username then follow the prompts to enter a **one-time password (OTP) code**, which they receive in an email.

Users can then choose which **Authentication Chain** method they want to use for authenticating their credentials in future logins: either receive OTP code or enter their **Password**.

OpenText provides you with two tenant administrator accounts. You use the ArcSight Tenant Administrator account to add more users to ArcSight. This guide assumes most users will choose the Password method for logging in. In the final step, users create their account password.

Understanding Your Two Tenant Administrator Accounts

The OpenText SaaS team provides you with two tenant administrator accounts:

ArcSight Tenant Administrator

Also known as the **Tenant Administrator for ArcSight**, this account allows you to manage ArcSight and its users. By default, this account has the *Admin* and *Analyst* roles in ArcSight.

You will need to create a password for this account. The account username is the email address specified by OpenText, which is usually based on the email address that your organization provided in the SaaS application.

> *NOTE:*The OpenText SaaS team does not provide you a password for the ArcSight Tenant Administrator account as you can log in to this account with an Email OTP.

Advanced Authentication Tenant Administrator

Also known as the **Tenant Administrator for the NetIQ Advanced Authentication as a Service**, this account enables you to manage your Advanced Authentication settings, such as password policy settings for your users.

The account username is the email address specified by OpenText, which is usually based on the email address that your organization provided in the SaaS application.

> The OpenText SaaS team provides you the password for the Advanced Authentication Tenant Administrator account. You must change it at first login so that it is a secret only you know.

Setting Up Credentials for Your ArcSight Tenant Administrator Account

As the ArcSight Tenant Administrator, you must configure your credentials before you can perform administrative tasks, such as creating other user accounts. In an email from OpenText, we confirm the email address that you will use to log in to your ArcSight Tenant Administrator account.

Before you set up your credentials, the default method for authenticating your account is **Email One-Time Password (OTP)**, which sends an (OTP) code to your specified email address. When you log in, after you have configured additional credentials, you will be prompted to Select Authentication Chain, which relates to the authentication method that you wish to use for that login session. The following steps show how to configure the authentication service to use the Password method instead of the OTP method for verifying your credentials.

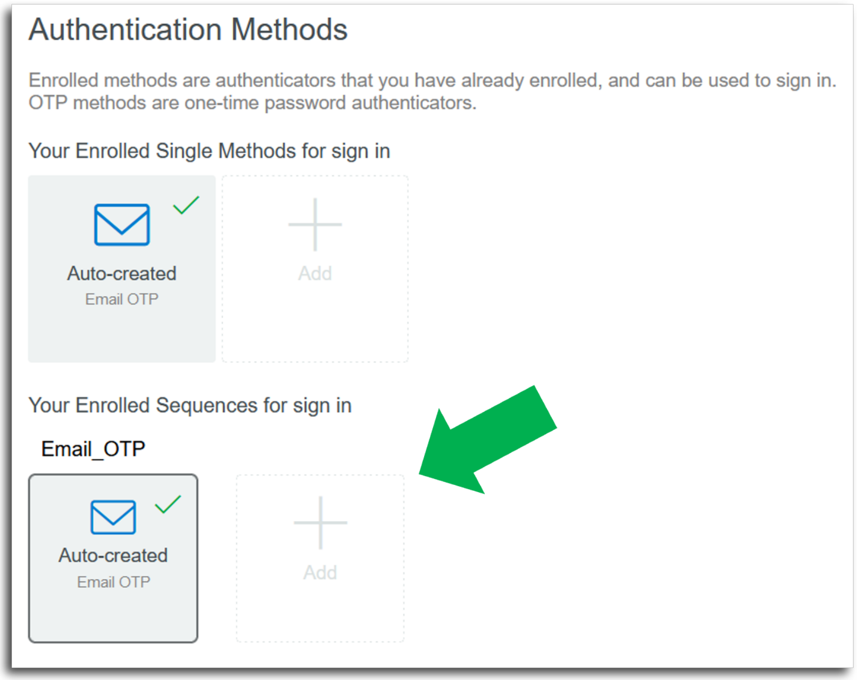
Your **username** is the email address specified by OpenText for the ArcSight Tenant Administrator account. To set up the credentials for this account, complete the following steps.

1. Log in to the Advanced Authentication service as the ArcSight Tenant Administrator to configure your credentials.
2. Check your email for a one-time password (OTP) code sent by the authentication service.
3. Enter the OTP sent to the email address for your ArcSight Tenant Administrator account, then click Next.

   > You will continue to be prompted to enter the Email OTP Code until you create a password and specify the Password method to authenticate your account.

4. Under **Your Enrolled Sequences for sign in** on the **Authentication Methods** page, click +Add.

Figure 1. *The green arrow indicates the appropriate +Add option that you should select*



Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

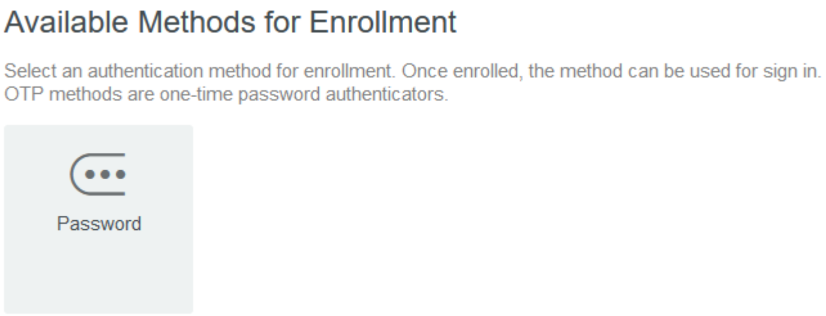
Your Enrolled Single Methods for sign in

Your Enrolled Sequences for sign in

Email_OTP

5. Click the Password option.

   Figure 2. *Password Enrollment Method*



Available Methods for Enrollment

Select an authentication method for enrollment. Once enrolled, the method can be used for sign in. OTP methods are one-time password authenticators.

6. Specify the password that you want to use for your ArcSight Tenant Administrator account, then click Finish.
7. Sign out of the Advanced Authentication service.

Setting Up Credentials for Your Advanced Authentication Tenant Administrator Account

The OpenText SaaS team provides the username and password for your Advanced Authentication Tenant Administrator account.

Changing the Password for the Account

The first time that you log in to the Advanced Authentication service, you must change the account password. It should be a credential that only you know. You can also configure your Advanced Authentication Tenant Administrator to use a one-time password (OTP) code to authenticate your credentials when you log in.

1. Log in to the Advanced Authentication service as the Advanced Authentication Tenant Administrator to change the account password.
2. Enter the password provided by the OpenText SaaS team.
3. On the Authentication Methods page, select the Password method.
4. Enter a new password.
5. Click Save.

   > OpenText recommends that you add Email OTP authentication to recover the account if the password is forgotten.

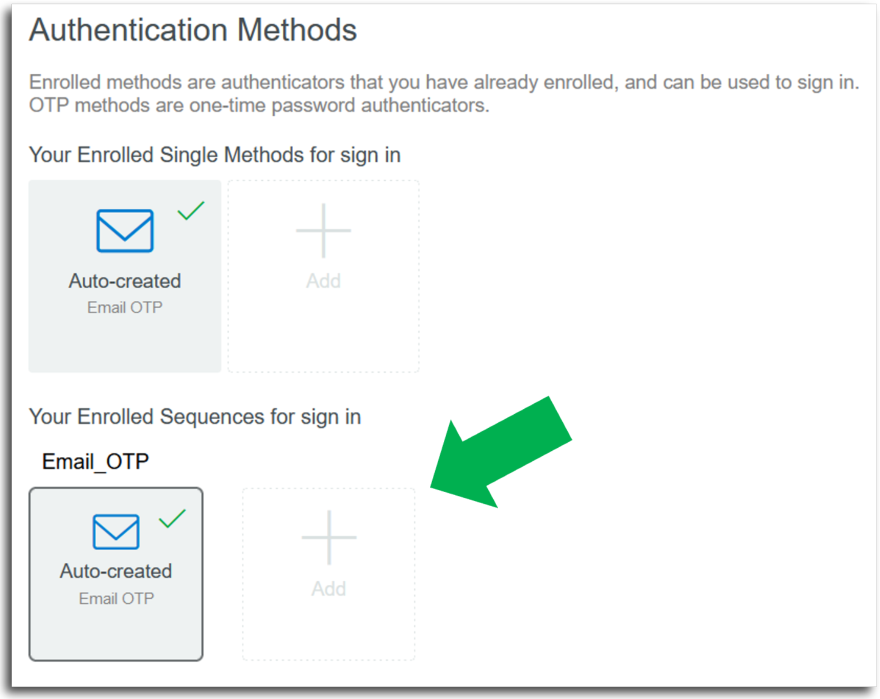
6. Sign out of the Advanced Authentication service.

Creating a Backup Method for the Account

OpenText recommends that you add Email OTP authentication to recover your Advanced Authentication Tenant Administrator account if the password is forgotten.

1. Log in to the Advanced Authentication service as the Advanced Authentication Tenant Administrator to add an authentication method.
2. Under **Your Enrolled Sequences for sign in** on the **Authentication Methods** page, click +Add.

Figure 3*. The green arrow indicates the appropriate +Add option that you should select*



Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in

Your Enrolled Sequences for sign in

Email_OTP

3. Click the Email OTP option.
4. Enter an Override Email ID.
5. Click Finish.
6. Sign out of the Advanced Authentication service.

Configuring Authentication

You can configure your SaaS environment to use a multi-factor authentication method or a trusted SAML provider to authenticate user logins. The Advanced Authentication service calls the combination of authentication methods a **chain**. The service also provides **authentication events** associated with login attempts. The procedures in this section enable you to create authentication chains and the events that correlate to the configured authentication methods.

For more information about chains, see “Creating a Chain” in the *Administrator’s Guide to Advanced Authentication*.

Configuring Multi-factor Authentication

You can enable multi-factor authentication for your users. When multi-factor authentication is enabled, first, the users will be prompted for password authentication and then for Email OTP, when they log in for the first time and thereafter.

To configure multi-factor authentication as a tenant administrator:

1. Log in to the Advanced Authentication service.
2. To create a chain of authentication, complete the following steps:
   a. From the left menu, select Chains.

      For more information about chains, see "Creating a Chain" in the Administrator's Guide to Advanced Authentication.

   b. Select New Chain
   c. For Authentication Methods, add the chain options in the following sequence:
      i. Password
      ii. Email OTP

      > Do not select authentication methods other than Password and Email OTP.

   d. For the repositories that use these authentication methods, specify the following names:
      - secops_localusers
      - igbootstraps

      > You must start typing the repo name before you can select it.

   e. Select Save.
3. To update authentication events, complete the following steps:
   a. From the left menu, select Events.
   b. Select the <tenant>-FUML event to update.
      i. Deselect current Chains in use.
      ii. Select the new chain that you created in Step 2.
      iii. Select Save.
   c. Select the <tenant>-FUMB event to update.
      i. Deselect current Chains in use.
      ii. Select the new chain that you created in Step 2.
   d. Select Save.

Configuring SAML Authentication

To use a trusted SAML identity provider, such as Okta, you must configure methods, chains, and events in Advanced Authentication. The metadata document for a trusted SAML identity provider, with which an SSO defined provider interacts, must be obtained in a provider-specific manner. While not all providers do so, many supply their metadata documents via URL.

- Checklist for Configuring SAML Authentication
- Configuring an External SAML Identity Provider
- Integrating with an External SAML Provider

Checklist for Configuring SAML Authentication

To configure an external SAML Identify Provider and proceed to integrate with it, you must complete the following steps in the given order:

	Task	See
❑	1. Configure Single Sign-On and Single Logout with your external SAML identity provider.	Configuring an External SAML Provider
❑	2. integrate with your external SAML identity provider.	Integrating with an External SAML Provider

Configuring an External SAML Identity Provider

You can configure an external SAML identity provider to use the metadata URL of Advanced Authentication SSO to derive the specific single sign-on and single logout URLs. These URLs include the following:

- Advanced Authentication single sign-on URL: https://aa.cyberresprod.com/osp/a/<tenant name>/auth/saml2/spassertion_consumer
- Advanced Authentication Entity ID, Issuer or Audience URL: https://aa.cyberresprod.com/osp/a/<tenant name>/auth/saml2/metadata
- Advanced Authentication single logout: https://aa.cyberresprod.com/osp/a/<tenant name>/auth/saml2/spslo

You can configure any external identity service provider. In the following section, Okta is used as an example of an external identity service provider. To configure Okta as an external service provider, complete the following steps:

- Configure Single Sign-On with Okta
- Configure Single Logout with Okta

> You can access the Signing Certificate, if and when required, from the Server Options page in the left-hand menu of Advanced Authentication.

For more information on Okta configurations, see Okta SAML App Integrations.

To Configure Single Sign-On with Okta:

1. Log in to Okta and go to **SAML Settings**.
2. Enter https://aa.cyberresprod.com/osp/a/<tenant name>/auth/saml2/spassertion_consumer as the Single Sign-On URL.

   > You must use this for both Recipient and Destination URLs

3. Enter https://aa.cyberresprod.com/osp/a/<tenant name>/auth/saml2/metadata as the Audience URL.
4. For attribute statements, specify, Name as *username* and Value as *user.email*.
5. Use default values for all other fields and follow on screen instructions to complete the configuration.

To Configure Single Logout with Okta:

1. Log in to Advanced Authentication and go to Server Options in the left-hand menu.
2. Click Signing Certificate to launch a pop-up window.
3. Copy content from“-----BEGIN CERTIFICATE-----" to”-----END CERTIFICATE-----” from the text on the pop-up window.
4. Paste the copied content into a new text file and save. For example, you can save the file as *aa_certificate.cert*.
5. Log in to Okta, go to SAML Settings and then click Show Advanced Settings.
6. Under Enable Single Logout, select the Allow application to initiate Single Logout check box.

   > When this check box is selected, if you log out of the application, the system logs you out of Okta and applications that use Okta SSO.

7. Enter https://aa.cyberresprod.com/osp/a/<tenant name>/auth/saml2/spslo as the Single Logout URL.

8. Enter https://aa.cyberresprod.com/osp/a/<tenant name>/auth/saml2/metadata as the SP Issuer.
9. Browse to select the saved *aa_certificate.cert* as the Signature Certificate and upload.
10. Follow on screen instructions to complete the configuration.
11. To create and update the latest Identity Provider Metadata file, follow the instructions in step 2 of Integrating with an External SAML Identity Provider.

> Any changes to Okta Single Sign-In or Single Logout configurations might require the associated Okta metadata file to be re-uploaded to the SAML Service Provider method in Advanced Authentication.

Integrating with an External SAML Identity Provider

> A user present in the external SAML identity provider solution must also exist in Advanced Authentication to proceed with integration. For more information, see Creating Additional User Accounts.

To integrate an external SAML identity provider:

1. Log in to the Advanced Authentication service.
2. To create the method for SAML authentication, complete the following steps:
   a. In the left menu, select Methods.
   b. Select SAML Service Provider.
   c. Click Add.
   d. For Authentication Type, select SAML.
   e. Click the save icon on the right.
   f. Enter a name for the Identity Provider.
   g. Enter *username* as the Assertion attribute.

   > Your assertion attribute must match in Advanced Authentication and your trusted SAML provider to complete the configuration successfully.

   h. Browse to select the Identity Provider Metadata File.
   i. Click the save icon on the right.
   j. Select Save.
3. To create a chain of authentication, complete the following steps:
   a. From the left menu, select Chains.
   b. Select New Chain.

c. For authentication Methods, select SAML Service Provider.

d. To specify the repo that uses this authentication method, select *secops_localusers*.

> You must start typing the repo name before you can select it.

e. Select Save.

4. To update the authentication event, complete the following steps:

   a. From the left menu, select Events.

   b. Select the <tenant>-FUML event to update.

   c. Deselect current Chains in use.

   d. Select the new chain that you created in Step 3.

   e. Select Save.

5. To update the Identity provider URL, complete the following steps:

   a. From the left menu, select Policies.

   b. Select Web Authentication.

   c. Select the Identity provider URL as https://aa.cyberresprod.com.

   d. Select Save.

Setting Up Data Ingestion

ArcSight uses SmartConnectors for data ingestion. SmartConnectors intelligently collect a large amount of heterogeneous raw event data from security devices in an enterprise network, process the data into ArcSight security events, and transport data to a destination. To help you effectively monitor and manage large SmartConnectors deployments, you can use the centralized management interface in ArcSight Management Center (ArcMC).

SmartConnectors and ArcMC can be deployed as standalone capabilities.

Understanding Data Ingestion

ArcSight SaaS can receive data from your environment through SmartConnectors that you deploy or by your migrating data from ArcSight Logger.

- "SmartConnectors" below
- " ArcSight Logger " on the next page

SmartConnectors

SmartConnectors can parse individual events and normalize event values into Avro format for log consumers and it sends these events to Amazon S3 and ArcSight SaaS destinations. Based on their configuration, SmartConnectors receive events over the network using SNMP, HTTP, Syslog, or proprietary protocols such as OPSEC. Managing SmartConnectors via an ArcMC instance offers centralized management and monitoring of SmartConnectors and remotely-deployed on customer-provisioned hosts. You can deploy each managed SmartConnector and bulk-configure with a standard Amazon S3 bucket or ArcSight SaaS destinations.

To understand and plan for data ingestion options that best match your requirements to use the full capabilities of ArcSight, review SmartConnector Installation Overview in the *Installation Guide for ArcSight SmartConnectors*.

You can install the data ingestion components in one of the following ways:

Standalone SmartConnectors

Enables deployment of only the SmartConnectors that you need, on operating systems that you install. These connectors deliver their event stream to the designated Amazon S3 or ArcSight SaaS destinations for data ingestion into ArcSight. This data ingestion method is usually required only when you deploy the SmartConnector in a location that ArcMC cannot reach.

Although not a recommended method, it is possible to deploy connectors on customer-provisioned hosts, with each connector independently configured to deliver their event stream to the designated Amazon S3 or ArcSight SaaS destinations for data ingestion.

Standalone SmartConnectors managed and deployed by a standalone ArcMC

Enables deployment and management of only the SmartConnectors that you need and ArcMC, on operating systems that you install.

> For maximum flexibility, you can deploy SmartConnectors in any mix of the SmartConnectors and ArcMC configurations, as determined by your environment and policy.

ArcSight Logger

If you have ArcSight Logger deployed, you can import the event data from your Loggers to ArcSight SaaS, thus allowing your users to run searches on those events. To do so, you must migrate first the metadata that defines the event archives, and then the event data. During the first phase of the migration process, the system temporarily stores the metadata files and archive catalogs in the AWS S3 bucket. After you complete the second phase of migration, the ArcSight Database stores the event data. Retention times in the Database depend on your product license. Users cannot search the event data until you complete the second phase.

For more information, see "Importing Copied Logger Data to the SaaS Database" on page 39.

Preparing for Data Ingestion

To prepare for setting up data ingestion, you must create an AWS Identity and Access Management (IAM) user and its associated policy.

Understanding the AWS IAM User

An AWS Identity and Access Management (IAM) user is an entity that you create in AWS, that allows you and data ingestion components you configure to access the Amazon S3 bucket for ArcSight provisioned for your tenant. The IAM user consists of a name and credentials. By creating and owning this IAM user, only you know the account’s credentials. You can change the credentials according to your preferred schedule without intervention from the OpenText SaaS team. This method gives you the highest level of security and convenience.

Before you create or configure the IAM user, review the following considerations:

- To comply with the principle of least privilege, a newly created IAM user has no privileges in the AWS account. You will need to assign a policy to the user.

- As a best security practice, the credentials for each IAM user should be unique and kept secure.
- Each IAM user can have two access keys (each with an `Access Key ID` and `Secret Access Key` pair) to enable key rotation. If you use the SmartConnector Amazon S3 destination, you should configure all of your SmartConnectors with the same access key. Then, when you perform a key rotation, use the other access key.

Creating an AWS IAM User

An AWS IAM user account is required for data ingestion. For more information, see "Understanding the AWS IAM User" on the previous page.

To create an IAM user, complete the following steps:

1. (Conditional) If your organization has an AWS account, log in to AWS.
2. (Conditional) If your organization does not have an AWS account, create an AWS Free Tier account, then log in to AWS.
3. Create an AWS IAM user.
4. For AWS Access Type, choose Programmatic Access and AWS Management Console Access.
5. When prompted, complete the following steps:
   a. For Set Permissions, click Next, which enables you to skip the step.
   b. (Conditional) For Add Tags, if you do not have a policy to tag users, click Next, which enables you to skip the step.
   c. (Conditional) For Add Tags, if you have a policy to tag users, add your tags then click Next.
6. In the final step of user account creation, select Close without saving the Access Key.

Providing the User ARN to the OpenText SaaS Team

For data ingestion purposes, your IAM user account needs access to the Amazon S3 bucket for ArcSight. You must provide the Amazon Resource Name (ARN) of your IAM user to the OpenText SaaS team in order for them to grant your IAM user the correct access. You do not need to reveal the credentials for the user.

> OpenText stores data ingestion installation files for both Log Management and Compliance and Real-time Threat Detection services in the Amazon S3 bucket for ArcSight.
> To download the files, see :
>
> Standalone SmartConnectors
> Standalone Instance of ArcMC
> Real-time Threat Detection Console

1. Log in to AWS.
2. Browse to AWS account.
3. Click the IAM User that you created.
4. Copy the displayed User ARN. For example, arn:aws:iam::111111111:user/iam-username.
5. Send the ARN to the OpenText SaaS team.
6. Expect the OpenText SaaS team to send you the following information to support data ingestion:

Information	Description
Account Number for the AWS IAM Role	For example, 222222222 You will use this information to download the data ingestion installers.
Name for the AWS IAM Role	For example, elo-222222222-ap-southeast-1-secopstn01-event-avro-role You will use this information to download the data ingestion installers.
ARN of AWS IAM Role	For example, arn:aws:iam::<Name of your S3 bucket> You will use this information to download the data ingestion installer and for the policy assigned to your IAM User.
Name for the Amazon S3 bucket	For example, 222222222-ap-southeast-1-secopstn01-avro
ARN for the Amazon S3 bucket	For example, arn:aws:s3:::<Name of your S3 bucket> You will need this information for the policy assigned to your IAM User.
Folder name for the Amazon S3 bucket	Use event-sync/in/<your_tenant_name> For example, event-sync/in/secopstn01
Amazon S3 Region Code	For example, ap-southeast-1
URL to the Amazon S3 Bucket	For example, https://s3.console.aws.amazon.com/s3/buckets/222222222-ap-southeast-1-secopstn01-avro/connector-download/ You will use this information to download the data ingestion installers.

Assigning a Policy to the AWS IAM User

For data ingestion purposes, your IAM User account must have a policy that specifies the ARN for the Amazon S3 bucket, which you received from the OpenText SaaS team. You can replace the existing JSON policy file. You can use any valid approach to apply policies to a given IAM User.

1. Log in to AWS.
2. Browse to AWS account.
3. Click the IAM User that you created.
4. In the Permissions Policies tab, select +Add inline policy.
5. Select the JSON tab.
6. Replace the existing JSON policy file with the following policy where <tenant bucket ARN> represents the ARN for the applicable Amazon S3 bucket.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToArcsightConnectorS3Location",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "<tenant bucket ARN>/*",
                "<tenant bucket ARN>"
            ]
        },
        {
            "Sid": "AllowDownloadsAssumeRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "<ARN of IAM role specified by OpenText SaaS
team>"
        }
    ]
}
```

For example:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessToArcsightConnectorS3Location",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::222222222-ap-southeast-1-secopstn01-avro/*",
                "arn:aws:s3:::222222222-ap-southeast-1-secopstn01-avro"
            ]
        },
        {
            "Sid": "AllowDownloadsAssumeRole",
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::222222222:role/elo-222222222-ap-
southeast-1-secopstn01-event-avro-role"
        }
    ]
}
```

7. Select Review Policy, then enter a name for the policy.

   For example, AllowAccessToArcsightConnectorS3Location

8. To complete the process, select Create Policy.

Installing the Data Ingestion Components

OpenText stores the installation files for SmartConnectors, Logger archive migration and ArcMC in the Amazon S3 bucket for ArcSight. To download the files, you will need your AWS IAM user and the information provided by the OpenText SaaS team.

To validate the downloaded files, also download their associated signature files (.sig). For example, ArcSight-8.2.0.8533.2-Connector-Linux64.bin.sig. OpenText provides a digital public key that is used to verify that the software you downloaded from the Amazon S3 bucket is indeed from OpenText and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the OpenText Code Signing site. If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please do not run the downloaded files again but contact OpenText SaaS Customer Success Support.

For more information about configuring the SmartConnectors after installing or adding them, review SmartConnectors Grand List - (A-Z) and Instant Connector Deployment in the *Arcsight Management Center Administrator's Guide*.

Note that some connector types might require additional, supplementary files to function correctly, such as Windows DLLs. Such files are not included in the connector installer file. For more information, see Managing Deployment Templates in the *Arcsight Management Center Administrator's Guide*.

To begin collecting data, install and configure the data ingestion components by using one of the following methods:

Installing Standalone SmartConnectors

You can install SmartConnectors on the machine hosting a standalone instance of ArcMC, another host machine, or the device. Standalone SmartConnectors do not require ArcMC.

> If you install the connector on a virtual machine, enable NTP for both host and guest systems to ensure proper timekeeping. For more information, see "Timekeeping best practices for Linux guests (1006427)" on the VMWare Customer Connect website.

To download the files, you will need your AWS IAM user and the information provided by the OpenText SaaS team:

1. Log in to the Amazon S3 Console as the AWS IAM user that you created for data ingestion.
2. To download data ingestion component installers from the S3 bucket, browse to the URL provided by the OpenText SaaS team.

   By default, the URL uses the format https://s3.console.aws.amazon.com/s3/buckets/<tenant bucket name>/connector-download/.

   For example: https://s3.console.aws.amazon.com/s3/buckets/222222222-ap-southeast-1-secopstn01-avro/connector-download/
3. Click your user name, and then select Switch Roles from the user menu.

   > If you performed the Switch Roles procedure earlier and did not clear the browser cache, the role to switch to appears under Role History which you can select, skip step 4, and save time.
4. Click the Switch Role button and enter the following details you received from the OpenText SaaS team to download the data ingestion component installers:

   a. Account

   b. Role

   c. (Optional) Display Name

   d. (Optional) Color

5. Click Switch Role.
6. Download the installation files for SmartConnectors.
7. Install the SmartConnectors.
8. Configure the SmartConnector. For more information about configuring the SmartConnector, see the see the *SmartConnectors Grand List - (A-Z)* page to refer to the documentation relevant for your SmartConnector.

   > When configuring a connector to use the Amazon S3 destination to send data to ArcSight, you must use the same Amazon Access Key for all connectors.

9. Configure one of the following destinations depending, on the SaaS services that you use:

Services in use	Destination	SmartConnector behavior
Log Management and Compliance only	Amazon S3	Sends batches of events to ArcSight
Either of the following scenarios: • Real-time Threat Detection only • Log Management & Compliance and Real-time Threat Detection	ArcSight SaaS	Sends a real-time stream of events to ArcSight

   For more information about configuring destinations, see the *Installation Guide for ArcSight SmartConnectors*.

10. (Conditional) Apply the latest parser update to the SmartConnectors:

    To download the parser update files for your SmartConnectors, go to ArcSight SmartConnector Parser Update in the ArcSight Marketplace. By default, the ArcSight-x.x.x.xxxx.x-ConnectorParsers.aup file that you download also includes the unobfuscated parser update, which allows you to modify the parsing logic as desired. For example, use the file ArcSight-8.3.3.8815.0-ConnectorParsers.aup.

11. Optimize the configuration of your SmartConnectors.

Installing a Standalone Instance of ArcMC

You can install a standalone instance of ArcMC in your environment to manage your SmartConnectors. The installer for the standalone ArcMC includes a built-in temporary license. Please request a permanent license from the OpenText SaaS team or your OpenText representative. For more information, see the *Arcsight Management Center Administrator's Guide*.

> If you install the connector on a virtual machine, enable NTP for both host and guest systems to ensure proper timekeeping. For more information, see “Timekeeping best practices for Linux guests (1006427)” on the VMWare Customer Connect website.

1. Review the requirements for installing ArcMC and SmartConnectors in your environment:
   a. Prerequisites for Installation in the *Arcsight Management Center Administrator’s Guide*
   b. Planning to Install and Deploy in the *Installation Guide for ArcSight SmartConnectors*
2. To download the files, you will need your AWS IAM user and the information provided by the OpenText SaaS team:
   i. Log in to the Amazon S3 Console as the AWS IAM user that you created for data ingestion.
   ii. To download data ingestion component installers from the S3 bucket, browse to the URL provided by the OpenText SaaS team.

      By default, the URL uses the format https://s3.console.aws.amazon.com/s3/buckets/<tenant bucket name>/connector-download/.

      For example: https://s3.console.aws.amazon.com/s3/buckets/222222222-ap-southeast-1-secopstn01-avro/connector-download/
   iii. Click your user name, and then select Switch Roles from the user menu.

      > If you performed the Switch Roles procedure earlier and did not clear the browser cache, the role to switch to appears under Role History which you can select, skip step 4, and save time.

   iv. Click the Switch Role button and enter the following details you received from the OpenText SaaS team to download the data ingestion component installers:
      A. Account
      B. Role
      C. (Optional) Display Name
      D. (Optional) Color
   v. Click Switch Role.
3. Download the installation files for ArcMC.
4. Install ArcMC.
5. Apply your ArcMC license.
6. (Conditional) Apply patches to ArcMC as needed.

   The files provided by OpenText might include a patch.

7. Install and configure SmartConnectors.
8. Add standalone SmartConnector to be managed by ArcMC.

Adding Standalone SmartConnectors to be Managed by ArcMC

If you have installed standalone SmartConnectors, you can add them by their IP address or FQDN in the standalone ArcMC.

When you use ArcMC, you can either use the Instant Connector Deployment functionality to install the SmartConnectors or complete the following steps to add SmartConnectors, if you have already installed them:

1. Log in to ArcMC.
2. Click Node Management > View All.
3. In the **Location** tab, click Default.
4. In the **Host** tab, click Add Host.
5. Specify the following information for Add a New Host:
    a. Enter the IP or FQDN address of the standalone SmartConnector that you already installed.
    b. Select Software Connector as Type:
        i. Enter the credentials for the SmartConnector.
        ii. Enter the port number.

Tuning SmartConnectors

The default settings of your SmartConnectors might not meet the needs for your environment. For example, by default they do not support event integrity checks, which validate that the event information in your database matches the content sent from SmartConnectors. Moreover, a SmartConnector might not use the full CPU capability.

Optimizing SmartConnectors to Your Event Flow

Although the default configuration of a SmartConnector might be sufficient for a lower EPS flow, you might want a higher EPS flow to get more out of your hardware. The default configuration values are as follows and also verifiable in ArcMC.

To optimize SmartConnector parameters:

1. Enable SSH for communication with ArcMC.

   For more information, see SSH Access to the Appliance to use standalone SmartConnectors, see User Management and Hosts in the ArcMC Help.

2. SSH in to /opt/arcsight/connectors/connector_<number>/current/user/agent/.

   > You could include Smart Connectors numbered 1 to 8.

3. In the agent.wrapper.conf file, modify the value 1024 to read 4096 for the following items:

   - wrapper.java.initmemory = 1024
   - wrapper.java.maxmemory = 1024

4. In the agent.properties file, modify the threadcount values based on the workload in your environment.

   > **Note:** The transport.avroawss3.threads property applies to Amazon S3 destinations. You only need to modify this parameter when Log Management and Compliance is the only service deployed.

   For example:

   - For medium workloads:

     ```
     syslog.parser.threadcount=4
     transport.avroawss3.threads=4
     ```

   - For large workloads:

     ```
     syslog.parser.threadcount=8
     transport.avroawss3.threads=8
     ```

5. To apply these changes, you must restart the modified SmartConnector:

   a. Browse to /etc/init.d.

   b. To restart the given SmartConnector, the following command:

      ```
      systemctl restart <connector_number>
      ```

      For example:

      ```
      systemctl restart arc_appliance_connector_6
      ```

   c. To verify the status of the given SmartConnector, the following command:.

      ```
      systemctl status <connector_number>
      ```

      For example:

      ```
      systemctl status arc_appliance_connector_6
      ```

For more information about tuning for a specific destination, see Destination Parameters in the *Installation Guide for ArcSight SmartConnectors*.

Configuring Event Integrity Checks

To validate that the event information in your database matches the content sent from SmartConnectors, run an **Event Integrity Check**. When you run the check, Log Management and Compliance searches the database for verification events received within the specified date range, then runs a series of checks to compare content in the database with information supplied by the verification event. The results of an Event Integrity Check help you identify whether event data might be compromised.

For more information about verification events and running integrity checks, see the Help for Recon.

Configuring a SmartConnector to Include a Verification Event for Raw Events

For a SmartConnector to support event integrity checks, you must enable it to include a verification event for each batch of events. This configuration ensures that the connector generates a verification event for the Raw Event field in an event at the moment that your environment captures it.

For this setting...	Enter...
Preserve Raw Event	Yes **NOTE**: When you enable this setting, the size of each event increases, which will require more storage space in your database.
Event Integrity Algorithm	SHA-256
Check Event Integrity Method	Recon

For more information about configuring SmartConnectors, see the following topics:

- “Configuring Processing” in the *Installation Guide for ArcSight SmartConnectors* (ArcSight SmartConnectors documentation)
- Destination Runtime Parameters

Creating Alerts for Real-time Threat Detection Events

Requires the Real-time Threat Detection service

When the Real-time Threat Detection service is deployed, SOAR automatically creates rule name filters for incoming correlation events. However, the system is configured to ignore all alert sources. To create alerts, you must configure the alert source rule name filter.

Importing Copied Logger Data to the SaaS Database

Requires archived event data in ArcSight Logger.

> This section applies to existing ArcSight Logger customers who want to import their data to the ArcSight SaaS environment. The Logger from which the information is being migrated can be either a software or an appliance version.

The process for migrating data from ArcSight Logger to ArcSight SaaS consists of two phases:

Phase One – Copy Metadata and Archived Event Data

On each Logger, use the Archive Migration Tool to copy the Logger data to an Amazon S3 bucket.

The first time that you run the tool, you will configure the Amazon S3 bucket to receive the files.

Executing the Archive Migration Tool will:

- Copy the files pertaining to the selected Logger archives to the Amazon S3 bucket.
- Generate an Archive Catalog file that contains information about the copied archives.
- Copy the Archive Catalog file to the Amazon S3 bucket to finish the process.

To complete this phase, follow the checklist in this Quick Start guide.

Phase Two – Import the Event Data

In ArcSight SaaS, import the copied Logger data to the ArcSight Database to make it available for searching and reporting. For more information about this phase, see Importing Logger data to ArcSight SaaS in the *User's Guide to ArcSight Platform*.

> Before you import event data from a Logger archive to the ArcSight Database (Phase Two), ensure that the Phase One process for copying the data from the Logger to the ArcSight SaaS S3 bucket has completed.

Checklist: Migrating Logger Data

Use the following checklist to migrate event data from Logger to ArcSight SaaS. You must perform the tasks in the listed order.

> This process assumes that you have already created the AWS IAM user and assigned it a policy, as described in "Preparing for Data Ingestion" on page 28.

	Task	See
❑	1. Ensure that you have the correct version of ArcSight Logger and that you have the correct credentials for the data migration	"Technical Requirements for Data Ingestion" on page 14 "Prerequisites for Importing Logger Data " below
❑	2. Install the **AWS Command Line Interface** in each of the Loggers that contain data to be imported	"Installing the AWS Command Line Interface in each Logger" on the next page
❑	3. Download the Archive Migration Tool	"Downloading the Archive Migration Tool" on the next page
❑	4. Installing the Archive Migration Tool in Each Logger	"Installing the Archive Migration Tool in Each Logger" on page 42
❑	5. Learn about using the Archive Migration Tool	"Navigating in the Archive Migration Tool" on page 43
❑	6. (Optional) Explore what you can do with the Archive Migration Tool	"Understanding the Archive Migration Tool " on page 54
❑	7. On each Logger, begin Phase One of the migration by copying Logger data to ArcSight SaaS	"Copying Logger Data to ArcSight SaaS" on page 43
❑	8. (Optional) Turn off Logger after you have copied all the Logger Data to ArcSight SaaS	"Removing a Logger after All Its Data Is Copied to ArcSight SaaS" on page 53
❑	9. Perform Phase Two of the migration by importing the copied data into the SaaS database	Importing Logger data to ArcSight SaaS

Prerequisites for Importing Logger Data

Since this process involves different ArcSight products interacting with each other, ensure that you have the correct credentials and requirements for all of them before you proceed.

- "Prerequisites for Logger" below
- "Prerequisites for the ArcSight Platform" on the next page

Prerequisites for Logger

- Logger installation user

> ⚠ OpenText does not recommend using a root user

- Follow the process detailed in "Preparing for Data Ingestion" on page 28 to obtain your:
  - **AWS S3 Bucket Tenant ID**: this is the `<your_tenant_name>` value mentioned in "Providing the User ARN to the OpenText SaaS Team" on page 29
  - **Access Key**: this is the `Access Key ID` from your IAM user, mentioned in "Understanding the AWS IAM User" on page 28
  - **Security Access Key**: this is the `Secret Access Key` from your IAM user, mentioned in "Understanding the AWS IAM User" on page 28

  You will need these values to set up and access your S3 bucket and to download the `logger-archive-catalog-tool-20230815.enc` file required to initiate metadata migrations.
- The **AWS Command Line Interface** has been installed in each Logger (see "Installing the AWS Command Line Interface in each Logger" below)

Prerequisites for the ArcSight Platform

- An AWS Identity and Access Management (IAM) user and its associated policy, created in "Preparing for Data Ingestion" on page 28
- For the migration process, the user must have the *Logger Data Migration* permission assigned in Fusion. This is assigned by default to the System Admin role, but the user could have a custom role that includes the permission.

Installing the AWS Command Line Interface in each Logger

> These steps must be performed by the Logger installation user. We do not recommend using a root user.

The **AWS Command Line Interface (CLI)** allows each of your Loggers to interact with Amazon services. This is necessary because the data being exported from Logger is temporarily saved into your Amazon S3 bucket for ArcSight during the migration process. The Amazon S3 bucket storage costs incurred during this process are included with your ArcSight SaaS license.

1. For the **AWS CLI v2** setup, complete the instructions listed in the following link:

   https://docs.aws.amazon.com/cli/latest/userguide/getting-started-version.html
2. Repeat the process on each Logger from which you want to migrate data.

Downloading the Archive Migration Tool

The Archive Migration Tool will allow you to copy archived data from your Loggers into ArcSight SaaS. The tool is stored in an S3 bucket, and you can download it by following the steps below.

To download the file, you will need your AWS IAM user and the information provided by the OpenText SaaS team.

1. Log in to the AWS S3 Console as the AWS IAM user that you created for data ingestion.
2. To download the migration tool from the S3 bucket, browse to the URL provided by the OpenText SaaS team.

   By default, the URL uses the format https://s3.console.aws.amazon.com/s3/buckets/<tenant bucket name>/logger/.

   For example: https://s3.console.aws.amazon.com/s3/buckets/222222222-ap-southeast-1-secopstn01-avro/logger/
3. Click your username, and then select Switch Roles from the user menu.

   > If you performed the Switch Roles procedure earlier and did not clear browser cache, the role to switch to appears under Role History which you can select, skip step 4 and save time.

4. Click the Switch Role button and enter the following details you receive from the OpenText SaaS team to download data ingestion component installers:

   a. Account

   b. Role

   c. (Optional) Display Name

   d. (Optional) Color
5. Click Switch Role.
6. Download the installation files for the Logger archive migration.

Installing the Archive Migration Tool in Each Logger

The **Archive Migration Tool** is a command-line interface designed to help you manage the migration of the metadata and Archive Catalog files from Logger to an Amazon S3 bucket. Note that after the files have been successfully copied to the S3 bucket, you can log in to ArcSight SaaS and import their associated event data. Before allowing the event migration to proceed, the Archive Migration Tool verifies that the AWS CLI has been installed.

1. Log in to the Logger server as the Logger installation user. We do not recommending using a root user.
2. Place the `logger-archive-catalog-tool-20230815.enc` file, which you obtained previously, into a directory accessible to the Logger.
3. In Logger, go to System Admin > System > License and Update
4. Select Browse.
5. Select the `logger-archive-catalog-tool-20230815.enc` file from its folder.

6. To load the file, select Upload Update.

> If you're using Logger version 7.2.1, the system might display an error message after the **Upload Update** process. If this happens, log out and then log back in. The system will process the update file properly.

Navigating in the Archive Migration Tool

To navigate the tool's menu, and any of the subsequent ones, use the following command keys:

Command	Key
Check or uncheck an option	x space
Check all	a
Uncheck all	A
Go up	k up arrow
Go back	b left arrow
Go down	j down arrow
Go to the end	G end key
Go to the start	g home
Confirm the selection	o enter right

Copying Logger Data to ArcSight SaaS

You must run the Archive Migration Tool on each Logger from which you want to copy data to ArcSight SaaS. The first time the tool runs, you will be prompted to configure the Amazon S3 bucket that stores the copied Logger Data. Note that you can reconfigure the bucket at any time after that initial configuration.

After the bucket has been configured, select the Logger archives that you want to copy to ArcSight SaaS. You can configure the tool to schedule the copy of Logger Data to the Amazon S3 bucket at specific times, instead of running it manually. The tool copies the files pertaining to the selected archives to the Amazon S3 bucket.

Once the copy process is completed, an `Archive Catalog` file is generated. This file contains metadata information about the archives that have been copied so far, plus additional information about Logger, such as its storage groups and their retention.

The `Archive Catalog` file is copied to the Amazon S3 bucket in a folder named:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_Dots/
```

The copied Logger archives' files will be available in folders such as:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_
Dots/Storage_Group_ID/YearMonthDay/
```

Every time the tool runs, and new Logger data is copied to ArcSight SaaS, the `Archive Catalog` file will be updated to include the information about the newly copied data.

> If the Logger event ingestion was not turned off before running the tool, you might have some new events that will need to be copied. Archive the new events and run the Archive Migration tool to copy them.

The Logger process needs to be up and running for Phase 1 of copying Logger Data to ArcSight SaaS. Once all the Logger archives' data has been copied, and the connectors have been switched to send events to ArcSight SaaS, you can choose to shutdown the Logger process.

Running the Archive Migration Tool

When you run the Archive Migration Tool, you can choose to copy the Logger data immediately, or schedule a time for it. The first time that you run this tool, you will be prompted to configure the Amazon S3 bucket.

1. Log in to the Logger server as the Logger installation user. We do not recommending using a root user.
2. Go to the *<LOGGER_INSTALLATION_PATH>*`/updates/logger-archive-catalog-tool` directory

   where:

   <LOGGER_INSTALLATION_PATH> represents the path where your Logger is installed. This parameter is required.
3. To execute the `loggerToReconArchiveCatalog.sh` script, run the following command:

```
./loggerToReconArchiveCatalog.sh -i <LOGGER_INSTALLATION_PATH>
```

If any errors occur during this process, the Archive Migration Tool will print messages on the screen to make you aware of them.

To review the execution log, look for the `logger_to_recon_archive_catalog_${loggerIPNoDots}.log` file, saved under the same path where the script is.

> During execution, the **loggerToReconArchiveCatalog.sh** script will print error messages only. To view more on-screen detail, activate the verbose mode by adding the `-v` parameter when executing the script.

4. (Conditional) The first time that you run this tool, follow the prompts to configure the Amazon S3 bucket.
5. (Optional) To browse the available files in the Logger, see "Viewing the Archives Contained in a Logger" on page 54.
6. (Conditional) To begin Phase One of the data migration, complete either of the following actions:
   - "Copy Logger Data to SaaS " on page 47
   - "Schedule the Copy of Logger Data to Arcsight SaaS" on page 51
7. Repeat the steps above for each Logger from which you want to migrate event data.

Configuring the AWS S3 Bucket for the First Time

The first time that you run the Archive Migration Tool, the system will prompt you to configure the Amazon S3 bucket to support the data migration.

1. Select Manage S3 Bucket from the initial menu:

```
What do you want to do?

[ x ] Manage S3 Bucket

[ ] Archives Available

[ ] Logger Information

[ ] Generator ID

[ ] Exit
```

2. To configure the bucket, select Yes:

   ```
   The S3 Bucket is not configured yet. Do you want to add an S3 Bucket?
   ```

   ```
   [ x ] Yes
   ```

   ```
   [ ] No
   ```

3. Specify values for the following prompts:

   ```
   Enter the Alias:
   ```

   ```
   Enter the Tenant ID:
   ```

   ```
   Enter the Access Key:
   ```

   ```
   Enter the Security Access Key
   ```

   Where:

   ALIAS

   Required

   Specifies the alias name that ArcSight SaaS uses to identify the Logger. The default value is `Logger_IP_Without_Dots`.

   The system transforms the IP address from the dotted-decimal format (four 8-bit fields separated by periods) to a 12-digit number. If any of the 8-bit fields of the IP has less than 3 digits, the system will complete the field adding a 0 before it.

   For example, for 15.214.134.2, the value would be 015214134002.

   TENANT ID

   Required on first use and when reconfiguring the bucket

   Represents the Amazon S3 Tenant ID.

   This value is the same as the `<your_tenant_name>` value mentioned in "Providing the User ARN to the OpenText SaaS Team" on page 29.

   ACCESS KEY

   The Amazon S3 bucket `Access Key ID` from your IAM user, mentioned in "Understanding the AWS IAM User" on page 28. This parameter is only mandatory the first time the tool is used, or whenever modifications to buckets are needed.

SECURITY ACCESS KEY

The Amazon S3 bucket `Secret Access Key` from your IAM user, mentioned in "Understanding the AWS IAM User" on page 28. This parameter is only mandatory the first time the tool is used, or whenever modifications are needed.

> ✓ You obtain the bucket's **Tenant ID**, **Access Key** and **Security Access Key** when you perform the "Preparing for Data Ingestion" on page 28 process.

4. Press Enter for the configuration to be checked.

   If the setup is finalized correctly, you will see the following message:

   ```
   Successful configuration!
   ```

5. (Optional) To browse the available files in the Logger, see "Viewing the Archives Contained in a Logger" on page 54.
6. (Optional) To immediately copy available metadata for the current Logger, see "Copy Logger Data to SaaS " below.
7. (Optional) To copy the metadata at a later time, see "Schedule the Copy of Logger Data to Arcsight SaaS" on page 51.

Copy Logger Data to SaaS

This process copies the data files and corresponding metadata for the selected archives to the Amazon S3 bucket.

1. Perform Steps 1–3 of the "Running the Archive Migration Tool" on page 44 procedure.
2. Select Archives Available from the initial menu:

   ```
   What do you want to do?

   [ ] Manage S3 Bucket

   [ x ] Archives Available

   [ ] Logger Information

   [ ] Generator ID

   [ ] Generate Catalog
   ```

```
[ ] Exit
```

3. Select one or several of the Storage groups listed at the top of the menu.
4. Select Copy.

   For example:

   ```
   [ x ] Internal Event Storage Group (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb)
   ```

   ```
   What do you want to do?
   ```

   ```
   [ x ] Copy
   ```

   ```
   [ ] Schedule
   ```

   ```
   [ ] More details
   ```

   ```
   [ ] Back
   ```

5. (Conditional) To choose archives from specific years, months or days, select More details.

   For more information about the levels of granularity to choose files from specific dates, see "Viewing the Archives Contained in a Logger" on page 54.

   > **Note:** If the **Generator ID** has not been configured, and it's not enabled by default in Logger, checking an option from the **More Details** menu will produce the following prompt:
   >
   > ```
   > To activate the migration process, check the Generator ID
   > ```
   >
   > To configure the option, which is required to initiate migrations, you must go back to the main menu, as detailed in "Adding a Unique ID to Migrated Events" on page 56.

6. After you select the archives and Copy, the system executes several verification steps to assess the availability and completeness of the archives to be migrated:

   - First, the existence and accessibility of the given path is verified. If either of these things cannot be verified, the tool will mark the “migration_status” as failed, and the “archive_status” as Not Accessed, and that archive will not be included in the **Archive Catalog**.
   - If the previous step completes successfully, the size and checksum of the files accessed inside the path is calculated (only for files with .xml, .csv and .dat extensions). The size

and checksum values are then attached to the **Archive Catalog**.

> **Note**: Be aware that the global process of calculating the size and checksum for each file will take time, depending on size and file number.

- Lastly, the system verifies the completeness of the archive. The archive size will indicate the number of datafiles (each 1 GB in size) that it should contain; an archive must have the same number of .csv and datafiles, and just one xml, so the tool would expect that if the archive size is x, the number of files contained in it will be 2x+1.

  If the above does not add up, the "archive_status" will be marked as Incomplete and this will be documented in the **Archive Catalog** as well.

If any errors occur during this process, the Archive Migration Tool will print messages on the screen to make you aware of them.

To review the execution log, look for the `logger_to_recon_archive_catalog_${loggerIPNoDots}.log` file, saved under the same path where the script is.

> During execution, the **loggerToReconArchiveCatalog.sh** script will print error messages only. To view more on-screen detail, activate the verbose mode by adding the `-v` parameter when executing the script.

Once the copy process is completed, an `Archive Catalog` file is generated. This file contains metadata information about the archives that have been copied so far, plus additional information about Logger, such as its storage groups and their retention.

The `Archive Catalog` file is copied to the Amazon S3 bucket in a folder named:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_Dots/
```

The copied Logger archives' files will be available in folders such as:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_Dots/Storage_Group_ID/YearMonthDay/
```

7. (Conditional) To migrate additional archives from the current Logger, select Yes at the prompt that displays after the previous copy process completes:

   ```
   Do you want to migrate more archives?

   [ x ] Yes

   [ ] No
   ```

   The system will take you back to the steps of the "Copy Logger Data to SaaS " on page 47 procedure.

8. If no more files will be copied, you may exit the tool.
9. Repeat this process for each Logger whose archived data you want to import.
10. (Optional) Schedule the data migration rather than copying the files right now.
11. (Optional) To repeat the copy procedure for files that have already been processed, see "Reprocessing Copied Files" below.

Reprocessing Copied Files

This process is optional.

The Archive Migration Tool will allow you to again copy files that have already been processed for migration. To identify files that have already been processed, note the **~** symbol and Done status. Files that have not been processed have an Available status. For example:

```
[] 2022 Jul 26 (Available: 1Gb)
```

```
[ ~ ] 2022 Jul 26 (Done: 1Gb)
```

Note that the system performs the re-copy process only when all selected files already have been processed for migration. If you select a mix of already-processed files and unprocessed files, only the unprocessed files will be copied when the command is executed. That is, the system perform a normal Copy procedure instead of reprocessing any already-processed files.

To reprocess a previously copied file:

1. Perform Steps 1–3 of the "Running the Archive Migration Tool" on page 44 procedure.
2. Select Archives Available from the initial menu.
3. Select the files that you want to reprocess, and then Copy.

   When you select a file marked with **~**, the tool will prompt you to confirm that want to reprocess them. For example:

   ```
   The selection has already been processed. Do you want to copy again the archives?
   ```

   ```
   [ ] Yes
   ```

   ```
   [ ] No
   ```

Once the copy process is completed, an `Archive Catalog` file is generated. This file contains metadata information about the archives that have been copied so far, plus additional information about Logger, such as its storage groups and their retention.

The `Archive Catalog` file is copied to the Amazon S3 bucket in a folder named:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_Dots/
```

The copied Logger archives' files will be available in folders such as:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_
Dots/Storage_Group_ID/YearMonthDay/
```

Schedule the Copy of Logger Data to Arcsight SaaS

This process is optional.

Rather than manually copying the metadata to the S3 bucket, you can schedule the Archive Migration Tool to copy the data.

1. Perform Steps 1–3 of the "Running the Archive Migration Tool" on page 44 procedure.
2. Select Archives Available from the initial menu:

   ```
   What do you want to do?

   [ ] Manage S3 Bucket

   [ x ] Archives Available

   [ ] Logger Information

   [ ] Generator ID

   [ ] Generate Catalog

   [ ] Exit
   ```

3. Select one or several of the Storage groups listed at the top of the menu.
4. Select Schedule.

   For example:

   ```
   [ x ] Internal Event Storage Group (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb)
   ```

```
What do you want to do?
```

```
[ ] Copy
```

```
[ x ] Schedule
```

```
[ ] More details
```

```
[ ] Back
```

5. (Conditional) To choose archives from specific years, months or days, select More details.

> **Note:** If the **Generator ID** has not been configured, and it's not enabled by default in Logger, checking an option from the **More Details** menu will produce the following prompt:
>
> ```
> To activate the migration process, check the Generator ID
> ```
>
> To configure the option, which is required to initiate migrations, you must go back to the main menu, as detailed in "Adding a Unique ID to Migrated Events" on page 56.

6. After choosing the archives that you want to schedule for copying, specify when to import the metadata:

```
Enter the schedule hour:
```

```
Enter the schedule timeout:
```

where:

schedule hour

Represents the hour of the day in a `00` to 23 format when you want to start the migration. For example, specify a time when the traffic is slower or resources are freer.

schedule timeout

Represents the maximum time in minutes during which the job can be run. You must specify a value smaller than 1440 (a full day). The following considerations apply:

- The schedule timeout value includes the time required to validate, calculate size and checksum, etc.

- If the job does not finish within the allotted timeout, it will resume the next day at the same time and for the same duration. The process starts from the point where it left off the previous day.
- If you schedule another copy to occur while an existing scheduled copy hasn't finished processing archives, the tool will not ask for a new schedule hour or schedule timeout parameters. Instead, the system will continue using the same settings for the existing scheduled copy.
- The system executes scheduled copies in the background.

If any errors occur during this process, the Archive Migration Tool will print messages on the screen to make you aware of them.

To review the execution log, look for the `logger_to_recon_archive_catalog_${loggerIPNoDots}.log` file, saved under the same path where the script is.

> During execution, the **loggerToReconArchiveCatalog.sh** script will print error messages only. To view more on-screen detail, activate the verbose mode by adding the -v parameter when executing the script.

Once the copy process is completed, an `Archive Catalog` file is generated. This file contains metadata information about the archives that have been copied so far, plus additional information about Logger, such as its storage groups and their retention.

The `Archive Catalog` file is copied to the Amazon S3 bucket in a folder named:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_Dots/
```

The copied Logger archives' files will be available in folders such as:

```
Bucket_Name/event-sync/logger-archives/Tenant_ID/Logger_IP_Without_Dots/Storage_Group_ID/YearMonthDay/
```

7. (Conditional) Repeat this process for each Logger whose archived data you want to schedule for migration.
8. If no more files will be scheduled, exit the tool.

Removing a Logger after All Its Data Is Copied to ArcSight SaaS

This process is optional.

In Phase One of the migration process, you copied the data of a Logger to the ArcSight SaaS S3 bucket. Once you have successfully completed this phase, you have the option to remove or repurpose that particular Logger because the next phase does not require the Logger. In Phase Two, you import the archived event data to the ArcSight Database.

1. To ensure that the Logger no longer receives events, reconfigure the SmartConnectors to send events to the ArcSight SaaS environment:

- Configure standalone SmartConnectors

2. Log in to ArcSight.

   For example, https://<your_tenant_name>.mp.cyberresprod.com

   Note that your login role must have the *Logger Data Migration* permission.

3. Select Configuration > Import Logger Data > Data Import.
4. Verify that all archives are listed and thus ready for import to the ArcSight Database as part of Phase Two.

   We recommend that you check the listed archives to ensure that you have copied all desired metadata from each Logger.

5. Shut down the Logger process.

   You can now repurpose the Logger host system.

Understanding the Archive Migration Tool

Beyond copying Logger Data to ArcSight SaaS, you can use the Archive Migration Tool for the following purposes:

Viewing the Archives Contained in a Logger

Before migrating data to the ArcSight Database, you might want to gauge the size of the data within a Logger, which might help you set priorities for executing or scheduling copies. In the Archive Migration Tool, you can view the summary of archives contained within the current Logger, as well as the migration status of the archive. Even when no AWS S3 bucket has been configured for the data migration, you can still use this method to check the archives.

> **Note:** If the **Generator ID** has not been configured, and it's not enabled by default in Logger, checking an option from the **More Details** menu will produce the following prompt:
>
> ```
> To activate the migration process, check the Generator ID
> ```
>
> To configure the option, which is required to initiate migrations, you must go back to the main menu, as detailed in "Adding a Unique ID to Migrated Events" on page 56.

1. Perform Steps 1–3 of the "Running the Archive Migration Tool" on page 44 procedure.
2. Select Archives Available from the initial menu:

   ```
   What do you want to do?
   ```

```
[ ] Manage S3 Bucket

[ x ] Archives Available

[ ] Logger Information

[ ] Generator ID

[ ] Generate Catalog

[ ] Exit
```

3. Select More details.

   For example:

```
[ x ] Internal Event Storage Group (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb)

What do you want to do?

[ ] Copy

[ ] Schedule

[ x ] More details

[ ] Back
```

4. Select the archive that you want to view.

   As you select items, the system progressively reveals further levels of detail. At every level except the last, you can select Yes to obtain further details. For example:

Level	Filtered by	Example
1	Storage group	[ ] Internal Event Storage Group (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb)
2	Year	[ ] 2021 (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb) [ ] 2022 (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb)
3	Month	[ ] 2021 Jul (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb) [ ] 2022 Jan (Total: xGb, Ava: xGb, Pen: xGb, Done: xGb, Fail: xGb)
4	Day	[ ] 2022 Jul 26 (Available: xGb)

where:

- **Total** represents the total data size in gigabytes
- **Ava** represents the available data to migrate in gigabytes
- **Pen** represents the data pending to migrate in gigabytes
- **Done** represents the data already migrated in gigabytes
- **Fail** represents the failed data migration in gigabytes

Adding a Unique ID to Migrated Events

To help you identify an imported event that might be seen by multiple ArcSight components, SmartConnectors can assign a unique 64-bit ID to each event. You can use this globalEventID (GEID) in search queries and view the GEID in an event’s details. This feature is enabled by default in Logger. However, in the case that imported events do not already have a GEID, use the Archive Migration Tool to generate IDs.

For more information about using Logger to generate the ID, see the *Administrator's Guide to ArcSight Logger*.

1. Perform Steps 1–3 of the "Running the Archive Migration Tool" on page 44 procedure.
2. Select Generator ID in the initial menu:

```
What do you want to do?

[ ] Manage S3 Bucket

[ ] Archives Available

[ ] Logger Information
[ x ] Generator ID

[ ] Generate Catalog

[ ] Exit
```

3. Depending on whether the Generator ID has already been assigned a value, the next menu will show one of the next two possible options:
   - If the Generator ID has no value assigned, the Archive Migration Tool will ask for a value to be set for it:

     ```
     Enter the Generator ID: your_value
     ```

     where `your_value` must be a number between 1 and 16383 to be accepted.
   - If the Generator ID was previously configured in Logger, the default selection (Receiver Process) will be displayed:

     ```
     Generator ID [14]

     Do you want to modify the Generator ID?

     [ x ] Yes

     [ ] No
     ```

     Select Yes to bring up a menu that allows you to change the Generator ID to a specific set value or your own choice:

     ```
     Select the Generator ID

     [ ] Aps [ 13 ]

     [ ] Servers [ 12 ]

     [ x ] Receivers [ 14 ]
     ```

```
[ ] Other Generator ID

[ ] Back
```

Regenerating an Archive Catalog

After at least one migration has been initiated, the option to regenerate an existing Archive Catalog becomes available in the Archive Migration Tool. The system includes only the archives that have already been processed in the most recent migration.

> You should regenerate a catalog only when something goes wrong during the last migration. For example, if the process for creating the Archive Catalog was interrupted.

1. Perform Steps 1–3 of the "Running the Archive Migration Tool" on page 44 procedure.
2. Select Generate Catalog in the initial menu:

```
What do you want to do?

[ ] Manage S3 Bucket

[ ] Archives Available

[ ] Logger Information

[ ] Generator ID

[ x ] Generate Catalog

[ ] Exit
```

Updating the Configuration of the AWS S3 Bucket

Follow this procedure whenever the configuration of an Amazon S3 bucket must be updated.

1. Perform Steps 1–3 of the "Running the Archive Migration Tool" on page 44 procedure.
2. Select Manage S3 Bucket in the initial menu:

```
What do you want to do?

[ x ] Manage S3 Bucket

[ ] Archives Available

[ ] Logger Information

[ ] Generator ID

[ ] Generate Catalog

[ ] Exit
```

3. When at least one bucket has been added, select Manage S3 Bucket to allow configuration changes to existing buckets:

```
The S3 Bucket alias [chosen_alias] already exists, please choose a different one. Do you
want to modify an S3 Bucket?

[ x ] Yes

[ ] No
```

4. To display the configuration options for the specified bucket, select Yes, and then enter the values to be modified, or leave them empty if you want to leave the value as is:

```
Leave empty to leave the value as is.

Enter the Tenant ID [*****]:

Enter the Access Key [*****]:

Enter the Security Access Key [******]:
```

```
Checking the S3 Bucket configuration....
```

Where:

ALIAS

Required

Specifies the alias name that ArcSight SaaS uses to identify the Logger. The default value is `Logger_IP_Without_Dots`.

The system transforms the IP address from the dotted-decimal format (four 8-bit fields separated by periods) to a 12-digit number. If any of the 8-bit fields of the IP has less than 3 digits, the system will complete the field adding a 0 before it.

For example, for 15.214.134.2, the value would be 015214134002.

TENANT ID

Required on first use and when reconfiguring the bucket

Represents the Amazon S3 Tenant ID.

This value is the same as the `<your_tenant_name>` value mentioned in "Providing the User ARN to the OpenText SaaS Team" on page 29.

ACCESS KEY

The Amazon S3 bucket `Access Key ID` from your IAM user, mentioned in "Understanding the AWS IAM User" on page 28. This parameter is only mandatory the first time the tool is used, or whenever modifications to buckets are needed.

SECURITY ACCESS KEY

The Amazon S3 bucket `Secret Access Key` from your IAM user, mentioned in "Understanding the AWS IAM User" on page 28. This parameter is only mandatory the first time the tool is used, or whenever modifications are needed.

> ✓ You obtain the bucket's **Tenant ID**, **Access Key** and **Security Access Key** when you perform the "Preparing for Data Ingestion" on page 28 process.

5. Press Enter for the configuration to be checked.

   If the setup is finalized correctly, you will see the following message:

```
Successful configuration!
```

Troubleshooting Issues in the Migration Tool

When you run the Archive Migration Tool, use the following table to resolve any errors.

Configuration Error	Message
Both the credentials and the bucket name are incorrect	Note: All fields are required. The tool will not proceed until a value is entered.
Bucket name is correct but the credentials are incorrect	Something went wrong while checking the credentials Do you want to try again? [x] Yes [ ] No
Credentials are correct but the bucket name is not	Something went wrong while checking if the bucket exists Do you want to try again? [x] Yes [ ] No
Bucket name is correct, but write permissions to the bucket directory are not granted (this happens during setup, when the tool tries to copy a file to the directory to test the permissions)	Something went wrong with the AWS command Something went wrong with the copy permission.

Archive file upload is attempted while the bucket credentials are incorrect	To activate the migration process, check the credentials in the S3 Bucket configuration Do you want to get more details? [x] Yes [ ] No
Archive file upload is attempted while the bucket name is incorrect	To activate the migration process, check the bucket name in the S3 Bucket configuration Do you want to get more details? [x] Yes [ ] No
Archive file upload is attempted while the write permission is not granted	To activate the migration process, check the copy permission in the S3 Bucket configuration Do you want to get more details? [x] Yes [ ] No

Setting Up Generator ID Management

Every event generated by an ArcSight component will have a unique Global Event ID. This will help in identifying the events in case the same event is seen in multiple ArcSight components. ArcMC enables users to generate an ID and to assign it to a non-managed product. Each assigned **Generator ID** should be unique for the ArcSight environment.

- "Setting Up Generator ID Management" on the next page
- "Getting Generator ID for Non-managed Nodes" on the next page
- " Setting Generator IDs on Managed Nodes" on the next page

Setting Up Generator ID Management

1. Log in to ArcMC.
2. On the top right side of the screen, click Generator ID Manager.
3. Select Yes to enable Generator ID Management in ArcMC.
4. Enter the numeric values between 1 and 16383 for the Generator ID range (**Start** and **End**) .
5. Click Save. ArcMC will set the generator ids for itself if not set already.
6. Restart all ArcMC processes to continue.

Getting Generator ID for Non-managed Nodes

1. Log in to ArcMC.
2. Select Configuration Management > Generator ID Management.
3. Click Assign a Generator ID.
4. Select the **Event Producer Type**. Other fields are optional.
5. Click Assign.
6. To copy the ID, click the copy to clipboard icon.
7. Click OK. The system displays a list of generated IDs.

Setting Generator IDs on Managed Nodes

If ArcMC is enabled as a Generator ID Manager, ArcMC will automatically set the generator IDs for each managed node when performing the following actions:

Connectors

- Adding a Host version 7.11 or later
- Scanning a Host
- Adding a Connector to a Container
- Connector upgrade to version 7.11 or later
- Instant Deployment

> **Note:** Multiple host deployment is disabled when the Generator ID Manager flag is enabled.

Logger

- Remote Upgrade: Upgrade from and to Logger version 6.7 or later.
- Adding a Host version 6.7 or later.

ArcMC

- Remote Upgrade: Upgrade from and to ArcMC version 2.9 or later
- Adding a Host version 2.9 or later
- Scanning a Host
- Setting the Generator IDs on localhost by enabling the Generator ID Manager

Setting Up the Real-time Threat Detection Console

The Real-time Threat Detection Console is a workstation-based interface intended for use by your full-time security staff in a Security Operations Center or similar security-monitoring environment. It is the authoring tool for rules, Threat Detector, dashboards, and data monitors. It is also the interface for administering users and workflow.

Depending on your role in the security operations center and the permissions you have, you can do anything in the ArcSight Console from routine monitoring to building complex correlation and long sequence rules, to performing routine administrative functions.

For information about using the console, see the User's Guide for the Real-time Threat Detection Console.

Note: The console is pre-configured to use FIPS 140-2 mode and OSP client authentication.

Installation Considerations for the Real-time Threat Detection Console

Review the following considerations before you install the console so that you can choose the options that best suit your needs:

- Single versus multiple users
- Character sets
- Linux computers
- Macintosh computers

Single versus Multiple Users

Single user:

- There is only one system account on this computer that one or more users will use to connect to the console. For example, a system account, `admin`, is used by console users Joe, Jack, Jill, and Jane.

  OR

- All users who will use this computer to connect to the console have their own user accounts on this computer AND these users have write permission to the console’s `\current` directory.

Advantage: Logs for all console users are written to one central location in the `\current\logs` directory. The user preferences files (denoted by `username.ast`) for all console users are located centrally in the `\current` directory.

Disadvantage: You cannot use this option if your security policy does not allow all console users to share a single system user account or all users to write to the `\current` directory.

Multiple users:

- With this option, each user’s log and preferences files are written to the user’s local directory (for example, `Documents and Settings\`*`username`*`\.arcsight\console` on Windows) on this computer.

  Advantage: You do not have to enable write permission for all console users to the `\current` directory.

  Disadvantages: Logs are distributed. Therefore, to view logs for a specific time period, you will have to access them from the local directory of the user who was connected at that time.

  If you do not enable write permission for all users to the `\current` directory, users can only run the following commands (found in the `\bin\scripts` directory) from the command-line interface:

  - `console`
  - `exceptions`
  - `portinfo`
  - `websearch`
- All users who use this computer to connect to the console have their own user accounts on this computer and these users do not have write permission to the `\current\logs` directory.
- All other commands require write permission to the `\current` directory.

> **Note:** The location from which the console accesses user preference files and to which it writes logs depends on the option you select above. Therefore, if you switch between these options after the initial configuration, any customized user preferences might appear to be lost. For example, the console is currently configured with the “This is a single system user installation” option on a Windows computer. Console user Joe’s customized preferences file is located in the console’s `<ARCSIGHT_HOME>\current` directory. Now, you run the `consolesetup` command and change the setting to ‘Multiple system users will use this installation.’ The next time the user Joe connects to the console, the console will access Joe’s preference file from `Documents and Settings\joe\.arcsight\console`, which will contain the default preferences.

Character Sets

Install the console on a computer that uses the same character set encoding as the Manager. If the character encodings do not match, then user IDs and passwords are restricted to using the following characters:

```
a-z A-Z 0-9_@.#$%^&*+?<>{}|,()-[]
```

Linux Computers

Do not attempt to install the console as the `root` user. If you do, the installer prompts you to change ownership of certain directories after the installation completes, so OpenText recommends performing the installation as a non-root user.

Macintosh Computers

Before you start the console, set up a default printer. if you open a channel, select some rows, right-click and select **Print Selected Rows**, the console will stop unexpectedly if a default printer is not set up.

Downloading the Console Installers

OpenText stores the installation files for the Real-time Threat Detection Console in the Amazon S3 bucket for ArcSight. To download the files, you will need your AWS IAM user and the information provided by the OpenText SaaS team.

To validate the downloaded files, also download their associated signature files (.sig). OpenText provides a digital public key that is used to verify that the software you downloaded from the Amazon S3 bucket is indeed from OpenText and has not been tampered with by a third party. For more information and instructions on validating the downloaded software, visit the OpenText Code Signing site. If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please do not run the downloaded files again but contact OpenText SaaS Customer Success Support.

1. Log in to the Amazon S3 Console as the AWS IAM user that you created.
2. To download the console installer for your operating system from the S3 bucket, browse to the URL provided by the OpenText SaaS team.

   By default, the URL uses the format https://s3.console.aws.amazon.com/s3/buckets/<bucket name>.

3. Click your username, and then select Switch Roles from the user menu.
4. Click Switch Role and enter the following details you receive from the OpenText SaaS team:
    a. Account
    b. Role
    c. (Optional) Display Name
    d. (Optional) Color
5. Click Switch Role.
6. Download the file for your operating system.

Installing the Real-time Threat Detection Console

For best results, install the console on an operating system that is set to the same locale as the automatically-installed Manager so that during startup, the console and the Manager automatically detect and use the locale from the operating system.

1. Run the self-extracting archive file that is appropriate for your target platform.
2. Click **Next** in the **Installation Process Check** screen. Follow the prompts until you reach **Choose ArcSight installation directory**.
3. Accept the default installation directory, click **Choose** to navigate to an existing folder, or type the path where you want to install the console. If you specify a folder that does not exist, the installation program creates it.

    > ⚠ **Caution:** Do not use spaces in installation paths. The installation program will not display an error message, but the console will not start.

4. Select the location to create a shortcut for the console and uninstall icons and click **Next**.
5. View the summary and click **Install** if you are satisfied with the paths listed.

    > **Note:** On Windows, when the installation program is configuring the console (the **Please Wait** panel), you might see a message that the TZData update was not successful. If you get that message, click **OK** and continue. The console installs successfully. Usually, TZData is correctly updated regardless of this message. To make sure, check that the timestamp on the files in the `<ARCSIGHT_HOME>\current\jre\lib\tzdb.dat` directory matches the date and time when you installed the console. If the timestamp is old or the files are missing, uninstall and then re-install the console.

6. (Optional) Review the log files for the installation:

Platform	Log file location
Linux	`/home/<user>`
Windows	`C:\Users\<user>`
Macintosh	`/Users/<user>`

Configuring the Real-time Threat Detection Console

After you install the console, you will need to configure it.

> **Note:** The console is pre-configured to use FIPS 140-2 mode and OSP client authentication.

1. In the **Manager Host Name** field, enter the host name or IP address that OpenText provided when you received your ArcSight SIEM as a Service account.
2. Select the **Use direct connection** option.

   You can set up a proxy server and connect to the Manager using that server if you cannot connect to the Manager directly. If you select the **Use proxy server** option, you will be prompted to enter the **Proxy Host Name** and **Proxy Host**. Enter the proxy host name.
3. The configuration wizard prompts you to specify the default web browser you want to use to display web page content. Specify the location of the executable for the web browser.
4. Select whether a single user or multiple users will use this installation of the console.
5. If you are installing the console on a Linux machine, add the following line to `/home/arcsight/.bash_profile`:

   ```
   export LANG=[language].UTF-8
   ```

   where [language] is one of the following:

   en_US (English)

   zh_CN (Simplified Chinese)

   zh_TW (Traditional Chinese)

   ja_JP (Japanese)

   fr_FR (French)

   ko_KR (Korean)

Reconciling Users With Fusion User Management

You must add all users that were created in Fusion to the Real-time Threat Detection Console before the user can access the console or the Real-time Threat Detection Command Center.

When you create users in Real-time Threat Detection, both the user name and External ID in Real-time Threat Detection should match the email address of the user in Fusion User Management. The authentication process for a user matches the email address provided to Fusion User Management with the External ID that you provide for that user within Real-time Threat Detection.

Starting the Real-time Threat Detection Console

After installation and setup is complete:

1. Start the console using the shortcuts installed or open a command window on the console's `bin` directory and run:

   On Windows:

   ```
   arcsight console
   ```

   On Unix:

   ```
   ./arcsight console
   ```

2. Click **OSP Client Login**.

   When you start the console for the first time, you are asked whether you want to trust the Manager's certificate. The prompt will show details specific to your settings.

3. Click **OK** to trust the Manager's certificate.

   The certificate will be permanently stored in the Console's truststore and you will not see the prompt again the next time you log in.

Uninstalling the Real-time Threat Detection Console

Before uninstalling the console, exit the current session.

Uninstalling on Windows

Run the **Start > All Programs > ArcSight Detect 8.1.x.x Console > Uninstall_ArcSight Detect Console_8.1.x.x** program. If a shortcut to the console was not installed on the Start menu, locate the console's `UninstallerData` folder and run:

```
Uninstall ArcSight Detect Console Installation.exe
```

Uninstalling on Unix

Run the uninstaller program from either the directory where you created the links while installing the console, or if you opted not to create links, then run this from the

`/opt/arcsight/console/current/UninstallerData` directory:

```
./"Uninstall ArcSight Detect Console Installation"
```

Alternatively, you can run one of the commands below from `/home/arcsight` (or wherever you installed the shortcut links) directory.

```
./"Uninstall_ArcSight_Detect_Console_8.1.x.x"
```

or

```
./Uninstall\ Uninstall ArcSight Detect Console Installation
```

Note: The `UninstallerData` directory contains a file `.com.zerog.registry.xml` with Read, Write, and Execute permissions for all users. On Windows hosts. These permissions are required for the uninstaller to work. However, on UNIX hosts, you can change the permissions to Read and Write for everyone (that is, 666).

Managing and Maintaining ArcSight

This chapter provides guidance for the long-term management of user accounts and the data ingestion components.

Managing User Accounts

This section provides a guidance on how to set up and manage your account in the long-term.

Creating Additional User Accounts

In ArcSight, the Tenant Administrator can create additional user accounts, then assign them roles and groups. The email ID specified for each user becomes their login username.

1. Log in to ArcSight with your ArcSight Tenant Administrator account.

   For example, https://<your_tenant_name>.mp.cyberresprod.com
2. Select ADMIN > Account Groups > Create User.

   > For more information about creating users; assigning roles; and using the Default Roles, see the *User's Guide for ArcSight SIEM as Service* or click Help.
3. Inform users that you created their accounts so they can log in to ArcSight.
4. After the user logs in and navigates to SOAR for the first time, revoke the Super User role.

   > This is a one time configuration and once the Super User role is revoked, the new user is automatically assigned to the Empty Role.
5. Repeat the steps above to create additional users, assign roles, set up credentials, and use ArcSight.
6. If Real-time Threat Detection is part of the ArcSight environment, reconcile users with Fusion User Management.

First-time Login for New Users

We recommend that you provide the following instructions when informing users of their new ArcSight account.

Each user can choose to set up their preferred authentication method when they log in for the first time. However, if multi-factor authentication is enabled for your account you must set up a login password before the first login. The following steps show how to configure the authentication service to use the Password method for verifying your credentials. You can continue using the OTP code method, if preferred, or use it as a backup method in case you lose your password.

Before you choose an authentication method, the default method configured for your account is Email One-Time Password (OTP), which sends an (OTP) code to your specified email address. When you log in, you are prompted to Select Authentication Chain which relates to the method you choose to use for that login session.

By default, your username is the email address provided to you by your ArcSight administrator.

Logging into ArcSight SaaS the First Time

By default your account does not have a password to log in. You will be prompted for an Email OTP code.

1. In a browser, enter the link provided by your ArcSight administrator.

   https://<your_tenant_name>.mp.cyberresprod.com

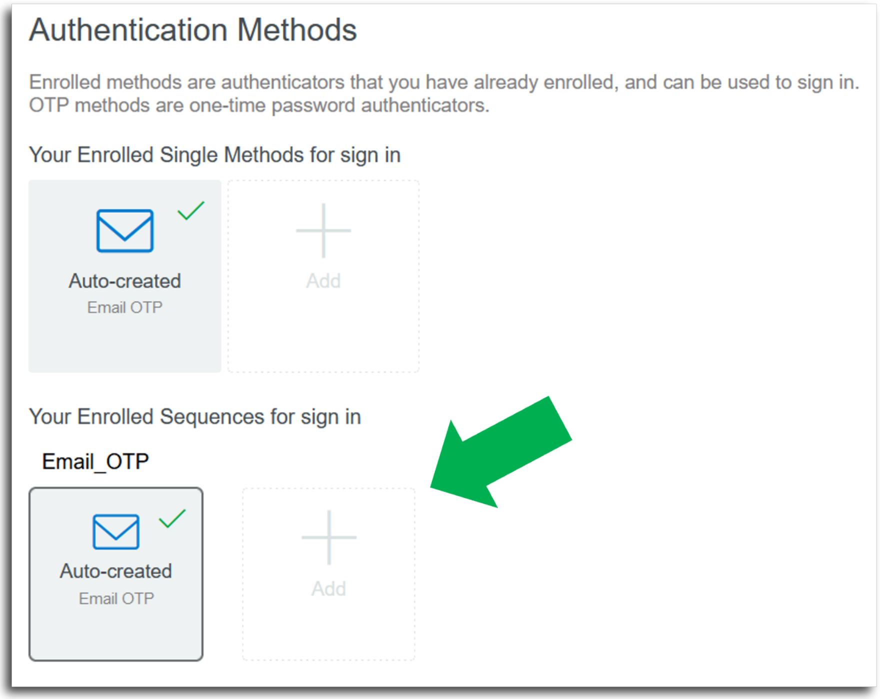
   For example, `https://extremelyfocused.mp.cyberresprod.com`
2. Enter your username, then click Next.
3. Check your email for a one-time password code sent by the authentication service.
4. Enter the OTP sent to your email address, then click Next.
5. You can begin using the features in ArcSight.
6. (Optional) To use the password method to log in, change your authentication method.

Choosing the Password Method to Log In

If you want to use a password to log in, specify the Password method for authenticating your account.

1. Log in to the Advanced Authentication service.
2. Check your email for a one-time password (OTP) code sent by the authentication service.
3. Enter the OTP sent to the email address for your ArcSight Tenant Administrator account, then click Next.
4. Under Your Enrolled Sequences for sign in on the Authentication Methods page, click +Add.

Figure 1*. The green arrow indicates the appropriate +Add option that you should select*



Authentication Methods

Enrolled methods are authenticators that you have already enrolled, and can be used to sign in. OTP methods are one-time password authenticators.

Your Enrolled Single Methods for sign in

Your Enrolled Sequences for sign in

Email_OTP

5. Click the Password option.
6. Specify the password that you want to use for your ArcSight account, then click Finish.
7. Sign out of the Advanced Authentication service.
8. After successfully creating your password, you can now log in to ArcSight with your password instead of with an Email OTP code.

   Use the link provided by your ArcSight administrator. For example, https://<your_tenant_name>.mp.cyberresprod.com

Logging in the First Time with Multi-Factor Authentication

If multi-factor authentication is enabled, you must add a password as an enrolled method to log in before the first login.

1. Follow the steps in section Choosing the Password Method to Log In to set up a password.
2. Log in to Arcsight using the link provided by your ArcSight administrator.

Logging in to the Advanced Authentication Service

To modify your authentication method, log in to the Advanced Authentication service as a user.

1. Browse to the Advanced Authentication service as a user:
   http://<tenant-name>.cyberresprod.com

For example:
https://extremelyfocused.cyberresprod.com

2. For your username, enter the following information:

   <tenant name>\secops_localusers\<email address>

   For example: extremelyfocused\secops_localusers\sam.landry@extremelyfocused.com

Resetting Passwords Manually

Users can change their password in the Self-service portal of Advanced Authentication. The process assumes that you have configured the authentication service to use the Password method for verifying your credentials.

1. Log in to the Advanced Authentication service.
2. Under Your Enrolled Sequences for sign in on the Authentication Methods page, click Password.
3. Specify the new password, then click Finish.
4. Sign out of the Advanced Authentication service.

Rotating Data Ingestion Credentials

For optimal security, it's a good practice to rotate the access keys for the AWS IAM user account that you created for data ingestion with resources such as the Amazon S3 bucket that have access to the account. When performing a key rotation for this user, you as the administrator must coordinate the rotation with the data ingestion configuration of SmartConnectors so that they do not lose access to the associated Amazon S3 bucket. This procedure also involves reconfiguring SmartConnectors, quite like the initial configuration.

To rotate the access key, use the rotating access keys procedure in the AWS documentation. Reconfigure all connectors to use the new access key to update all applications and tools to use the new access key as follows:

1. Start the SmartConnectors installation wizard.
2. For Type, select Amazon S3 as the destination.
3. Enter the user account that you used earlier to configure SmartConnectors.
4. Enter the your AWS access key.
5. Enter the your AWS secret key.
6. Complete the installation.

For optimal security, create a schedule for rotating credentials that best fits your organization and implement the schedule accordingly. After each rotation, ensure that you reconfigure SmartConnectors with updated access and secret key pairs.

Managing Advanced Authentication

This section provides a guidance on how to add users to the Tenant Admins role for the Advanced Authentication service, as well as manage password expiration.

- Logging In as the Advanced Authentication Tenant Administrator
- Managing Advanced Authentication Administrators
- Configuring Password Expiration

Logging In as the Advanced Authentication Tenant Administrator

You must have the Advanced Authentication Tenant Administrator credentials to perform this action.

1. Browse to the Advanced Authentication service:

   http://<tenant-name>.cyberresprod.com/admin

   For example:
   https://extremelyfocused.cyberresprod.com/admin
2. For your username, enter the following information:

   <tenant name>\<user repository>\<email address>

   Depending on the account, the user repository might be SECOPS_LOCALUSERS or LOCAL. For example:

   a. The **default administrator ID** provided by CyberRes resides in the LOCAL user repository. You would enter the username like this:

      extremelyfocused\LOCAL\sam.landry@extremelyfocused.com

   b. The user accounts that you create in ArcSight reside in the SECOPS_LOCALUSERS user repository. You would enter these usernames like this:

      extremelyfocused\SECOPS_LOCALUSERS\sam.landry@extremelyfocused.com
3. Complete any actions as needed.

Managing Advanced Authentication Administrators

You must have the Advanced Authentication Tenant Administrator credentials to perform this action.

By default, you are provided with a single user account to use as an Advanced Authentication Tenant Administrator. You might want to add or manage the set of users that are Advanced Authentication Tenant Administrators. To manage this set of users, complete the following steps:

1. Create the user account that your Advanced Authentication Tenant Administrators will use to access ArcSight.

   This step adds the new user account to the SECOPS_LOCALUSERS user repository within the Advanced Authentication service.

2. Log in to the Advanced Authentication service.
3. Navigate to Repositories > LOCAL > Global Roles > TENANT ADMINS.
4. To add the required user to the TENANT ADMINS role, enter the username in the text field using the following syntax:

   ```
   SECOPS_LOCALUSERS\<email address>
   ```

   For example:

   ```
   SECOPS_LOCALUSERS\sam.landry@extremelyfocused.com
   ```

5. Save your changes.

   Now the user can log in to the Advanced Authentication service.

Configuring Password Expiration

You must have the Advanced Authentication Tenant Administrator credentials to perform this action.

By default, passwords expire every 42 days. However, you can change the maximum password age to suit your organization’s security policies. Upon password expiry users are prompted at next login and receive a link to reset it.

For more information about managing passwords and user credentials, see Configuring Passwords in Advanced Authentication in the *Administrator’s Guide to Advanced Authentication*.

1. Log in to the Advanced Authentication service Advanced Authentication Tenant Administrator to configure password expiration.
2. Select Methods.
3. For the Password option, select ✎.
4. Configure the password options:

- Minimum password length
- Maximum password age

Upgrading a Standalone Instance of ArcMC

This section details steps to upgrade a standalone instance of ArcMC.

Upgrade Standalone ArcMC Locally

Complete the following steps to upgrade standalone ArcMC locally:

1. Download the ArcMC local installer and upgrade files.
2. Perform the procedure detailed in Upgrading ArcMC in the ArcSight Management Center help.

Upgrade Standalone ArcMC Remotely

Complete the following steps to upgrade standalone ArcMC remotely:

1. Download the ArcMC remote upgrade files.
2. Perform the procedure detailed in Upgrading ArcMC in the ArcSight Management Center help.

Upgrade Standalone SmartConnectors

To upgrade your standalone SmartConnectors, see Installing SmartConnectors in the *ArcSight SmartConnector Release Notes 8.4.0*.

To upgrade your standalone SmartConnectors, see Installing SmartConnectors in the *ArcSight SmartConnector Release Notes 8.4.1*.

Verifying Your Data and Services

In the rare occasion that your SaaS service encounters problems, the OpenText SaaS team might ask you to check the services to ensure that they're functioning appropriately and your data is available as expected. For example, if OpenText must restore your data from a backup, then the team will let you know the restoration date of the backup.

The SaaS team will recommend which of the following procedures they would like you to perform to ensure that you can access and use ArcSight's features.

Verifying that Services are Available

It’s possible that the OpenText SaaS team must restore the availability of a service. For example, the server hosting one or more services might have gone offline. After the SaaS team validates the restored services, the team might ask you to verify that the services are available to you.

Follow these procedures to verify service functionality.

1. Log in to ArcSight.
2. (Optional) To verify the Dashboard functionality, complete the following steps:
   a. Select Dashboard.
   b. Verify that the list of dashboards displays.
3. To verify the user management functionality, complete the following steps:
   a. Select Admin > Account Groups.
   b. Verify that you can access the list of users.

      If you have not previously added users to Arcsight or assigned them roles, you can follow the steps in Creating Additional User Accounts.
4. To verify the Search functionality, complete the following steps:
   a. Select Search.
   b. Check whether you can enter a query and execute a search.
   c. Select Configuration > Storage.
   d. Ensure that the page opens, and that it displays storage groups, if any have been created.
   e. Select Configuration > Outlier.
   f. Ensure that the page opens, and that it display models if any have been created.
5. To verify the Reports functionality, complete the following steps:
   a. Select REPORTS > Portal.
   b. In the new tab, select Repository.
   c. Verify that the Reports Portal opens.
6. To verify the Respond functionality, complete the following steps:
   a. Select Respond > Cases. Ensure that the Cases page is displayed.
   b. Select Dashboard and click the +button.

   c. Click the +button on the right side of the Main Context tab.
   d. Enter soar on the Widget Search screen. Ensure that a list of widgets is displayed.

7. To verify the Real-time Threat Detection functionality, complete the following steps:
   a. Navigate to Detect.
   b. Select Command Center.
   c. Navigate to Dashboards and select Cluster View.
   d. Ensure that all configured services are displayed and show as Active.

> **Note:** Disregard any messages regarding content not installed.

Verifying Data for a Service

It’s possible that the OpenText SaaS team will need to restore the ArcSight database or the configuration data for one or more services from a backup. For example, a service might have experienced data loss or corruption. After the SaaS team validates the restored data, the team might ask you to verify that the data is available as expected. They will let you know the restore point for the backup, which represents the date and time that the backup occurred. For example, the SaaS team discovers a problem with some data on the morning of June 2. They restore the affected service and its data by using the backup from May 29. Depending on the amount of time that has lapsed between the restore point (May 29) and when the SaaS team resolved the issue with the service (by 1 pm on June 2), you might lose data that had been queued to or ingested by the database. However, data sent during the restoration process (between late morning and 1 pm on June 2) might be available to you.

Follow these procedures to verify that your data has been returned to the restore point and possibly includes data queued during service restoration. The SaaS team might tell you which steps to perform or functions to verify.

Verify the Restored Database

If the SaaS team must restore the ArcSight Database, they will ask you to validate that your data has been returned up to the time of the restore point. You can also verify the time when the database began loading queued data after the restoration. Complete the following steps.

1. Select Search.
2. To confirm that the database contains data received up to the restore point, create a query with a custom time range where Start Time is an hour before and End Time is an hour after the restore point.

3. To confirm that the database contains data queued during the service restoration, create a query with a Custom Time range where Start Time is an hour before and End Time is an hour after the time when the SaaS team stopped the database service for the restoration process.
4. To confirm that the database contains data queued or received after the service restoration, create a query with a Custom Time range where Start Time is an hour before the SaaS team stopped the database service for the restoration process and End Time is the current time.
5. Repeat Step 4 until you no longer see additional events added for the time range.

   If the database service was stopped for a significant amount of time, the ingest queue might contain a significant amount of data. Thus, it might take a while to load the queued data into database. You can repeat this search to determine when the loading of the backlog of events is complete and matches what you would expect.
6. Select Configuration > Lookup Lists.
7. Check whether each lookup list includes the appropriate content.
8. (Conditional) If your organization had made changes to the lookup lists after the restore point, update the lists.
9. Select Configuration > Storage.
10. Verify that the list includes all storage groups that existed before the restore point.
11. Check the settings for each storage group.
12. (Conditional) If your organization had made changes to the storage groups after the restore point, update the groups.
13. To verify data used by Outlier Analytics, complete the following steps:
    a. Select Configuration > Outlier.
    b. Create, build, and score a model.

       For example, create a query such as sourceAddress in subnet 10.1.1.0/24.
    c. Select Insights > Outlier to verify that the model successfully scores.

Verify Data for User Management Functions

To validate the data for user management functions, complete the following steps. Note that user credentials and configuration settings stored by the Advanced Authentication service will not be affected by restoration of the user management data.

1. Log in to ArcSight.
2. Select Admin > Account Groups.

3. Ensure that the list of user groups reflects all groups added, deleted, or modified before the restore point and any changes that might have been queued during the restoration.
4. Select each account group.
5. For each group of users, ensure that the group includes all users that were added, deleted, or modified before the restore point.
6. Select Roles.
7. Verify that the list of roles reflects all roles added or deleted before the restore point.
8. For each role, ensure that the permissions match the state of the role before the restore point.
9. Check whether each role includes the users that were assigned to that role before the restore point.

Verify Data for User Configuration

To validate the data required for user configuration settings, complete the following steps.

1. Log in to ArcSight.
2. Select Dashboard.
3. Verify that the list includes the dashboards and their configuration available before the restore point.
4. Select Search.
5. Verify that the saved and scheduled searches reflect their state from the restore point.
6. (Conditional) If your organization had made changes to the search functions after the restore point, update the saved and scheduled searches as needed.
7. Select Configuration > Lookup Lists.
8. Verify that the feature includes all lookup lists that existed before the restore point.
9. (Conditional) If your organization had made changes to the lookup lists after the restore point, update the lists.
10. (Conditional) Select Configuration > Outlier.
11. Verify that Outlier Analytics includes all model configurations that existed before the restore point.
12. (Conditional) If your organization had made changes to the outlier models after the restore point, add or modify the models.

Verify Data in the Reports Portal

To validate your custom reports and dashboards in the Reports Portal, complete the following steps.

1. Log in to ArcSight.
2. Select REPORTS > Portal.

   The portal opens in a new browser tab.
3. Select Repository.
4. Verify that the repository includes all custom reports and dashboards that existed before the restore point.
5. (Conditional) If your organization had made changes to the repository after the restore point, add, delete, or modify the custom dashboards and reports.

Verify Data for Real-time Threat Detection

To validate the data in the Real-time Threat Detection application, complete the following steps:

1. Log in to ArcSight.
2. Select Detect > Rules.
   a. Verify that the Rules page includes all rules that existed before the restore point.
   b. (Conditional) If your organization had made changes to the rules after the restore point, update the rules as needed.
3. Select Detect > Active List.
   a. Verify that the My Active Lists page includes all lists that existed before the restore point.
   b. (Conditional) If your organization had made changes to the lists after the restore point, update the lists as needed.
4. Select Detect > Command Center.
5. Verify the presence of all custom dashboards, channels, and resources that existed before the restore point.
6. (Optional) To verify the Real-time Threat Detection Console:
   a. Go to a workstation where the Real-time Threat Detection Console has been installed.
   b. Verify that you can log in successfully and that the Console is fully operational.

Verify Data for SOAR

To validate the data in the SOAR application, complete the following steps:

1. Log in to ArcSight.
2. Select **RESPOND** > **Cases**.
3. Verify that the **Cases** page includes all cases that existed before the restore point.

4. (Conditional) Update the cases as needed, if your organization had made changes to the cases after the restore point.

Using REST APIs

User interfaces use REST APIs to manage and access data and configuration information. You can also access the APIs directly, if needed. For example, you might want to update a particular user’s dashboard or the end point documentation.

> Note: ArcSight SOAR supports REST API authentication without requiring an active ArcSight user account, due to its ability to integrate with third party applications.

Setting Up Access to REST APIs

You must have the Advanced Authentication Tenant Administrator credentials to perform this action.

To allow users access to the REST APIs, you must create an authentication event in the Advanced Authentication service. This event specifies a **Client ID** and **Client Secret** to authenticate with the REST APIs. After you have established the client secret, you might want to update it according to your password rotation policies.

1. Log in to the Advanced Authentication service.
2. Click Events > New Event.

   For more information, see Configuring Events in the *SaaS Administration Guide for Advanced Authentication*.
3. Specify a name for the Event.

   For example, enter REST API Event.
4. For Event type, select OAuth2 / OpenID Connect.
5. For Chains Used, select Password Only.
6. Copy the Client secret for later use.

   > You cannot view the Client secret after saving the event. However, you can reset the Client secret if you need.
7. Click + to expand **Advanced Settings**, enable the following fields but leave the others disabled:

- Enable Public Client
- Use for Resource Owner Password Credentials
- Enable Token Sharing

8. Set Attribute Maps:

```
localName="DN" clientName="name" accessToken="jwt"
localName="userRepository" clientName="auth_src_id" accessToken="jwt"
localName="userLastName" clientName="last_name" accessToken="jwt"
localName="userFirstName" clientName="first_name" accessToken="jwt"
localName="mail" clientName="email" accessToken="jwt"
```

For more information, see Creating an OAuth 2.0/ OpenID Connect Event.

9. Click Save.
10. Select **Events** > **Authenticators Management**.
11. Ensure Authenticators Management is set to ON for the following fields, and the rest disabled:
    - Is enabled
    - Allow basic authentication

> You must set the Event Type to Generic and Logon with expired password to Ask to change.

Configuring ArcSight SOAR

To configure ArcSight SOAR, perform the following steps:

1. Log in to ArcSight as an admin user.
2. Navigate to **RESPOND** > **Configuration** > **REST Clients.**
3. Click the **Create REST Client** button to create a new REST Client.
4. In the **REST Client Editor** window, specify details for the following fields, and click **Save**.

Value	Description
Client ID	This value will be automatically generated.
Description	Specify the description of the REST client.

A client secret is created for this REST client and is displayed in the **REST Client Details** window.

5. Note down the REST client secret along with the credentials as these would be needed whenever you call SOAR application using the REST API.

> Note:If you have lost the Client ID and Client Secret that you created for the REST client, then you can not call the SOAR application using the respective REST API. In such cases, you must create the **REST Client** credentials along with the **Client Secret** again.

Authenticating to and Calling the REST API

Before calling a REST API, you must authenticate your session, which involves generating access, refresh and session tokens. The REST API client uses these tokens when you call the REST API server.

> You must use the Password Method to be able to authenticate and call REST APIs.

1. To generate access tokens for SaaS in your API client, use the POST method and the following URL:

```
https://<tenant-name>.cyberresprod.com/osp/a/<tenant-
name>/auth/oauth2/grant
```

> Your `<tenant-name>` is part of the URL. For example, *extremelyfocused* is the tenant name in the following URL: `https://extremelyfocused.cyberresprod.com/osp/a/extremelyfocused/auth/oauth2/grant`

Select and specify *Header and Body* information as follows, where:

Authorization

- Authorization type as **Basic**
- Client_ID:Client_Secret as **base64 encoded**
- Use the client ID and secret that you created when you set up access to the REST APIs.

Header

- Content-Type as **application/x-www-form-urlencoded**
- Accept as **application/json**
    - Authorization as Basic

Body

- Enter **grant_type** as password
- Enter **Username** as User ID
- Enter **password** as the password of the UserID

> The server replies with the access_token, the expires_in number of seconds for the access_token validity, and a refresh_token to generate a new access token when the access token expires. To understand how to generate a new access token using the refresh_token, see "Refreshing Access Tokens" on page 89.

For example:

Server Request -

```
curl --location --request POST
'https://aa.cyberresprod.com/osp/a/extremelyfocused/auth/oauth2/grant' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Accept: application/json' \
--header 'Authorization: Basic Q2xpZW50SWQ6Q2xpZW50U2VjcmV0' \
--data-urlencode 'grant_type=password' \
--data-urlencode 'username=samantha.landry@extremelyfocused.com' \
--data-urlencode 'password=samanthapassword'
```

Server Response -

```
{
"access_
token":"eyJ0eXAiOiJhdCtqd3QiLCJhbGciOiJSUzI1NiIsImtpZCI6IkhCb2JINGNtS012Tl
d1TC1hZWNtSWNJajNFTSJ9.eyJpc3MiOiJodHRwczovL2FhLm1maWNzaWVkZXYuY29tL29zcC9
hL1NFQ09QU1ROMDEvYXV0aC9vYXV0aDIiLCJleHA

iOjE2OTcwMzIwODUsIm5iZiI6MTY5NzAyODQ4NSwiaWF0IjoxNjk3MDI4NDg1LCJqdGkiOiJpe
GZUQUZEWlJILXdsbTUzcUQwMWlnIiwiY2xpZW50X2lkIjoiYXV0b21hdGlvbi1vYXV0aC1jbGl
lbnQiLCJzdWIiOiJhc1xcLWFhLTg0NTNlMmY3MWQ0N2RkNDl

mOThlZmJhMzdkMjhjY2ZkIiwidHhuIjoid3NvOTF6Z21TWlMxYm50WldWMnVVdyIsImVtYWlsI
joiaWdhZG1pbkBzZWNvcHN0bjAxLmNvbSIsImZpcnN0X25hbWUiOiJpZ2FkbWluIiwibGFzdF9
uYW1lIjoiY3VzdG9tZXIiLCJhdXRoX3NyY19pZCI6IlNFQ09

QU19MT0NBTFVTRVJTIiwiYXVkIjpbImF1dG9tYXRpb24tb2F1dGgtY2xpZW50IiwiZnVtci1HS
zJabktGVzNhIiwiaWQtVkRUYzd0eVlONTBLVjM1cTFLWGtDRXpHdW82WUpMOXIiLCJyZXN0LW9
hdXRoLWNsaWVudCJdLCJhdXRoX3RpbWUiOjE2OTcwMjg0ODU

sImFtciI6WyJwd2QiXSwiX3B2dCI6IkFOQUJCUUxEQUluRHVnRWdPRFExTTJVeVpqY3haRFEzW
kdRME9XWTVPR1ZtWW1Fek4yUXlPR05qWm1RV2FXZGhaRzFwYmtCelpXTnZjSE4wYmpBeExtTnZ
iUWRKUjBGRVRVbE9FVk5GUTA5UVUxOU1UME5CVEZWVFJWSlR

DQWNXYVdkaFpHMXBia0J6WldOdmNITjBiakF4TG1OdmJSQXNOamsyTnpZeE5qUTJaRFk1Tm1VM
E1EY3pOalUyTXpabU56QTNNemMwTm1Vek1ETXhNbVUyTXpabU5tUUVJRGcwTlRObE1tWTNNV1E
wTjJSa05EbG1PVGhsWm1KaE16ZGtNamhqWTJaa0VTQmhWMlJ
vV2tjeGNHSnJRbnBhVjA1MlkwaE9NR0pxUVhoTWJVNTJZbEU5UFFBSFNVZEJSRTFKVGdJUlUwV
kRUMUJUWDB4UFEwRk1WVk5GVWxOdUFDa0F1d0EifQ.ZjbTFtoNTiWMeW-yGoo629krVXG-
0vp6TFa73x4yz8zMRcx3HkuDO4tZhGktTyj2w9pOU8yrbTjWpx-S
BB2kfJ-mjZ-bhcm80MM1-KLYNL3LXipEatWx8Drr_j9a0U-
M88wnqZiEq65ZmfqZoTfUTVk7YZ446aWbjovtKV2A-
YoM83sI5F2ow4OlAAD8IyjJDkyH5pJXVXyKS1jPs9Kazvw8JbtOZrkzliqqpyeJ-
hH5b3RrKEiAA2g4pgt50J3nC8iQkGAWY7fNRqHqLtNe
3JkJfyudQpMPYpo4GKhF55PuQpfMJYeoOwzg2oNOVCFVJdlHqZp2hcNlX7Gppt56Ug",
"token_type":"Bearer",
"expires_in":3600,
"refresh_token":"eHwAIA3qCBH_1ooIojuM4PeL4nD5kk8FGdbgB-
1Mov9xkO4OO6pRaW6qLBHuTjTWkTgUXoPzzac-mic-
5XYpPOCWtMhts7wjM9cl92KlHX3NPnPn9C4yUIVJnHIHWoYIj-r_8eDVdrHDs4jfb_
diqHG2mJYMOHqFriV8qFtHQUJRHWmkN__
dzSgQIX_ILRw-0PPx8qaczf8TscE9ABdeGxTA_OgXPdjXeyj3N6cU4_
91bQGASZ7JeCTtix0ibTrwmkKWe6tW-
MLXTFYiNfdqGFCC6N8ih8OrH40FxFnbYvWzX0488ITzcPsBMsvbtb_BNg_
IaMUf15QzPXLXjagbJx8HgkDJJi2KITQf8uX_x-TDUr2eWXzJTNT
7oAmF3LLE5m1gRp8jlUQvv0aABl_JpvmbFl-ptSu8WO5THhaGBWj-foxGzv_
YLs8V4vhxv3TpVdnn_ZTpUyRFdA7k-EEE4ssDjZI4uQmY7R1k-
k7OsioRy0Av4MH5ss7jBrJQGDeFl7Hlr-YKx5t2-
bIy4C0doXzrqCSuKQKJABcbHlOeNlN5XxwCDMCMlfUb4qb
D5tmrYdUxOgIAh5nVu7k7HQXWWxtylvcilng7hvlRdTit02bIohN3Qsz9llABzcY0bVPfBYC-
Zm_l84NkTrTrkNO6rgDkzKT-930AXVpNUsDyGPWHgLWe1rqxFGH5Tu7fvRXTmmfOTzclVE-
tBJQA0leaw04XJvkiMF7n3COAScDPhzQNRAXwfWvAcqi3yLhCRxC
kRIFu_ND2im-MTpviqa4-ZM4UBw_XqLP9o1DjLsbZJCnAMbf8"
}
```

2. To generate a session token using the access token in your API client, use the method GET and the following URL:

   ```
   https://<arcsight-saas>/mgmt/api/users/me/details
   ```

   where <*arcsight-saas*> represents your ArcSight SaaS product

   For example:

   ```
   https://extremelyfocused.mp.cyberresprod.com/mgmt/api/users/me/details
   ```

   Select and specify Header information as follows:

   Authorization

   - Authorization type as **Bearer**
   - Use the Access token generated in step 1

   For example:

```
curl -v --location --request GET
'https://extremelyfocused.mp.cyberresprod.com/mgmt/api/users/me/details' \
--header 'Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6I
kpvaG
4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_
adQssw5c'
```

3. Review the documentation for REST API endpoints.
4. Access your REST API endpoint with the session token generated in step 2 as a cookie.

   For example, to search all the dashboards owned by the logged in user ID, and the dashboards that are being shared with the logged in user ID’s role, you might use the following content:

```
curl --location --request GET
'https://extremelyfocused.mp.cyberresprod.com/metadata/api/v1/dashboards'
\
--header 'Cookie: SESSIONTOKEN=1E4C45F0B8DC821FF251EC17558B1ABF'
```

Refreshing Access Tokens

Refreshing Access Tokens

To generate the access token again with the refresh token in your API client, use the method POST and the following URL:

https://<tenant-name>.cyberresprod.com/osp/a/<tenant-name>/auth/oauth2/token

> Your <tenant-name> is part of the URL. For example, extremelyfocused is the tenant name in the following URL:
> https://extremelyfocused.cyberresprod.com/osp/a/extremelyfocused/auth/oauth2/granttoken

Select and *specify Header and Body* information as follows, where:

Authorization

Authorization type as Basic and

Client_ID: Client_Secret as base64 encoded

Use the client ID and secret that you created while Setting Up Access to REST APIs.

Header

Content-Type as application/x-www-form-urlencoded

Accept as application/json

Authorization as Basic

Body

Set grant_type as refresh_token

Set refresh_token as generated in Step 1

```
curl --location --request POST
'https://aa.cyberresprod.com/osp/a/extremelyfocused/auth/oauth2/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Accept: application/json' \
--header 'Authorization: Basic Q2xpZW50SWQ6Q2xpZW50U2VjcmV0' \
--data-urlencode 'grant_type=refresh_token' \
--data-urlencode 'refresh_token=IWmk3ugO-KI-XlM16EXSS0WJKBeN08pGh3o'
```

Using SOAR REST APIs

To use the ArcSight SOAR REST APIs, follow the steps below:

1. Navigate to https://<*OMT-machine-hostname*>/soar-api/api/v1/rest-api-docs.
2. Specify **Client ID** as **Username** and **Client Secret** as **Password.**
3. Click **Sign in**.
4. After creating the REST Client definitions, you can access REST API details UI at **/soar-api/api/v1/openapi.yaml** to familiarize yourself with the API. In the **REST API Details** UI, you can access **create scope item**, **update case**, **create case with or without scope items**, **create case comment** and **create case comment attachment** functionalities.

   The following is a sample curl request to create a SOAR case:

   > **Note**: The Authorization request header contains the Base64-encoded username/client id and password/client secret, separated by a colon. When handling the request, the server decodes the login details and checks if the user can access the requested content.

   ```
   curl -k -v 'https://<OMT-machine-hostname>/soar-api/api/v1/case' \
   -H 'authorization: Basic
   ODI5ODE4NjctODA1NC00M2YxLWE2MTQtNzgzNTUyMzg1NGUwOmY7Si9Tc1xCZlZFP0FCUS5bdE
   J5cmQ3aUZjNy9eV04w' \
   -H 'accept: application/json' \
   -H 'content-type: application/json' \
   --data-raw '{"external_id":"54","rulename":"Action
   failed","subject":"Example subject","description":"Example
   description","creation_
   time":1647441423000,"severity":"Urgent","scopeItems":
   [{"role":"RELATED","value":"example@example.com","category":"EMAIL_
   ADDRESS"}]}' \
   ```

Setting Up Access to SOAR REST APIs

You can create SOAR REST Client definitions and call the API as follows:

To create and call SOAR REST API

1. Log in to ArcSight.
2. Navigate to **RESPOND** > **Configuration** > **REST Clients**.
3. Click the **Create Rest Client** button to create a new REST Client.
4. In the **REST Client Editor** window, specify details for the following fields, and click **Save**.

Value	Description
Client ID	This value will be automatically generated.
Description	Specify the description of the REST client.

   A client secret is created for this REST client and is displayed in the **REST Client Details** window.

5. Note down the REST client secret along with the credentials as these would be needed whenever you call SOAR application using the REST API.

> **Note**:If you have lost the **Client ID** and **Client Secret** that you created for the REST client, then you can not call the SOAR application using the respective REST API. In such cases, you must create the **REST Client** credentials along with the **Client Secret** again.

Links to REST API Documentation

To review the documentation for REST API endpoints, access the URLs in the table below where <*arcsight-saas*> represents your ArcSight SaaS product. For example:

To review documentation for...	Use this URL...
Search	https://<*arcsight-saas*>/re/rest-api-docs
Event Integrity, scheduled searches	https://<*arcsight-saas*>/rec/rest-api-docs
System metadata (ArcSight Dashboard)	https://<*arcsight-saas*>/metadata/rest-api-docs
SOAR	https://<*arcsight-saas*>/soar-api/api/v1/rest-api-docs
Database monitoring	https://<*arcsight-saas*>/db-mon/rest-api-docs
Real-time Threat Detection	https://detect.<*arcsight-saas*>/detect-api https://detect.<*arcsight-saas*>/scim

Appendix - Installation Files

This section lists the installation files for your data ingestion component, which you can download from the Amazon S3 bucket. Note that a signature file (.sig) accompanies the component files so that you can verify the files have not been tampered with. The bucket might also include files for patching standalone ArcMC, and SmartConnectors.

Standalone SmartConnector Files

The Amazon S3 bucket should have the latest version of the connector files. However you will need to apply the provided parser update to your SmartConnectors. To install standalone SmartConnectors you need the following components, which you can find in the connectors folder in the S3 bucket.

Ensure that you also have downloaded the latest parser update files.

Components for your SmartConnector Environment	**File Names**
SmartConnector installer Used for adding standalone SmartConnectors, by operating system	Linux • ArcSight-8.4.x.xxxx.x-Connector-Linux64.bin • ArcSight-8.4.x.xxxx.x-Connector-Linux64.bin.sig Solaris • ArcSight-8.4.x.xxxx.x-Connector-Solaris64.bin • ArcSight-8.4.x.xxxx.x-Connector-Solaris64.bin.sig • ArcSight-8.4.x.xxxx.x-Connector-SolarisIA64.bin • ArcSight-8.4.x.xxxx.x-Connector-SolarisIA64.bin.sig Windows • ArcSight-8.4.x.xxxx.x-Connector-Win64.exe • ArcSight-8.4.x.xxxx.x-Connector-Win64.exe.sig
SmartConnector Load Balancer	• ArcSightSmartConnectorLoadBalancer-8.4.x.xxxx.x.bin • ArcSightSmartConnectorLoadBalancer-8.4.x.xxxx.x.bin.sig
(Optional) Discloses open source code used within the SmartConnector Load Balancer	• ArcSightSmartConnectorLoadBalancer-opensource-8.4.x.xxxx.x.tgz • ArcSightSmartConnectorLoadBalancer-opensource-8.4.x.xxxx.x.tgz.sig

ArcSight WiNC Hosting Appliance Collects data from Windows event log	• ArcSight_WiNC_Hosting_Appliance.8.3.x.xxxx.x.tgz • ArcSight_WiNC_Hosting_Appliance.8.3.x.xxxx.x.tgz.sig
AWS CloudWatch Connector Sends CloudWatch data to a SmartConnector	• ArcSight-AWS-CloudWatch-Connector-8.4.x.xxxx.x.zip • ArcSight-AWS-CloudWatch-Connector-8.4.x.xxxx.x.zip.sig
AWS SecurityHub Connector Sends AWS SecurityHub data to a SmartConnector	• ArcSight-AWS-SecurityHub-Connector-8.4.x.xxxx.x.zip • ArcSight-AWS-SecurityHub-Connector-8.4.x.xxxx.x.zip.sig
Azure Monitor EventHub Connector Sends EventHub data to a SmartConnector	• ArcSight-Azure-Monitor-EventHub-Connector-8.4.x.xxxx.x.zip • ArcSight-Azure-Monitor-EventHub-Connector-8.4.x.xxxx.x.zip.sig
Discloses open source code used within the SmartConnector.	• ArcSight-8.4.x.xxxx.x-opensource.tgz • ArcSight-8.4.x.xxxx.x-opensource.tgz.sig

Standalone ArcMC Files

To install or upgrade a standalone instance of ArcMC, you need the files in the table below, which you can find in the arcmc folder in the Amazon S3 bucket.

Ensure that you also have downloaded the latest parser update files.

Components for your ArcMC environment	**File Names**
ArcMC local installer and upgrade	• ArcSight-ArcMC-3.2.1.2328.0.bin • ArcSight-ArcMC-3.2.1.2328.0.bin.sig
ArcMC remote upgrade to v3.2.1	• arcmc-sw-2328-remote.enc • arcmc-sw-2328-remote.enc.sig
ArcMC agent installer	• arcsight-arcmc-agent-3.2.1.1524.0.enc • arcsight-arcmc-agent-3.2.1.1524.0.enc.sig • ArcSight-ArcMCAgent-3.2.1.1524.0.bin • ArcSight-ArcMCAgent-3.2.1.1524.0.bin.sig
Discloses open source code used within ArcMC	• arcsight-management-center-3.2.1-bundle-license.txt
SmartConnectors	See Standalone SmartConnector Files

If you have a version older than v3.1.*n*, please contact your Customer Success team to get the files for upgrading to 3.1.*n*. Then you can upgrade to 3.2.*n* using the files listed here.

Real-time Threat Detection Console Files

To install the console, use the self-extracting archive file listed in the table for the platform where you want to install the console. You can find these files in the Amazon S3 bucket.

Note that xxx stands for the build number in the following table:

Platform	Installation File
Linux	• `ArcSight-8.1.0.xxxxx.0-Console-SaaS-Linux.bin` • `ArcSight-8.1.0.xxxxx.0-Console-SaaS-Linux.bin.sig`
Windows	• `ArcSight-8.1.0.xxxx.0-Console-SaaS-Win.exe` • `ArcSight-8.1.0.xxxx.0-Console-SaaS-Win.exe.sig`
macOS	• `ArcSight-8.1.0.xxxx.0-Console-SaaS-MacOSX.zip` • `ArcSight-8.1.0.xxxx.0-Console-SaaS-MacOSX.zip.sig`

Logger Archive Migration Files

To begin the process of migrating Logger archived events to ArcSight SaaS, you need the Archive Migration Tool. You can download the file from the logger folder of the Amazon S3 bucket.

Component for Logger Archive Migration	Filename
Archive Migration Tool	• `logger-archive-catalog-tool-20230815.enc` • `logger-archive-catalog-tool-20230815.enc.sig`

Legal Notice

Confidential computer software. Valid license from OpenText required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for OpenText products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. OpenText shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information

Publication Status

Released: November 1, 2023

Updated: Monday, November 13, 2023

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Quick Start for Administrators (ArcSight SIEM as a Service 23.9.1)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!