

OpenText™ Core Application Security

Guía de usuario

Version : 26.1

PDF Generated on : February 12, 2026

Table of Contents

1. Guía de usuario	1
1.1. Prefacio	2
1.2. Introducción	3
1.2.1. Cambios de nombre de producto	4
1.2.2. Información general sobre OpenText Core Application Security	5
1.2.3. Sistema de clasificación de seguridad	7
1.2.3.1. Probabilidad y repercusión	8
1.2.3.2. Orden de prioridad	9
1.2.3.3. Clasificación de la evaluación de cinco estrellas	11
1.2.4. Objetivos de nivel de servicio	12
1.3. Primeros pasos	14
1.3.1. Antes de comenzar	15
1.3.2. Inicio y cierre de sesión en el portal	16
1.3.3. Restablecimiento de la contraseña	19
1.3.4. Navegación por el portal	20
1.3.5. Búsquedas en el portal	24
1.3.6. Administración de la configuración de la cuenta	25
1.3.6.1. Edición de la configuración de la cuenta	26
1.3.6.2. Cambio de la contraseña de la cuenta	30
1.3.7. Administración de notificaciones	32
1.3.7.1. Visualización de notificaciones	33
1.3.7.2. Creación de una suscripción individual	35
1.3.7.3. Creación de una suscripción global	39
1.3.7.4. Edición de una suscripción	43
1.3.7.5. Eliminación de una suscripción	45
1.3.8. Cambio de inquilinos	46
1.4. Administración de aplicaciones y versiones	47

1.4.1. Estructuración de aplicaciones y versiones	48
1.4.2. Administración de una aplicación	52
1.4.2.1. Creación de una aplicación	53
1.4.2.2. Visualización de los detalles de la aplicación	65
1.4.2.2.1. Desplazamiento por la página Información general de la aplicación	66
1.4.2.2.2. Filtrado de la página Información general de la aplicación	69
1.4.2.3. Edición de ajustes de aplicación	71
1.4.2.4. Administración de la asignación de usuarios a una aplicación	74
1.4.2.5. Visualización del registro de eventos de aplicaciones	78
1.4.2.6. Eliminación de una aplicación	80
1.4.3. Administración de una versión	81
1.4.3.1. Creación de una versión	82
1.4.3.2. Visualización de los detalles de la versión	86
1.4.3.2.1. Gráficos de información general de la versión	90
1.4.3.3. Reemplazo de la directiva de seguridad de una versión	98
1.4.3.4. Edición de la configuración de la versión	100
1.4.3.5. Eliminación de una versión	103
1.4.4. Visualización de aplicaciones del inquilino	104
1.4.4.1. Desplazamiento por la página Sus aplicaciones	105
1.4.4.2. Filtrado de la página Sus aplicaciones	112
1.4.5. Visualización de versiones del inquilino	115
1.4.5.1. Desplazamiento por la página Sus versiones	116
1.4.5.2. Filtrado de la página Sus versiones	121
1.4.6. Búsqueda de aplicaciones y versiones	124
1.4.7. Creación de vínculos en profundidad	125
1.5. Ejecución de evaluaciones	126
1.5.1. Evaluaciones estáticas	127
1.5.1.1. Requisitos de OpenText SAST	128

1.5.1.1.1. Lenguajes admitidos	129
1.5.1.1.2. Compiladores admitidos	134
1.5.1.1.3. Bibliotecas, marcos y tecnologías compatibles	136
1.5.1.2. Preparación de archivos en evaluaciones estáticas	150
1.5.1.2.1. Requisitos del archivo de evaluación estática	151
1.5.1.2.2. Instalación y uso del cliente Fortify ScanCentral SAST	152
1.5.1.2.3. Preparación de los archivos de aplicaciones .NET	153
1.5.1.2.4. Preparación de archivos de aplicaciones Java	157
1.5.1.2.5. Preparación de los archivos JavaScript Technology/HTML/XML	160
1.5.1.2.6. Preparación de archivos de aplicaciones Kotlin	162
1.5.1.2.7. Preparación de los archivos de aplicación de ABAP (SAP)	163
1.5.1.2.8. Preparación de archivos de aplicaciones C y C++	168
1.5.1.2.9. Preparación de archivos de aplicaciones Classic ASP, VBScript y Visual Basic	170
1.5.1.2.10. Preparación de archivos de aplicación Dart y Flutter	171
1.5.1.2.11. Preparación de archivos de aplicaciones ColdFusion Markup Language (CFML)	172
1.5.1.2.12. Preparación de archivos de aplicaciones COBOL	173
1.5.1.2.13. Preparación de archivos Dockerfiles e infraestructura como código (IaC)	175
1.5.1.2.14. Preparación de archivos de aplicaciones Go	177
1.5.1.2.15. Preparación de los archivos de aplicaciones PHP	179
1.5.1.2.16. Preparación de los archivos de aplicaciones Python	181
1.5.1.2.17. Preparación de archivos de aplicaciones Ruby	183
1.5.1.2.18. Preparación de archivos de aplicaciones Solidity	184
1.5.1.2.19. Preparación de los archivos de aplicaciones de Salesforce (Apex y Visualforce)	185
1.5.1.2.20. Preparación de archivos de aplicaciones Scala	186
1.5.1.2.21. Preparación de archivos de aplicación de Android (código fuente)	188
1.5.1.2.22. Preparación de archivos de aplicaciones iOS (código fuente)	189
1.5.1.3. Configuración de un análisis estático	190
1.5.1.4. Carga de una carga de evaluación estática	208

1.5.1.5. Validación de la carga de una evaluación estática	212
1.5.2. Análisis de composición de software de código abierto	214
1.5.2.1. Preparación de archivos de evaluación de código abierto	215
1.5.2.2. Realización de una carga de evaluación de código abierto a través del portal	225
1.5.2.3. Visualización de componentes de código abierto en una versión	227
1.5.2.4. Visualización de componentes de código abierto en un inquilino	229
1.5.3. Evaluaciones dinámicas	231
1.5.3.1. Preparación del sitio web para la prueba dinámica	232
1.5.3.2. Preparación de archivos de API web	234
1.5.3.3. Configuración de OpenText Core Application Security Connect	238
1.5.3.4. Configuración de análisis dinámicos	240
1.5.3.5. Programación de análisis dinámicos	296
1.5.3.6. Edición de la configuración de análisis dinámico para análisis en curso y completados	300
1.5.4. Evaluaciones móviles	302
1.5.4.1. Plataformas compatibles y sistemas operativos	303
1.5.4.2. Preparación de archivos en evaluaciones móviles	305
1.5.4.2.1. Preparación de archivos de aplicaciones Android (binarios)	306
1.5.4.2.2. Preparación de archivos de aplicaciones iOS (binarios)	308
1.5.4.3. Preparación del back-end para la prueba móvil	310
1.5.4.4. Configuración de análisis móviles	311
1.5.4.5. Programación de análisis móviles	322
1.5.4.6. Edición de la configuración de análisis móvil para un análisis en curso	327
1.5.5. Uso de derechos	328
1.5.6. Administración de análisis	329
1.5.6.1. Visualización de todos los análisis	330
1.5.6.2. Visualización de análisis de la aplicación	335
1.5.6.3. Visualización de análisis de versión	339
1.5.6.4. Desplazamiento por la página Análisis	343

1.5.6.5. Filtrado de la página Sus análisis	350
1.5.6.6. Comprobación del estado del análisis	352
1.5.6.7. Cancelación de un análisis	354
1.5.6.8. Reanudación de un análisis detenido	356
1.5.6.9. Visualización de vales del Centro de ayuda vinculados a un análisis	359
1.6. Corrección de vulnerabilidades	361
1.6.1. Revisión de problemas	362
1.6.1.1. Visualización de los problemas de la aplicación	364
1.6.1.2. Visualización de los problemas de versión	366
1.6.1.3. Desplazamiento por la página Problemas	368
1.6.1.4. Opciones de filtrado y agrupación en la página Problemas	374
1.6.1.5. Personalización de filtros y agrupaciones de problemas	383
1.6.1.6. Asignación de atributos para un problema	386
1.6.2. Detalles del problema	388
1.6.2.1. Detalles de los problemas de un análisis estático	389
1.6.2.2. Detalles de problemas del análisis de código abierto	394
1.6.2.3. Detalles de los problemas de un análisis dinámico	399
1.6.2.4. Detalles de los problemas de un análisis móvil	404
1.6.3. Actualizar problemas	407
1.6.3.1. Edición de un problema	408
1.6.3.2. Edición de varios problemas	412
1.6.3.3. Carga de capturas de pantalla	417
1.6.4. Auditoría de la corrección de problemas	420
1.6.4.1. Flujo de trabajo de auditoría para auditores	421
1.6.4.2. Flujo de trabajo de auditoría para desarrolladores	423
1.6.5. Auditoría y corrección con SAST Aviator	424
1.6.6. Plantillas de auditoría	432
1.6.6.1. Creación de una plantilla de auditoría global	433

1.6.6.2. Creación de una plantilla de auditoría de aplicaciones	439
1.6.6.3. Creación de un filtro de plantilla de auditoría de aplicaciones para un problema	445
1.6.6.4. Uso de plantillas de auditoría y ejemplos	449
1.6.7. Reglas de limpieza de flujo de datos	451
1.6.7.1. Creación de una regla de limpieza de flujo de datos global	452
1.6.7.2. Creación de una regla de limpieza de flujo de datos de aplicación	458
1.6.7.3. Uso de reglas de limpieza de flujo de datos y ejemplos	463
1.6.8. Solicitud de un análisis de corrección	464
1.7. Paneles e informes	465
1.7.1. Paneles de Magellan	466
1.7.1.1. Visualización de los paneles de Magellan	467
1.7.1.2. Tipos de paneles de Magellan	471
1.7.1.3. Limitaciones del panel de Magellan	473
1.7.2. Paneles heredados	474
1.7.2.1. Visualización de paneles	475
1.7.2.2. Tipos de gráfico del panel	477
1.7.2.3. Creación de un panel	482
1.7.2.4. Edición de un panel	484
1.7.2.5. Eliminación de un panel	489
1.7.3. Informes	491
1.7.3.1. Visualización de informes	492
1.7.3.1.1. Visualización de todos los informes	493
1.7.3.1.2. Filtrado de la página Sus informes	496
1.7.3.1.3. Visualización de los informes de la aplicación	497
1.7.3.1.4. Visualización de informes de la versión	498
1.7.3.2. Generación de un informe	500
1.7.3.3. Programación de informes generados automáticamente	506
1.7.3.4. Plantillas	509

1.7.3.4.1. Creación de una plantilla de informe personalizada	510
1.7.3.4.2. Edición de una plantilla de informe personalizada	515
1.7.3.4.3. Eliminación de una plantilla de informe personalizado	516
1.7.3.4.4. Supresión de una plantilla de informe del sistema	517
1.7.3.5. Exportaciones de datos	518
1.7.3.5.1. Vista de exportaciones de datos	519
1.7.3.5.2. Creación de una plantilla de exportación de datos	521
1.7.3.5.3. Generación de una exportación de datos	529
1.8. Administración	531
1.8.1. Administración del portal	532
1.8.1.1. Configuración de la seguridad de usuarios	533
1.8.1.2. Administración de claves de API	539
1.8.1.2.1. Creación de una clave de API	540
1.8.1.2.2. Roles de la clave de API	542
1.8.1.2.3. Edición o eliminación de una clave de API	544
1.8.1.3. Administración de atributos	548
1.8.1.3.1. Adición de un atributo	549
1.8.1.3.2. Edición de un atributo	554
1.8.1.3.3. Eliminación de un atributo	558
1.8.1.4. Gestión de redes de OpenText Core Application Security Connect	559
1.8.1.4.1. Agregar una red de OpenText Core Application Security Connect	560
1.8.1.4.2. Borrando una red de OpenText Core Application Security Connect	563
1.8.1.5. Visualización de derechos	564
1.8.1.6. Visualización del registro de eventos de administración	566
1.8.1.7. Configuración del estado del auditor de SAST Aviator	568
1.8.2. Administración de usuarios	570
1.8.2.1. Roles y permisos	571
1.8.2.1.1. Permisos	572

1.8.2.1.2. Roles predeterminados	582
1.8.2.1.3. Visualización de roles	586
1.8.2.1.4. Creación de un rol	588
1.8.2.1.5. Edición de un rol	590
1.8.2.1.6. Eliminación de un rol	592
1.8.2.2. Usuarios	593
1.8.2.2.1. Visualización de usuarios	594
1.8.2.2.2. Crear un usuario	596
1.8.2.2.3. Edición de una cuenta de usuario	598
1.8.2.2.4. Administración de la asignación de aplicaciones a un usuario	601
1.8.2.2.5. Eliminación de una cuenta de usuario	605
1.8.2.3. Grupos	606
1.8.2.3.1. Visualización de grupos	607
1.8.2.3.2. Creación de un grupo	609
1.8.2.3.3. Edición de un grupo	611
1.8.2.3.4. Administrar la asignación de aplicaciones para un grupo	614
1.8.2.3.5. Eliminación de un grupo	618
1.8.3. Administración de directivas	619
1.8.3.1. Creación de una directiva de seguridad	620
1.8.3.2. Configuración de la directiva de seguridad	633
1.8.3.3. Eliminación de una directiva de seguridad	635
1.8.4. Registro único (SSO)	636
1.8.4.1. Configurar SSO en OpenText Core Application Security	637
1.8.4.2. Adición de los metadatos del proveedor de identidades	652
1.8.4.3. Configuración del cifrado	655
1.8.4.4. Descarga de los metadatos de OpenText Core Application Security	658
1.8.4.5. Configuración SSO en el proveedor de identidad	659
1.8.4.6. Solución de errores de inicio de sesión	669

1.8.5. Administración de proveedores	671
1.8.5.1. Inicio de una relación con otro inquilino	672
1.8.5.2. Aceptación de una relación iniciada por otro inquilino	675
1.8.5.3. Publicación de un informe de administración de proveedores	677
1.8.5.4. Visualización de informes publicados	679
1.9. API de OpenText Core Application Security	680
1.9.1. Visualización de la documentación de la API a través del Explorador de API	681
1.9.2. Pruebas de extremos de API mediante el Explorador de API	684
1.9.3. Autenticación de API	690
1.9.4. Ámbitos de API	694
1.9.5. Límites de frecuencia de API	695
1.9.6. Tokens de acceso personal	699
1.9.6.1. Creación de un token de acceso personal	700
1.9.6.2. Edición o eliminación de los tokens de acceso personal	703
1.10. Integraciones y herramientas	705
1.10.1. Herramientas de CICD	706
1.10.2. Herramientas de IDE	710
1.10.3. Herramientas de preparación y seguimiento del análisis	715
1.10.4. Herramientas de visualización y descarga	718
1.10.5. Integraciones de portales	719
1.10.5.1. Integración con el seguimiento de errores	720
1.10.5.1.1. Configuración de la integración con el seguimiento de errores	721
1.10.5.1.2. Envío de problemas al seguimiento de errores	726
1.10.5.1.3. Vinculación manual de un problema	730
1.10.5.2. Integración de análisis externo	733
1.10.5.2.1. Importación de un análisis en las instalaciones	734
1.10.5.2.2. Importación de una lista de materiales de software	736
1.10.5.2.3. Eliminación de un análisis importado	738

1.10.5.3. Integración con Secure Code Warrior	739
1.10.5.3.1. Inicio de la formación de Secure Code Warrior	740
1.10.5.4. Integración con Slack para las notificaciones	743
1.10.5.4.1. Configuración de la integración con Slack	744
1.10.5.4.2. Eliminación de la integración con Slack	747
1.10.5.5. Integración de control de código fuente	749
1.10.5.5.1. Configuración de la integración de control de código fuente con Bitbucket	750
1.10.5.5.2. Configuración de la integración de control de código fuente con GitHub	752
1.10.5.6. Seguimiento de integraciones configuradas	754
1.10.5.7. Webhooks	757
1.10.5.7.1. Configuración de un webhook	758
1.10.5.7.2. Solicitudes y respuestas de webhook	764
1.10.5.7.3. Visualizar entregas de webhook	766
1.10.6. Cursos de formación	769
1.10.6.1. Visualización de los cursos de formación	770
1.10.6.2. Asignación de cursos de formación	771
1.10.6.3. Visualización del informe de formación	772
1.11. Directivas y soporte técnico	774
1.11.1. Programación de mantenimiento y actualizaciones de software	775
1.11.2. Directiva de retención de datos	777
1.11.3. Obtención de soporte técnico	780
1.11.3.1. Acceso a los recursos de soporte técnico	781
1.11.3.2. Envío de un vale del Centro de ayuda	782
1.11.3.3. Seguimiento de los vales del Centro de ayuda	783

1. Guía de usuario

En esta guía, se proporcionan instrucciones sobre el uso de OpenText Core Application Security para ejecutar pruebas de seguridad de aplicaciones en la nube. Esta guía está dirigida a los profesionales de la seguridad de aplicaciones y a los equipos de desarrollo.

1.1. Prefacio

Contacto con el Soporte técnico de OpenText Core Application Security

Comuníquese con el servicio de soporte técnico de OpenText Core Application Security de las siguientes maneras:

- Iniciar un chat activo o crear un vale de soporte técnico en el Centro de ayuda de OpenText Core Application Security, al cual se puede acceder desde el portal de OpenText Core Application Security.
- Llamar al 1.800.893.8141 o al 650.800.3233.

Para más información

Para obtener más información acerca de los productos Pruebas de seguridad de las aplicaciones de , vaya a Seguridad de las aplicaciones"> Seguridad de las aplicaciones.

Acerca del paquete de documentación

El conjunto de documentación del software de contiene guías de instalación, guías de usuario y guías de implementación para todos los productos y componentes de software de . Además, encontrará notas técnicas y notas de la versión que describen las nuevas características, los problemas conocidos y las actualizaciones de última hora. Puede obtener las versiones más recientes de estos documentos en el siguiente sitio web de documentación de producto de :

<https://www.microfocus.com/support/documentation>

1.2. Introducción

Esta sección contiene los siguientes temas:

- [Cambios de nombre de producto](#)
- [Información general sobre OpenText Core Application Security](#)
- [Sistema de clasificación de seguridad](#)
- [Objetivos de nivel de servicio](#)

1.2.1. Cambios de nombre de producto

OpenText está en proceso de cambiar los siguientes nombres de productos:

Nombre anterior	Nuevo nombre
Fortify Static Code Analyzer	Pruebas de seguridad de las aplicaciones estáticas OpenText™ (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	Pruebas de seguridad de las aplicaciones dinámicas OpenText™ (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	Análisis de composición de software OpenText™ Core (OpenText Core SCA)
Fortify Applications and Tools	OpenText™ Application Security Tools
Fortify Aviator	SAST Aviator

Los nombres de los productos han cambiado en las páginas de presentación, encabezados, páginas de inicio de sesión y otros lugares donde se identifica el producto. Los cambios de nombre tienen como objetivo aclarar la funcionalidad del producto y alinear mejor los productos de Fortify Software con OpenText. En algunos casos, como en la página de título de la documentación, el nombre antiguo podría incluirse temporalmente entre paréntesis. Es posible que veamos más cambios en futuros lanzamientos de productos.

1.2.2. Información general sobre OpenText Core Application Security

OpenText Core Application Security es una solución de software como servicio (SaaS) que permite que la organización cree y amplíe un programa de garantía de seguridad de software de forma rápida y sencilla. Las pruebas de seguridad de software de OpenText Core Application Security incorporan las tecnologías de pruebas de aplicaciones más avanzadas y actualizadas con revisión de expertos, administración de cuentas dedicada y soporte todos los días a toda hora.

Servicios

Una aplicación que se envía a OpenText Core Application Security pasa una evaluación de seguridad en la que realiza un análisis en busca de distintas vulnerabilidades de seguridad de software. OpenText Core Application Security ofrece evaluaciones estáticas, dinámicas y móviles en varios niveles de servicio.

- Una evaluación estática analiza el código fuente, el código de byte o el código binario de una aplicación.
- Una evaluación dinámica analiza una aplicación web en ejecución.
- Una evaluación móvil analiza el archivo binario de una aplicación móvil (también está disponible el análisis del servidor web de red y back-end).
- Un análisis de composición de software de código abierto analiza los componentes de código abierto en la carga útil.

El equipo de pruebas lleva a cabo un análisis exhaustivo de su aplicación en busca de vulnerabilidades de seguridad, entre las que se incluyen:

- Análisis de aplicaciones: la aplicación se analiza utilizando el software Fortify.
- Revisión por expertos: se realiza una auditoría automatizada de los resultados del análisis para garantizar el mayor grado de exactitud posible. Algunos tipos de evaluaciones incluyen una auditoría manual.
- Validación de corrección: una evaluación incluye al menos un análisis de corrección gratuito para validar que los problemas encontrados se solucionaron. El análisis de corrección se ejecuta en la misma aplicación después de implementar los cambios para solucionar las vulnerabilidades detectadas en la evaluación de referencia.

OpenText Core Application Security usa un sistema de clasificación de cinco estrellas para calificar las aplicaciones evaluadas. Los resultados de las evaluaciones se proporcionan de diferentes maneras, incluidas varias vistas en la interfaz de usuario, informes personalizables y exportaciones de datos detalladas.

Precios

Los servicios de OpenText Core Application Security están disponibles al comprar derechos en forma de unidades de evaluación o análisis. Los derechos son válidos durante un periodo de 12 meses, el cual comienza a partir de la fecha de vigencia del plazo del pedido.

Las unidades de evaluación pueden canjearse por suscripciones o evaluaciones únicas de cualquier tipo de evaluación. Los derechos de análisis representan las cantidades de suscripciones o evaluaciones únicas de un tipo específico de evaluación. Las suscripciones permiten realizar evaluaciones ilimitadas de aplicaciones seleccionadas durante el periodo de suscripción.

Para obtener información específica sobre los derechos, consulte su contrato.

Soporte técnico

OpenText Core Application Security ofrece soporte técnico a través de recursos de autoservicio y mediante el Centro de ayuda de OpenText Core Application Security, el cual está disponible de manera ininterrumpida y cuenta con un equipo de soporte dedicado.

1.2.3. Sistema de clasificación de seguridad

OpenText Core Application Security proporciona información útil acerca de la vulnerabilidad de sus aplicaciones. Para tener la certeza de que los resultados que recibe son coherentes, comprensibles y procesables, OpenText Core Application Security emplea las siguientes convenciones de informes para clasificar sus aplicaciones:

- [Probabilidad y repercusión](#)
- [Orden de prioridad](#)
- [Clasificación de la evaluación de cinco estrellas](#)

1.2.3.1. Probabilidad y repercusión

Las calificaciones de probabilidad y repercusión definen el nivel de riesgo de cada vulnerabilidad detectada.

Probabilidad

La probabilidad es la posibilidad de que una vulnerabilidad sea identificada de forma precisa y aprovechada con éxito.

Repercusión

La repercusión es el daño potencial que puede causar un atacante en los activos al aprovechar con éxito una vulnerabilidad. Estos daños pueden adoptar la forma de pérdidas financieras, incumplimiento de las normativas, pérdida de la reputación de la marca y publicidad negativa, entre otros.

1.2.3.2. Orden de prioridad

OpenText Core Application Security establece los seis niveles de prioridad que se describen a continuación para categorizar la gravedad de las vulnerabilidades (también conocidas como "problemas").

Crítico

Los problemas críticos tienen una alta probabilidad de producirse y una repercusión potencialmente elevada. Son fáciles de detectar y vulnerar, y pueden causar daños significativos en los activos. Estos problemas representan el mayor riesgo de seguridad para una aplicación. Por tanto, deben corregirse inmediatamente.

La inyección de SQL es un ejemplo de problema crítico.

Alto

Los problemas de prioridad alta tienen una baja probabilidad de producirse, pero una repercusión potencialmente elevada. Igualmente, suelen ser difíciles de detectar y vulnerar, pero pueden causar daños importantes en los activos. Estos problemas representan un riesgo de seguridad alto para la aplicación. Corrija los problemas de prioridad alta en la siguiente revisión programada.

Una contraseña incluida en el código es un ejemplo de problema de prioridad alta.

Medio

Los problemas de prioridad media tienen una alta probabilidad de producirse, pero una repercusión potencialmente baja. Asimismo, son fáciles de detectar y vulnerar, pero normalmente causan pocos daños en los activos. Estos problemas representan un riesgo de seguridad moderado para la aplicación. Corrija los problemas de prioridad media en la siguiente actualización del producto programada.

La manipulación de las rutas es un ejemplo de problema de prioridad media.

Bajo

Los problemas de prioridad baja tienen una probabilidad de producirse y una repercusión potencial bajas. Pueden ser difíciles de detectar y vulnerar, y normalmente dan como resultado pequeños daños en los activos. Estos problemas representan un riesgo de seguridad menor para la aplicación. Corrija los problemas de prioridad baja cuando el tiempo lo permita.

El código no alcanzado es un ejemplo de problema de gravedad baja.

Mejores procedimientos

"Mejores procedimientos" indica que no hay vulnerabilidades significativas en su aplicación, solo problemas menores que no son ideales para ese tipo de aplicación.

Información

"Información" es el nivel de prioridad más bajo. OpenText Core Application Security ofrece información sobre la aplicación que no representa una vulnerabilidad, pero que puede ser de su interés.

1.2.3.3. Clasificación de la evaluación de cinco estrellas

El sistema de clasificación de cinco estrellas de OpenText Core Application Security proporciona información general sobre la probabilidad y la repercusión de las vulnerabilidades presentes en una aplicación. Una clasificación perfecta en este sistema es de cinco estrellas, lo que indica que no se detectó ninguna vulnerabilidad.



OpenText Core Application Security concede una estrella a las aplicaciones que son objeto de una revisión de seguridad que no identifica problemas críticos (alta probabilidad y alta repercusión). Las vulnerabilidades que son fáciles de aprovechar y tienen una alta repercusión empresarial o técnica jamás deberían existir en el software importante para el negocio.



OpenText Core Application Security concede dos estrellas a las aplicaciones que han sido objeto de una revisión de seguridad que no identifica problemas críticos (alta probabilidad y alta repercusión). Las vulnerabilidades que tienen una repercusión alta, incluso si son difíciles de aprovechar, jamás deberían existir en el software importante para el negocio.



OpenText Core Application Security concede tres estrellas a las aplicaciones que son objeto de una revisión de seguridad que no identifica problemas graves (baja probabilidad y alta repercusión) y cumple con los requisitos necesarios para recibir dos estrellas. Las vulnerabilidades con una repercusión baja, pero fáciles de aprovechar, deben considerarse cuidadosamente, ya que pueden convertirse en una amenaza mayor si un atacante aprovecha muchas de ellas como parte de un esfuerzo concertado o aprovecha una vulnerabilidad de repercusión baja para lanzar un ataque de alto impacto.



OpenText Core Application Security concede cuatro estrellas a las aplicaciones que son objeto de una revisión de seguridad que no identifica problemas de gravedad media (alta probabilidad y baja repercusión) y cumple con los requisitos para recibir tres estrellas.



OpenText Core Application Security concede cinco estrellas, la clasificación más alta, a las aplicaciones que son objeto de una revisión de seguridad que no identifica ningún problema.

1.2.4. Objetivos de nivel de servicio

Todas las evaluaciones tienen un tiempo de respuesta objetivo, que se representa mediante el objetivo de nivel de servicio (SLO) del tipo de evaluación elegido. El SLO se especifica en días laborables, en función de la zona horaria del centro de datos de OpenText Core Application Security. El SLO tarda de cuatro horas a dos días laborables para una evaluación estática, de dos a tres días laborables para una evaluación dinámica y de uno a cuatro días laborables para una evaluación móvil.



Note

El portal muestra el SLO del tipo de evaluación seleccionado cuando se configura una evaluación. Para obtener más información, consulte [Finalización de la configuración de análisis estático](#), [Finalización de la configuración de análisis dinámico](#) y [Finalización de la configuración de análisis móvil](#).

Si una evaluación no cumple con los requisitos de pruebas habituales, el equipo de pruebas puede pausar el temporizador de SLO mientras se espera la respuesta del cliente. El equipo de pruebas se compromete a reiniciar el temporizador y las pruebas lo antes posible.

Si tiene más preguntas sobre los SLO y sobre cómo equilibrar los plazos del negocio con un nivel de servicio de evaluación, póngase en contacto con el soporte.



Note

Los contratos de nivel de servicio (SLA) son contratos específicos con los clientes. Los tiempos de respuesta pueden ser distintos de los SLO definidos. Los contratos de nivel de servicio se definen en el plan de trabajo (SOW) del cliente e incluyen los objetivos y las responsabilidades en caso de que estos no se cumplan.

Fechas de inicio y finalización del objetivo de nivel de servicio

Las fechas de inicio y finalización del SLO se definen del siguiente modo:

- **Fecha de inicio:** la fecha en que debe iniciarse la evaluación de la aplicación, según lo solicitado.
- **Fecha de finalización:** la fecha en la que están disponibles los resultados.

Excepciones del objetivo de nivel de servicio

El SLO de evaluación estática no se aplica a ninguna de las siguientes excepciones:

- La aplicación no se empaquetó correctamente según los procedimientos recomendados de OpenText Core Application Security
- La carga de la aplicación supera los 1000 MB.

El SLO de evaluación dinámica o móvil no se aplica a ninguna de las siguientes excepciones:

- El equipo de pruebas no tiene acceso continuo las 24 horas del día ni credenciales de prueba totalmente operativas para evaluar la aplicación que está dentro del ámbito.
- El equipo de pruebas no puede configurar herramientas de pruebas de seguridad para usar un mínimo de quince (15) conexiones simultáneas y continuas para evaluar una única aplicación con un tiempo de respuesta promedio de menos de 600 ms para una solicitud HTTP/HTTPS.
- El archivo binario móvil está ofuscado o no está preparado según los procedimientos recomendados de OpenText Core Application Security.

1.3. Primeros pasos

Esta sección contiene los siguientes temas:

- [Antes de comenzar](#)
- [Inicio y cierre de sesión en el portal](#)
- [Restablecimiento de la contraseña](#)
- [Navegación por el portal](#)
- [Búsquedas en el portal](#)
- [Administración de la configuración de la cuenta](#)
- [Administración de notificaciones](#)
- [Cambio de inquilinos](#)

1.3.1. Antes de comenzar

Antes de acceder a OpenText Core Application Security, verifique que cuenta con lo siguiente:

- Una conexión a Internet activa
- Credenciales del portal



Note

Recibirá instrucciones para configurar sus credenciales en un correo electrónico de bienvenida. Si no recibió el correo electrónico, compruebe su filtro de spam.

- Monitor con una resolución de visualización mínima de 1280 × 720 (recomendada: 1920 × 1080)
- Uno de los siguientes navegadores compatibles instalado en el equipo:
 - La versión más reciente de Chrome
 - La versión más reciente de Firefox Quantum
 - La versión más reciente de Safari para Mac (Safari para PC no es compatible)
 - La versión más reciente de Edge

1.3.2. Inicio y cierre de sesión en el portal

Puede acceder al portal una vez que haya recibido las credenciales de este.

Inicio de sesión en el portal

Para iniciar sesión en el portal:

1. Escriba la URL del portal suministrada junto con sus credenciales de usuario en la barra de direcciones del navegador.

Aparecerá la página Inicio de sesión.

2. Escriba su nombre de usuario, contraseña y código de inquilino.

opentext™

Core Application Security

26.1

Nombre de usuario

Contraseña

Inquilino

[Registro CSA STAR de nivel 1](#)

[¿Olvidó su contraseña?](#)

Iniciar sesión



Español ▾

[Información de contacto](#)

[Aviso de privacidad](#)



Note

Si ha iniciado sesión a través de SSO en los últimos 30 días, el enlace inicio de sesión de SSO estará disponible para volver a iniciar sesión.

3. Haga clic en **Iniciar sesión**.

Aparecerá la página de aterrizaje. Si no definió una pregunta y una respuesta para restablecer la contraseña, se le redirigirá a la página de configuración de la

cuenta en su lugar.



Note

Si la autenticación en dos fases está habilitada en su organización, se le pedirá que escriba un código de seguridad que recibirá por SMS, correo electrónico o TOTP.

Cierre de sesión en el portal

Cierre sesión en el portal desde la configuración de la barra de herramientas del portal. Tenga en cuenta que el portal automáticamente cierra su sesión después de un período de inactividad de 20 minutos.

Para cerrar sesión en el portal:

1. Haga clic en el nombre de la cuenta y seleccione **Cerrar sesión**.



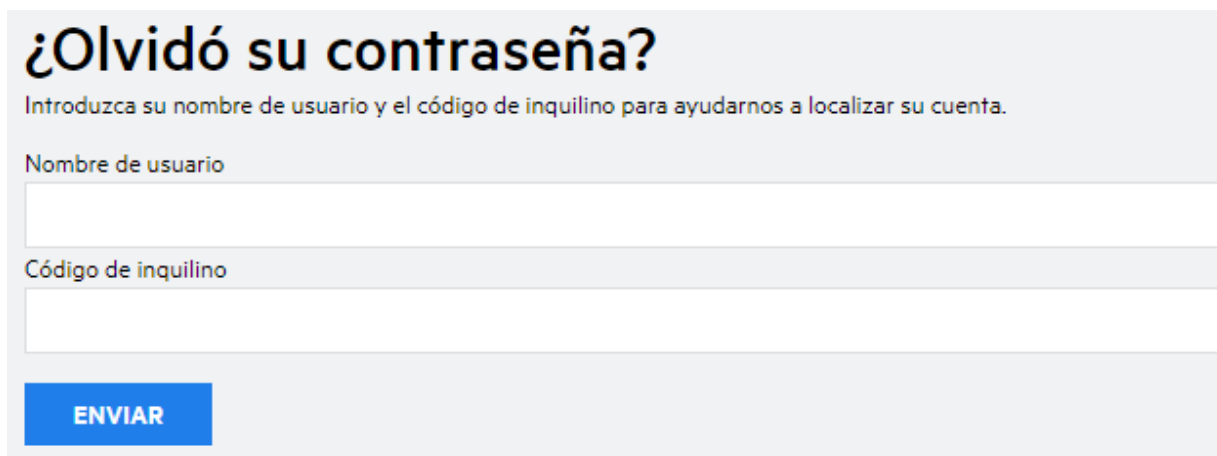
- Configuración de cuenta
- Explorador de API
- Tokens de acceso personal
- Herramientas
- Cerrar sesión

1.3.3. Restablecimiento de la contraseña

Para restablecer una contraseña olvidada:

1. Haga clic en **¿Olvidó su contraseña?** en la página de inicio de sesión.

Se abrirá la página ¿Olvidó su contraseña?.



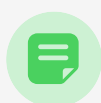
2. Escriba el nombre de usuario y el código de inquilino.

3. Haga clic en **Enviar**.

Se enviará un mensaje con un vínculo para restablecer la contraseña a la dirección de correo electrónico asociada con la cuenta de usuario.

4. Haga clic en el vínculo del mensaje de correo electrónico.

Se abrirá la página Restablecer contraseña.



Note

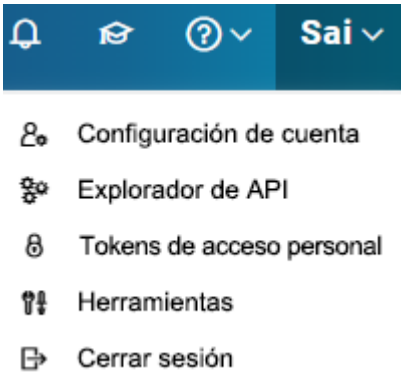
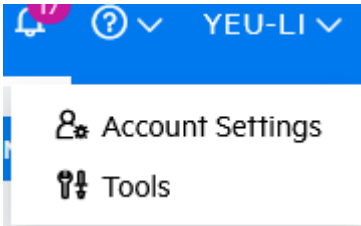
Si el vínculo para restablecer la contraseña caducó, siga las instrucciones del correo electrónico para solicitar uno nuevo.

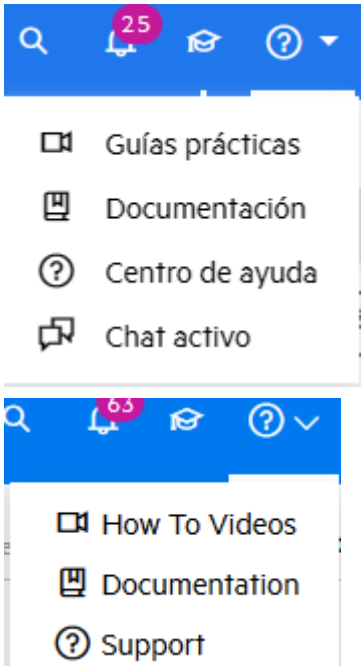
5. En el campo **Respuesta de desafío de contraseña**, escriba la respuesta a la pregunta para restablecer la contraseña. Si no tiene una pregunta y una respuesta para restablecer la contraseña, este paso no se aplica.
6. Introduzca la nueva contraseña y vuelva a escribirla para confirmarla.
7. Haga clic en **Aceptar**.

La contraseña se restablecerá.

1.3.4. Navegación por el portal

Las páginas del portal comparten un diseño de página en común. La siguiente tabla describe la navegación general por el portal.

Tarea	Acción
Navegar a una vista principal	Seleccione una de las siguientes vistas: 
Reproducir navegación de usuario	Haga clic en Restablecer elementos emergentes de visita en la barra de herramientas. 
Acceder a la configuración de la cuenta y los recursos adicionales	Haga clic en el nombre de su cuenta en la barra de herramientas.  
Acceder a la búsqueda del portal	Haga clic en . Para obtener más información, consulte Búsqueda en el portal.
Acceder a las notificaciones del portal	Haga clic en . Para obtener más información, consulte Administración de notificaciones.

Tarea	Acción
Acceder a los cursos de formación	Haga clic en  . Para obtener más información, consulte Cursos de formación .
Acceder a los recursos de ayuda	Haga clic en el menú de ayuda. 
Navegar a una vista dentro de una vista principal	Haga clic en un icono en la barra de herramientas lateral.
Acceder a la ayuda contextual	Haga clic en  . Se abrirá una ventana nueva que muestra el tema de ayuda de la característica.
Ordenar las columnas de una página	Haga clic en un encabezado de columna. Un triángulo blanco en el encabezado indica el campo que se ordena y el orden de clasificación de los datos. Para invertir el orden, simplemente haga clic otra vez en el encabezado.

Tarea	Acción
Cambiar el número de elementos mostrados en una página	Haga clic en 25, 50 o 100. Mostrar: 25 50 100 Note La pestaña Detectado en la página Sus aplicaciones admite la visualización de 250 y 500 elementos por página.
Ver otra página de la lista	Haga clic en un número de página o en una flecha. 1 2 3 4 → →

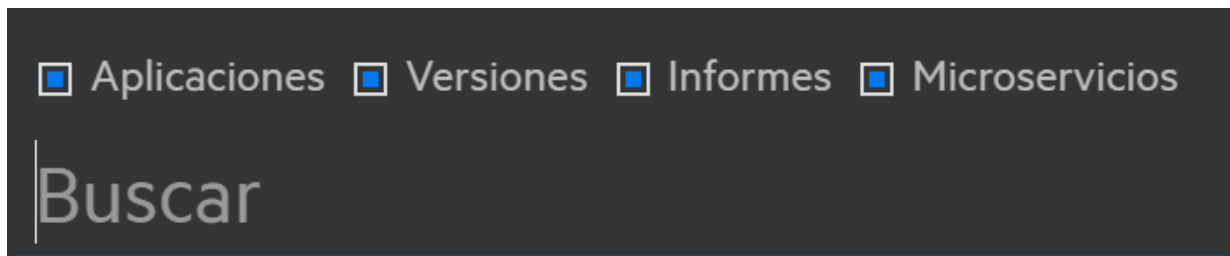
1.3.5. Búsquedas en el portal

OpenText Core Application Security proporciona varias formas de localizar un recurso en el portal. Puede usar el cuadro **Buscar** ubicado en la barra de herramientas del portal para buscar una aplicación, versión, microservicio o informe a nivel de inquilino.

Para buscar una aplicación, versión, microservicio o informe en el portal:

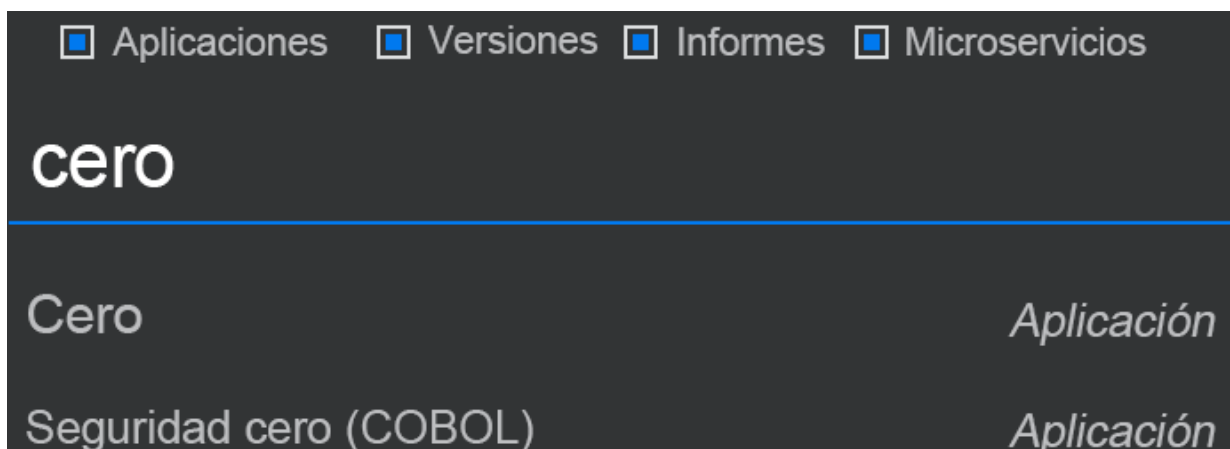
1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá el cuadro de búsqueda. Todos los tipos de elementos se incluyen en la búsqueda de forma predeterminada.



2. Desactive una o más casillas de **Aplicaciones**, **Versiones**, **Informes** y **Microservicios** para restringir los resultados de búsqueda a la selección que desee.
3. En el cuadro de búsqueda, introduzca el nombre completo o parcial del elemento que desee buscar.

Los resultados de búsqueda aparecen en una lista desplegable.



4. Seleccione un elemento de la lista. El portal se actualizará según la selección.

1.3.6. Administración de la configuración de la cuenta

Puede ver y editar la configuración de su cuenta en la barra de herramientas del portal.

Esta sección aborda los siguientes temas:

- [Edición de la configuración de la cuenta](#)
- [Cambio de la contraseña de la cuenta](#)

1.3.6.1. Edición de la configuración de la cuenta

En la página Mi cuenta, puede modificar su información de contacto personal, preferencias de portal y la pregunta y respuesta para restablecer la contraseña.

Para administrar la configuración de la cuenta:

1. Haga clic en el nombre de la cuenta y seleccione **Configuración de cuenta**.

Aparecerá la página Mi cuenta.

2. Actualice los campos según sea necesario. Los campos indicados en rojo son obligatorios.

Campo	Descripción
Nombre de pila	Su nombre
Apellido	Su apellido
Número de teléfono	Su número de teléfono
Formato de fecha	Formato de fecha mostrado: MM/DD/AAAA, DD/MM/AAAA, AAAA/MM/DD
Formato de hora	Formato de hora mostrado: 12 horas AM/PM, 24 horas
Idioma	Idioma mostrado: English, Español, 日本語  Note Los informes se generan en el idioma que seleccionó.
Pregunta de desafío de contraseña	Lista de preguntas para restablecer la contraseña

Campo	Descripción
Respuesta de desafío de contraseña	Su respuesta, que no distingue mayúsculas de minúsculas, a la pregunta para restablecer la contraseña seleccionada  Note Si no definió una pregunta y una respuesta para restablecer la contraseña, no podrá guardar los cambios de la cuenta.

- Actualice sus suscripciones en la sección **Suscripciones por correo electrónico**. Las suscripciones por correo electrónico le mantienen al día de los eventos de OpenText Core Application Security. Puede registrarse para recibir notificaciones sobre versiones y mantenimiento, avisos de seguridad y seminarios web y conferencias relevantes.
- Para solicitar un nuevo autenticador TOTP, haga clic en **Generar nuevo código QR**. Aparece la pantalla Código de seguridad.

×

Código de seguridad



Introduzca el código de verificación TOTP

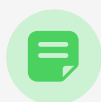
Enviar

1. Escanee el código QR.
 2. Introduzca el código de verificación TOTP.
 3. Haga clic en **Enviar** para verificar el código.
5. Haga clic en **Guardar**.

Aparecerá un mensaje de confirmación indicando que se han guardado correctamente sus cambios.

1.3.6.2. Cambio de la contraseña de la cuenta

Puede cambiar la contraseña de su cuenta en la página Mi cuenta.



Note

Las contraseñas deben tener al menos 16 caracteres, no deben tener frases de contraseña comunes ni fáciles, y deben incluir al menos una letra mayúscula, una letra minúscula, un número y un carácter especial.

Para cambiar la contraseña de la cuenta:

1. Haga clic en el nombre de la cuenta y seleccione **Configuración de cuenta**.

Aparecerá la página Mi cuenta.

Mi cuenta Cambiar contraseña Guardar

Advertencia de seguridad: A fin de mejorar la seguridad de la cuenta, proporcione una pregunta y una respuesta de desafío para el restablecimiento de la contraseña.

Nombre de pila Sai Apellido Fu Número de teléfono La siguiente configuración determina los formatos utilizados para mostrar fechas y horas. Los cambios en los formatos de presentación no se reflejarán hasta la próxima actualización de datos. Formato de fecha AAAA/MM/DD Formato de hora 12 horas AM/PM Idioma English Pregunta de desafío de contraseña ¿Cómo se llama su mascota favorita? Respuesta de desafío de contraseña	Nombre de usuario saislead Inquilino Go Suscripciones de correo electrónico Registro (marcar para suscribirse) ☐ Notificaciones de versión y mantenimiento ☐ Eventos (p. ej., seminarios web, conferencias, etc.) ☐ Avisos de seguridad e investigación	Configuración de pantalla Tema Configuración del navegador

2. Haga clic en **Cambiar contraseña**.

Aparecerá la página Cambiar contraseña.

Cambiar contraseña

Escriba su contraseña actual como verificación.

Contraseña anterior

Nueva contraseña

Confirmar nueva contraseña

ACEPTAR

VOLVER A LA CUENTA

3. Escriba su contraseña actual en el campo **Contraseña anterior**.
4. Escriba una nueva contraseña en el campo **Nueva contraseña**.
5. Vuelva a introducir la contraseña en el campo **Confirmar nueva contraseña**.
6. Haga clic en el botón **Aceptar** para cambiar la contraseña o haga clic en **Volver a la Cuenta** para salir de la página.

1.3.7. Administración de notificaciones

OpenText Core Application Security proporciona un motor sólido de notificaciones en los productos para permitir que los usuarios supervisen mejor la actividad clave del portal, lo cual es de particular importancia para bases de aplicaciones y usuarios amplias. A los usuarios se les asignan inicialmente suscripciones globales predeterminadas del sistema para eventos importantes (por ejemplo, cuando cambia la importancia para el negocio de una aplicación; cuando una versión con errores se promueve a producción; y cuando se inician, se detienen, se completan o se cancelan los análisis de una aplicación). Los usuarios pueden acceder cómodamente a las notificaciones para las aplicaciones para las que tienen acceso desde la barra de herramientas del portal.

Los usuarios pueden crear suscripciones individuales para recibir notificaciones adicionales. Los líderes en seguridad pueden crear suscripciones globales de nivel de inquilino para todos los usuarios, los roles concretos o los grupos específicos. Están disponibles los siguientes tipos de desencadenadores de notificación:

- Creación, actualización y eliminación de aplicaciones
- Creación, actualización (incluida la promoción de versiones con errores a producción) y eliminación de versiones
- Actualizaciones del estado del análisis
- Actualizaciones de problemas
- Generación de informes

Esta sección contiene los siguientes temas:

- [Visualización de notificaciones](#)
- [Creación de una suscripción individual](#)
- [Creación de una suscripción global](#)
- [Edición de una suscripción](#)
- [Eliminación de una suscripción](#)

1.3.7.1. Visualización de notificaciones

Puede ver notificaciones desde cualquier página en el portal. Cuando ocurre un evento desencadenador para el cual está suscripto, se incrementa un número junto al icono de notificaciones en la barra de herramientas. Este número representa el total de notificaciones que no se marcaron como leídas.



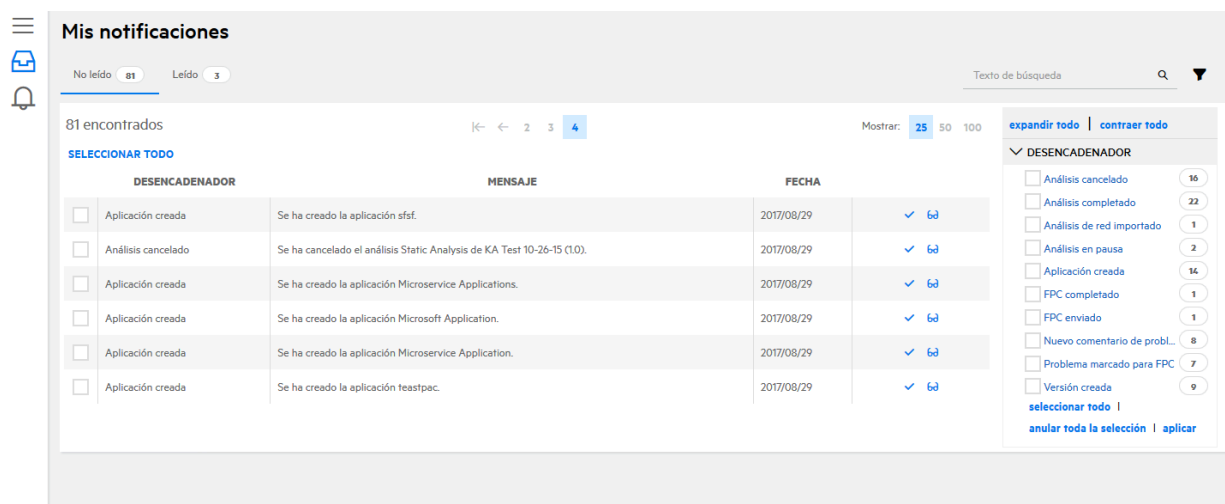
Note

Todas las notificaciones, leídas o no leídas, se eliminan transcurridos tres meses.

Para ver las notificaciones:

1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá la página Notificaciones y se mostrará una lista de las notificaciones sin leer.



Mis notificaciones

No leído 81 Leído 3

Texto de búsqueda 🔍

81 encontrados |< 2 3 4 |> Mostrar: 25 50 100

[SELECCIONAR TODO](#)

DESENCADENADOR	MENSAJE	FECHA	Acción
☐ Aplicación creada	Se ha creado la aplicación sfst.	2017/08/29	✓ 6d
☐ Análisis cancelado	Se ha cancelado el análisis Static Analysis de KA Test 10-26-15 (1.0).	2017/08/29	✓ 6d
☐ Aplicación creada	Se ha creado la aplicación Microservice Applications.	2017/08/29	✓ 6d
☐ Aplicación creada	Se ha creado la aplicación Microsoft Application.	2017/08/29	✓ 6d
☐ Aplicación creada	Se ha creado la aplicación Microservice Application.	2017/08/29	✓ 6d
☐ Aplicación creada	Se ha creado la aplicación teastpac.	2017/08/29	✓ 6d

DESENCADENADOR

- ☐ Análisis cancelado 16
- ☐ Análisis completado 22
- ☐ Análisis de red importado 1
- ☐ Análisis en pausa 2
- ☐ Aplicación creada 14
- ☐ FPC completado 1
- ☐ FPC enviado 1
- ☐ Nuevo comentario de probl... 8
- ☐ Problema marcado para FPC 7
- ☐ Versión creada 9

[seleccionar todo](#) | [anular toda la selección](#) | [aplicar](#)

2. Para ver una notificación con mayor detalle, haga clic en el icono  en la columna de acción de la notificación. Irá a la página de la aplicación, la versión o el problema individual correspondiente.
3. Para marcar una notificación como leída, haga clic en el icono  en la columna de acción de la notificación. También puede filtrar la lista de notificaciones y hacer clic en **Marcar como leído** para editar notificaciones por lotes.

Las notificaciones se moverán a Notificaciones leídas y se eliminarán del total.

4. Para ver las notificaciones marcadas anteriormente como leídas, seleccione la pestaña **Leído**.

Aparecerá la lista de notificaciones leídas.

Mis notificaciones

No leído 85

Leído 3

Texto de búsqueda

3 encontrados

Mostrar:

25

50

100

expandir todo

contraer todo

SELECCIONAR TODO

DESENCADENADOR

MENSAJE

FECHA

☐	Análisis completado	Se ha completado el análisis Dynamic Website Assessment de 174 Dynamic Website Assessment (1).	2017/11/08	6d
☐	FPC completado	Se ha completado un desafío de falso positivo de 174 Dynamic Website Assessment (1).	2017/11/08	6d
☐	FPC enviado	Se ha enviado un desafío de falso positivo de 174 Dynamic Website Assessment (1).	2017/11/08	6d

DESENCADENADOR

☐ Análisis completado 1

☐ FPC completado 1

☐ FPC enviado 1

seleccionar todo | anular toda la selección | aplicar

1.3.7.2. Creación de una suscripción individual

Además de recibir notificaciones globales, puede crear sus propias suscripciones para recibir notificaciones desencadenadas por los criterios que especifique.

Para crear una suscripción individual:

1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá la página Notificaciones.

2. Haga clic en **Suscripciones**.

Aparecerá una lista de sus suscripciones individuales.



La interfaz muestra el título 'Mis suscripciones' con pestañas para 'Mis suscripciones' (1) y 'Suscripciones globales' (14). Hay un campo de búsqueda y un botón '+ NUEVA SUSCRIPCIÓN'. Se muestran 1 resultado en una tabla con las siguientes columnas:

DESENCADENADOR	ÁMBITO	ENVIAR CORREOS ELECTRÓNICOS	NOTA
Aplicación eliminada	Todas las aplicaciones	☐	trtr12345

En la parte superior derecha de la tabla, se indica 'Mostrar: 25 50 100'.

3. Haga clic en **+Nuevas suscripciones**.

Se abrirá la ventana modal Crear suscripción.

Crear suscripción

Opciones

Resumen

Desencadenador

(Elija uno)

Ámbito

Todas las aplicaciones

Nota

Enviar correos electrónicos

No

Enviar a Slack

No

ATRÁS

SIGUIENTE

GUARDAR

Create Subscription

Options

Summary

Trigger

(Choose One)

Scope

All Applications

Note

Send Emails

No

BACK

NEXT

SAVE

4. Complete los campos. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Desencadenador	Seleccione el tipo de desencadenador en la lista.
Ámbito	Seleccione el ámbito al que se aplicará el desencadenador en la lista: Todas las aplicaciones (predeterminado), Aplicación , Tipo de aplicación , Atributo de la aplicación , Importancia para el negocio y Todas mis versiones .
	(Opcional) Escriba una nota para la suscripción.
Enviar correos electrónicos	(Opcional) Mueva el control deslizante de No a Sí para habilitar las notificaciones por correo electrónico. Esta opción está disponible para el desencadenador Problema asignado al usuario y todos los desencadenadores no relacionados con problemas.
Enviar a Slack	(Opcional) Mueva el control deslizante de No a Sí para publicar notificaciones en Slack. Esta opción solo estará disponible si se ha configurado la integración con Slack y está limitada a los líderes en seguridad.

5. Haga clic en **Siguiente**.

Si ha seleccionado un ámbito que no sea **Todas las aplicaciones**, se abrirá la página **Ámbito**. De lo contrario, vaya al paso 7.

6. Seleccione el valor de ámbito y haga clic en **Siguiente**.

7. Revise la configuración de desencadenadores de notificación y haga clic en **Guardar**.

La nueva suscripción aparecerá en la lista de suscripciones individuales.

1.3.7.3. Creación de una suscripción global

Los líderes en seguridad pueden crear suscripciones globales de nivel de inquilino para todos los usuarios, los roles concretos o los grupos específicos.

Para crear una suscripción global:

1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá la página Notificaciones.

2. Haga clic en **Suscripciones**.

Aparecerá una lista de sus suscripciones individuales.



Mis suscripciones					
Mis suscripciones 1		Suscripciones globales 14		Texto de búsqueda 🔍 + NUEVA SUSCRIPCIÓN	
1 encontrados					
DESENCADENADOR	ÁMBITO	ENVIAR CORREOS ELECTRÓNICOS	NOTA		
Aplicación eliminada	Todas las aplicaciones	☐	trtr12345		

3. Seleccione la pestaña **Suscripciones globales**.

Aparecerá una lista de las suscripciones globales, incluidas las suscripciones globales predeterminadas del sistema.



Mis suscripciones					
Mis suscripciones 0		Suscripciones globales 12		Texto de búsqueda 🔍 + NUEVA SUSCRIPCIÓN	
12 encontrados					
DESENCADENADOR	ÁMBITO	ENVIAR CORREOS ELECTRÓNICOS	CREADO POR	DESTINATARIO	NOTA
Análisis reanudado	Todas las aplicaciones	☐	ChuSecLead Last, ChuSecLead First (ChuSecLead)	Todos	Default System Notification for S...
La carga no tiene archivos de origen	Todas las aplicaciones	☐	ChuSecLead Last, ChuSecLead First (ChuSecLead)	Todos	Default System Notification for ...

4. Haga clic en **+Nueva suscripción**.

Se abrirá la ventana modal Crear suscripción.

Crear suscripción



Opciones

Resumen

Desencadenador

(Elija uno)

Destinatario

Todos

Ámbito

Todas las aplicaciones

Nota

Enviar correos electrónicos

No

Enviar a Slack

No

ATRÁS

SIGUIENTE

GUARDAR

- Complete los campos. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Desencadenador	Seleccione el tipo de desencadenador en la lista.
Destinatario	Seleccione el público para la suscripción de la lista: Todos (predeterminado), Grupo y Rol. Si selecciona Grupo o Rol, seleccione un grupo o rol específico, respectivamente.  Note Los destinatarios están limitados a usuarios que tienen acceso a la aplicación a la que se hace referencia en una notificación.
Ámbito	Seleccione el ámbito al que se aplicará el desencadenador en la lista: Todas las aplicaciones (predeterminado), Aplicación , Tipo de aplicación , Atributo de la aplicación , Importancia para el negocio y Todas mis versiones .
	(Opcional) Escriba una nota para la suscripción.

Campo	Descripción
Enviar correos electrónicos	(Opcional) Mueva el control deslizante de No a Sí para habilitar las notificaciones por correo electrónico. Los desencadenadores Análisis cancelado y Análisis en pausa tienen la opción Enviar correos electrónicos habilitada permanentemente. Esta opción está disponible para el desencadenador Problema asignado al usuario y todos los desencadenadores no relacionados con problemas.
Enviar a Slack	(Opcional) Mueva el control deslizante de No a Sí para publicar notificaciones en Slack. Esta opción estará disponible si se ha configurado la integración con Slack y está limitada a los líderes en seguridad.

6. Haga clic en **Siguiente**.

Si ha seleccionado un ámbito que no sea **Todas las aplicaciones**, se abrirá la página **Ámbito**. De lo contrario, vaya al paso 8.

7. Seleccione el valor de ámbito y haga clic en **Siguiente**.

8. Revise la configuración de desencadenadores de notificación y haga clic en **Guardar**.

La nueva suscripción aparecerá en la lista de suscripciones globales.

1.3.7.4. Edición de una suscripción

Puede editar las suscripciones personalizadas. Si es un líder en seguridad, también puede editar las suscripciones globales.

Para editar suscripciones:

1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá la página Notificaciones.

2. Haga clic en **Suscripciones**.

Aparecerá una lista de sus suscripciones personalizadas.



3. Si desea editar una suscripción personalizada, permanezca en la pestaña **Mis suscripciones**. Si desea editar una suscripción global como líder en seguridad, seleccione la pestaña **Suscripciones globales**.
4. Haga clic en el icono  junto a la suscripción que desea editar.

Aparece la ventana Editar suscripción.

Crear suscripción



Opciones

Resumen

Desencadenador

(Elija uno)



Destinatario

Todos



Ámbito

Todas las aplicaciones



Nota

Enviar correos electrónicos

No

ATRÁS

SIGUIENTE

GUARDAR

5. Edite los campos según sea necesario. Para obtener información sobre los campos, consulte [Creación de una suscripción individual](#) y [Creación de una suscripción global](#).

Se guardarán los cambios aplicados en la suscripción.

1.3.7.5. Eliminación de una suscripción

Puede eliminar suscripciones individuales que haya creado. Los líderes en seguridad pueden eliminar todas las suscripciones globales, incluidas las suscripciones globales predeterminadas del sistema.

Para eliminar una suscripción:

1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá la página Notificaciones.

2. Haga clic en **Suscripciones**.

Aparecerá una lista de sus suscripciones individuales.



3. Si desea eliminar una suscripción individual, permanezca en la pestaña **Mis suscripciones**. Si desea eliminar una suscripción global, seleccione la pestaña **Suscripciones globales**.

4. Haga clic en el icono  junto a la suscripción que desea eliminar.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí** para confirmar la eliminación.

Se eliminará la suscripción de la lista de suscripciones.

1.3.8. Cambio de inquilinos

Los TAM pueden cambiar entre las cuentas de inquilinos que administran en un centro de datos del portal.

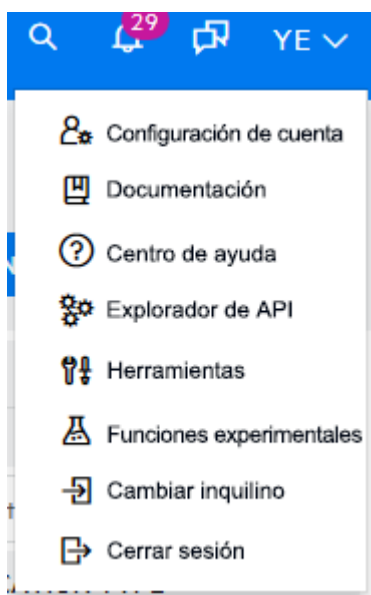


Note

Esta es una función exclusiva de TAM.

Para cambiar los inquilinos:

1. Haga clic en el nombre de la cuenta y seleccione **Cambiar inquilinos**.



Aparece la página Cambiar inquilinos.

2. Seleccione el inquilino deseado en la lista de inquilinos disponibles.

El portal se actualiza con los datos seleccionados del inquilino.

1.4. Administración de aplicaciones y versiones

Los resultados de las evaluaciones de seguridad se organizan conforme a las aplicaciones y las versiones asociadas en OpenText Core Application Security. Los usuarios pueden administrar las aplicaciones y las versiones en el portal.

Esta sección contiene los siguientes temas:

- [Estructuración de aplicaciones y versiones](#)
- [Administración de una aplicación](#)
- [Administración de una versión](#)
- [Visualización de aplicaciones del inquilino](#)
- [Visualización de versiones del inquilino](#)
- [Búsqueda de aplicaciones y versiones](#)
- [Creación de vínculos en profundidad](#)

1.4.1. Estructuración de aplicaciones y versiones

OpenText Core Application Security define una aplicación y versión para las evaluaciones de seguridad.

Definición de aplicación

Una aplicación es un código base. Sirve como un contenedor de nivel superior para una o más versiones.

OpenText Core Application Security define una aplicación en los siguientes contextos:

Para las evaluaciones estáticas, una aplicación se define como una unidad de código que puede implementarse que consta de una colección de archivos de instrucciones de código fuente o de byte que:

- Puede ofrecer parte o la totalidad de la funcionalidad de una aplicación empresarial
- Está escrito en la misma familia de tecnología.
- Está construido en una sola plataforma.
- No incluye ningún componente sin conexión directa
- Se puede configurar para ejecutarse en un servidor de aplicaciones (por ejemplo, un archivo de aplicación web [WAR] o Enterprise [EAR] para una aplicación Java o una solución en Team Foundation Server para una aplicación .NET).

Un microservicio es un servicio pequeño y modular que se ejecuta como un proceso independiente y sin conexión directa y se comunica a través de un mecanismo bien definido y liviano para servir a una función única de una aplicación empresarial. Para una aplicación que usa una arquitectura de microservicios, una suscripción estática le permite a un cliente probar hasta 10 microservicios que forman total o parcialmente la aplicación. Cada microservicio debe empaquetarse y enviarse como un solo archivo ZIP de 100 MB o menos. Para todos los otros servicios de evaluación estática, cada microservicio se considera como una aplicación separada.

Las aplicaciones de microservicios están sujetas a las siguientes condiciones:

- Los componentes tecnológicos compatibles son los siguientes: .NET, .NET Core, C/C++, Go, JAVA/J2EE, JS/TS/HTML, PHP, Python, Scala, y Ruby.

- Los análisis estáticos enviados para varios microservicios se colocan en una cola y se analizarán en el orden en el que se encuentran en la cola.
- Las bibliotecas de terceros siempre se excluyen cuando se analizan microservicios.

Para las evaluaciones dinámicas, una aplicación se define como un nombre de dominio completo (FQDN). Por ejemplo, para www.microfocus.com:

- www.microfocus.com es el FQDN y es la aplicación.
- www.microfocus.com/news/ es el mismo nombre de host y, por lo tanto, el mismo FQDN, es decir, la misma aplicación.
- community.microfocus.com es un subdominio diferente y, por lo tanto, un FQDN diferente, es decir, es una aplicación diferente.
- www.microfocus.co.uk es un nombre de dominio diferente y, por lo tanto, un FQDN diferente, es decir, es una aplicación diferente.

La aplicación solo puede tener un único sistema de gestión de autenticación con las siguientes excepciones:

- Se permite la autenticación de formularios y la autenticación de red única (basic/digest/NTLM).
- Se permite la autenticación de formularios, la autenticación de red única y la autenticación generada por aplicaciones, como tokens Bearer.

Los inicios de sesión del usuario no se pueden “conectar en serie”. Por ejemplo, no se permiten mecanismos de autenticación de dos formularios.

Solo para las aplicaciones de API web, el cliente debe proporcionar una definición de los extremos del API:

- Evaluaciones dinámicas
 - REST API: especificación OpenAPI JSON o colección Postman con valores válidos para todos los parámetros y un token de autenticación codificado y duradero
- Evaluaciones Dinámicas+
 - REST API: especificación OpenAPI JSON o colección Postman
 - SOAP: un archivo único SOAP WSDL

Se deben proporcionar ejemplos de trabajo con valores válidos para todos los parámetros.

Para evaluaciones móviles, una aplicación es una sola aplicación que puede instalarse para una plataforma de hardware única. Las aplicaciones móviles que se envían para su comprobación deben tener la forma de un IPA (iOS) o un APK (Android) compilados.

Definición de la versión

Una versión es una iteración particular de un código base. En OpenText Core Application Security, la versión de lanzamiento proporciona una forma útil de diferenciar la actividad de análisis y realizar su seguimiento. Puede estructurar las versiones según las necesidades de preparación de informes y los procesos de desarrollo de su organización.

En los siguientes ejemplos se muestra cómo pueden estructurarse las versiones:

- Evaluaciones estáticas:
 - Cree una versión principal, copiada de una versión de línea de base inicial, para análisis automatizados en compilaciones de un servidor de compilaciones de integración continua. Periódicamente, cree versiones en rama para escenarios como implementaciones importantes de código (mediante copiar estado), análisis más detallados (incluidas bibliotecas de terceros o la elección de auditoría manual para una línea de base) o versiones de prueba para realizar un análisis por única vez sin afectar las métricas.
 - Cree una nueva versión para cada versión de producto importante (mediante copiar estado) y realice análisis durante un ciclo de versión antes de continuar con la siguiente versión.
 - Cree una versión por cada compilación. Este enfoque no se recomienda debido a la falta de tendencias y al aumento de la carga.
- Evaluaciones dinámicas:
 - Cree una sola versión, sobre la base del entorno bajo análisis (desarrollo, representación, prueba de aceptación del usuario o producción) para todos los análisis. Por lo general, la URL le da nombre a la versión.
 - Cree una nueva versión para cada implementación importante (mediante copiar estado).
- Evaluaciones estática más dinámica:

- Implemente los ejemplos indicados arriba de manera individual o en combinación. Por ejemplo, puede implementar el primer ejemplo de evaluación estática como enfoque principal y realizar análisis dinámicos sobre las ramas de versión importantes y principales, o bien realizar análisis dinámicos sobre una versión separada que sea independiente de los análisis estáticos.
- Evaluaciones móviles:
 - Para las evaluaciones solo del binario móvil, implemente los ejemplos de evaluación estática.
 - Para las evaluaciones que incluyen servicios web back-end, implemente los ejemplos de evaluaciones dinámicas.

Además, puede asignar etapas del ciclo de vida de desarrollo de software (SDLC) a una versión para darle seguimiento a medida que avanza a través del SDLC. OpenText Core Application Security usa las siguientes etapas de SDLC:

- Desarrollo
- Control de calidad/Prueba
- Producción
- Retirado



Note

No se pueden iniciar nuevos análisis para una versión retirada. Aunque se retire una versión mientras hay un análisis en curso, el análisis finalizará.

1.4.2. Administración de una aplicación

Puede crear, visualizar y editar las aplicaciones según sus permisos de usuario.

Esta sección aborda los siguientes temas:

- [Creación de una aplicación](#)
- [Visualización de los detalles de la aplicación](#)
- [Edición de ajustes de aplicación](#)
- [Administración de la asignación de usuarios a una aplicación](#)
- [Visualización del registro de eventos de aplicaciones](#)
- [Eliminación de una aplicación](#)

1.4.2.1. Creación de una aplicación

Antes de comenzar la evaluación inicial de seguridad de una aplicación, es necesario crear una aplicación nueva en OpenText Core Application Security.

Para crear una aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **+ Nueva aplicación**.

Aparece el asistente para crear aplicaciones.

3. En la página **Detalles de la aplicación**, defina la aplicación. Los siguientes campos son obligatorios a menos que se indique lo contrario.

Crear aplicación

- Detalles de la aplicación**
- Información de la versión
- Atributos de aplicación
- Atributos de versión
- Grupos de usuarios
- Resumen

Nombre de aplicación

prueba

Importancia para el negocio

Medio

Tipo de aplicación

Web/Ciente pesado

☐ Aplicación de microservicios ⓘ

Descripción

Notificaciones de correo electrónico

Separe las direcciones de correo electrónico mediante punto y coma o coma.

Atrás

Siguiente

Guardar

Campo	Descripción
Nombre de la aplicación	Escriba el nombre de su aplicación.
Importancia para el negocio	Seleccione el nivel de importancia de la aplicación: ◦ Alta: los problemas de seguridad podrían acarrear consecuencias catastróficas para el negocio. ◦ Media: los problemas de seguridad acarrearían consecuencias importantes, pero que no suponen una amenaza de vida o muerte para el negocio. ◦ Baja: los problemas de seguridad se pueden ignorar o se pueden abordar gradualmente conforme sea posible.
Descripción	(Opcional) Escriba una descripción de la aplicación que le ayudará a administrar varias aplicaciones.
Notificaciones de correo electrónico	(Opcional) Enumere las direcciones de correo electrónico a las que se enviarán notificaciones de las actualizaciones del estado del análisis para la aplicación. Separe las direcciones de correo electrónico mediante punto y coma o coma.
Tipo de aplicación	Seleccione el tipo de aplicación: Web/Cliente pesado o Móvil.

Campo	Descripción
Aplicación de microservicios	Cree un vale del Centro de ayuda para que se habilite la función. (Solo aplicaciones Web/Cliente pesado) Active la casilla para analizar la aplicación como una aplicación de microservicios.  Important La designación de una aplicación de microservicios es permanente y no se puede cambiar después de crear la aplicación.

4. Haga clic en **Siguiente**.

5. (Solo aplicaciones de microservicios) En la página **Microservicios**, escriba el nombre de un microservicio en el cuadro de texto y haga clic en **+**.

El microservicio se agrega abajo. Puede agregar hasta 10 microservicios.



Note

También puede agregar microservicios a una aplicación después de crearla.

Crear aplicación



✓ Detalles de la aplicación

Microservicios

Información de la versión

Atributos de aplicación

Grupos de usuarios

Resumen

Microservicios



Defina uno o más microservicios para esta aplicación (límite: 10).

ATRÁS

SIGUIENTE

GUARDAR

6. Haga clic en **Siguiente**.

7. Si se han configurado atributos de microservicio, especifique los atributos de microservicio (solo aplicaciones de microservicio). Haga clic en **Siguiente** para hacer lo mismo para cada microservicio que haya agregado anteriormente.

Crear aplicación



✓ Detalles de la aplicación

✓ Microservicios

M1

Información de la versión

Atributos de aplicación

Grupos de usuarios

Resumen

Microservice 1

Microservice 2

ATRÁS

SIGUIENTE

GUARDAR

8. Haga clic en **Siguiente**.

9. En la página **Detalles de la versión**, defina una versión de la aplicación. La versión representa una iteración de la aplicación que se comprobará. Los siguientes campos son obligatorios a menos que se indique lo contrario.

Crear aplicación



✓ Detalles de la aplicación

✓ Microservicios

Información de la versión

Atributos de aplicación

Grupos de usuarios

Resumen

Nombre de la versión

Estado de SDLC

Microservicio

Propietario

Descripción

ATRÁS

SIGUIENTE

GUARDAR

Campo	Descripción
Nombre de la versión	Escriba el nombre de su versión.
Estado de SDLC	Seleccione Ciclo de vida de desarrollo del software de la lista. La opción Retirado no está disponible.
Microservicio (solo aplicaciones de microservicios)	En la lista desplegable, seleccione el microservicio que se vinculará con la versión. Una versión debe vincularse con un microservicio.
Propietario	Seleccione el propietario de la versión. El propietario recibirá notificaciones por correo electrónico relacionadas con las actualizaciones del estado del análisis de la versión.
Descripción	(Opcional) Escriba una descripción que ofrezca información sobre la versión.

10. Haga clic en **Siguiente**.

11. Si se configuran atributos de aplicación personalizados para el inquilino, en la página **Atributos de aplicación**, especifique los atributos de la aplicación.

Crear aplicación



✓ Detalles de la aplicación

✓ Microservicios

✓ Información de la versión

Atributos de aplicación

Grupos de usuarios

Resumen

Test Attrib 1

(Elija uno)



Test123

(Elija uno)



QA Owner

(Elija uno)



Keywords

fgfdd

sdf

(Elija uno)



Date

New

(Elija uno)



ATRÁS

SIGUIENTE

GUARDAR

12. Haga clic en **Siguiente**.

13. Si se configuran atributos de versión personalizados para el inquilino, en la página **Atributos de versión**, especifique los atributos de la versión.

Crear aplicación

- ✓ Detalles de la aplicación
- ✓ Información de la versión
- ✓ Atributos de aplicación
- Atributos de versión**
- Grupos de usuarios
- Resumen

RelAttr

(Elija uno)

ATRÁS

SIGUIENTE

GUARDAR

- Si se configuraron grupos de usuarios para el inquilino, seleccione los grupos que tienen acceso a la aplicación en la página **Grupos de usuarios**. Puede usar el cuadro de búsqueda para buscar nombres de grupos.

Crear aplicación



- ✓ Detalles de la aplicación
- ✓ Microservicios
- ✓ Información de la versión
- ✓ Atributos de aplicación
- Grupos de usuarios**
- Resumen

Seleccione grupos que deberían tener acceso a esta aplicación.

	NOMBRE DEL GRUPO	USUARIOS ASIGNADOS
☐	17.3	1
☐	test group 1	3

ATRÁS

SIGUIENTE

GUARDAR

15. Haga clic en **Siguiente**.

16. En la página **Resumen**, revise la configuración de la aplicación.

Crear aplicación



✓ Detalles de la aplicación

✓ Microservicios

✓ Información de la versión

✓ Atributos de aplicación

✓ Grupos de usuarios

Resumen

Detalles de la aplicación

Nombre de la aplicación

Microservice App

Importancia para el negocio

Bajo

Descripción de aplicación

(ninguno)

Tipo de aplicación

Web/Cliente pesado

Aplicación de microservicios

Sí

Notificaciones de correo electrónico

(ninguno)

Atributos de aplicación

Información de la versión

Nombre de la versión

V1

Estado de SDLC

Desarrollo

Microservicio

M1

Propietario

User, Test

Descripción de la versión

(ninguno)

Grupos de usuarios

Grupos seleccionados

(ninguno)

ATRÁS

SIGUIENTE

GUARDAR

17. Haga clic en **Crear aplicación**.

Se le redirigirá a la página Información general de la versión de su aplicación nueva.

1.4.2.2. Visualización de los detalles de la aplicación

La página Información general de la aplicación muestra información general de la aplicación y sus versiones. Cumple la función de panel de la aplicación, y ofrece así un resumen rápido e integral del riesgo de seguridad de producción de la aplicación. En ella podrá filtrar las versiones de la aplicación, buscar versiones concretas, crear nuevas versiones e iniciar análisis.

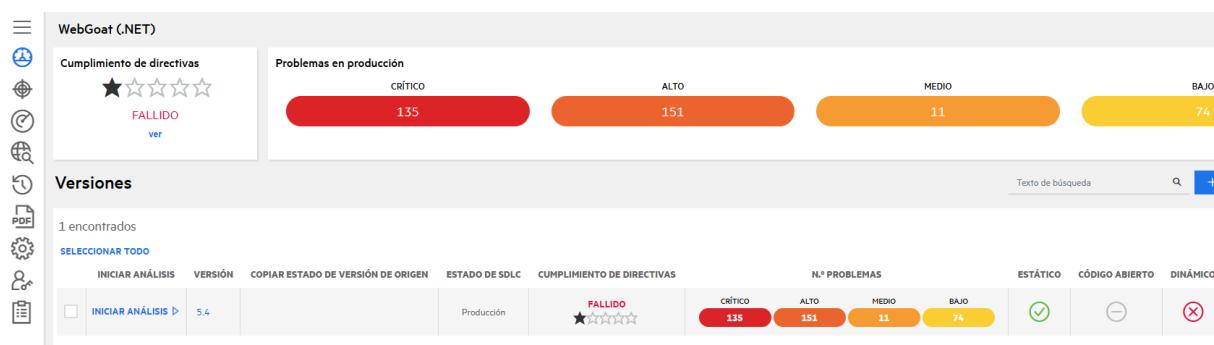
Para ver los detalles de una aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación que desea ver.

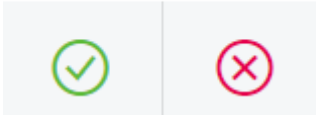
Aparecerá la página Información general de la aplicación. En la página, se muestran los siguientes detalles sobre la aplicación: riesgo de producción y cumplimiento de directivas, estado de seguridad y lista de versiones asociadas (ordenadas de forma predeterminada por fecha de último análisis completado, de más reciente a más antigua).



1.4.2.2.1. Desplazamiento por la página Información general de la aplicación

En la siguiente tabla, se describe cómo desplazarse por la página Información general de la aplicación.

Tarea	Acción
Ver la directiva de seguridad aplicada a la aplicación	Haga clic en Ver en el cuadro Cumplimiento de directivas.
Ver métricas combinadas en las versiones de producción de la aplicación	Los cuadros Cumplimiento de directivas y Problemas en producción muestran la clasificación por estrellas combinada y la cantidad de problemas en las versiones de producción de una aplicación. Haga clic en Crítico , Alto , Medio o Bajo para ver los detalles de los problemas por prioridad. También puede buscar un problema por su id. de instancia específico en la página Problemas de la aplicación.
Ver el estado de seguridad de la aplicación	El cuadro Estado de seguridad muestra el estado de seguridad de la aplicación.
Buscar las versiones de la aplicación	Introduzca la palabra de búsqueda en el cuadro de texto.
Crear una versión	Haga clic en + Nueva versión .
Iniciar un análisis	Haga clic en Iniciar análisis junto a una versión y seleccione el tipo de análisis. El botón está deshabilitado para las versiones con el estado de SDLC Retirado .
Ver detalles adicionales de la versión	Haga clic en el nombre de la versión.
Ver datos que forman parte de un gráfico	Haga clic en una sección del gráfico.

Tarea	Acción
Ver los estados de análisis más recientes de una versión	Coloque el cursor sobre el icono de estado relevante. Haga clic en él para acceder directamente a los detalles del estado del análisis. ESTÁTICO DINÁMICO  • Los análisis programados muestran la fecha de inicio programada. • La fecha de finalización se calcula sumando la fecha de inicio, el SLO del tipo de evaluación elegido, el periodo de pausa y los fines de semana. En caso de que un análisis se realice después del SLO, la fecha de finalización prevista mostrará un mensaje que indica: "Análisis de larga ejecución en <versión>. Póngase en contacto con nosotros para obtener más información".
Expandir o contraer filtros	Haga clic en expandir todo contraer todo  o en la flecha junto al nombre del filtro.
Mostrar u ocultar la lista de filtros	Haga clic en  .
Quitar los filtros aplicados	Haga clic en X o en X Borrar filtros .

1.4.2.2.2. Filtrado de la página

Información general de la aplicación

De forma predeterminada, la página Información general de la aplicación muestra todos los resultados. Puede personalizar los datos mostrados aplicando filtros.



Note

Un filtro aparece en la lista de filtros solamente cuando los resultados contienen varios valores para ese filtro.

Para filtrar la página Información general de la aplicación:

1. Haga clic en ▼ para mostrar la lista de filtros si no está abierta aún.
2. Expanda los filtros que desee aplicar.
3. Seleccione los valores de filtro. La siguiente tabla describe los filtros de la página Información general de la aplicación.

Filtro	Descripción	Valores
Estado de análisis dinámico	Estado de análisis dinámicos	Completado, Cancelado, En curso, No iniciado
Estado del análisis móvil	Estado del análisis móvil	Completado, Cancelado, En curso, No iniciado
Aprobar/Suspender	Clasificación Aprobar/Suspender definida por el usuario	Suspender, Aprobar
Fecha de creación de la versión	Fecha de creación de la versión	
Tipo de análisis	Tipo de análisis.	Estático, Dinámico, Móvil, Red, Código abierto
Estado de SDLC	Estado de SDLC de las versiones	Desarrollo, Control de calidad/Prueba, Producción, Retirada
Clasificación por estrellas	Sistema de clasificación de 5 estrellas	1, 2, 3, 4, 5
Estado del análisis estático	Estado de análisis estáticos	Completado, Cancelado, En curso, No iniciado

La página se actualizará automáticamente con los resultados filtrados. Los filtros aplicados se muestran en la parte superior de la página.

1.4.2.3. Edición de ajustes de aplicación

Puede editar la configuración de la aplicación después de crearla.

Para editar la configuración de la aplicación:

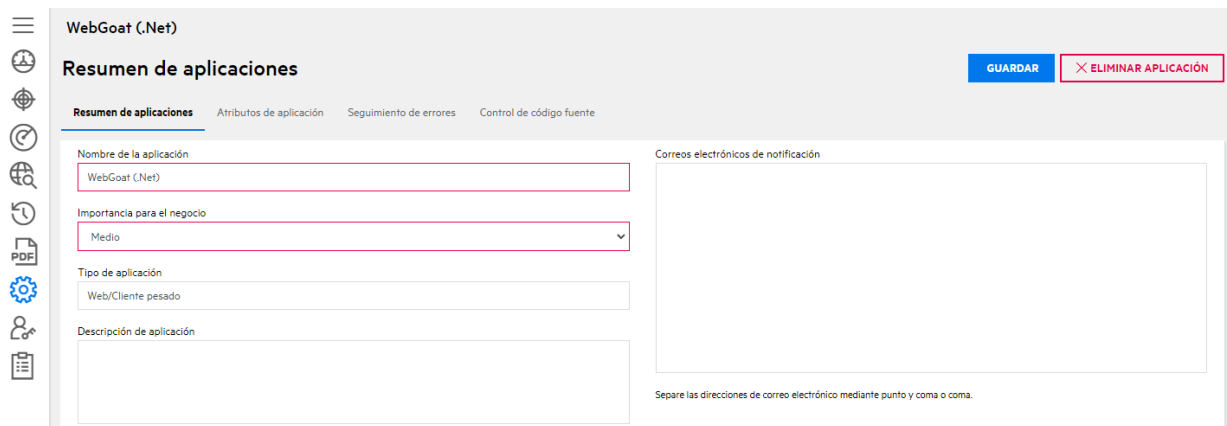
1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación que desee editar.

3. Haga clic en **Configuración**.

Aparecerá la página Configuración.



The screenshot displays the 'WebGoat (.Net)' application configuration interface. On the left is a sidebar with various icons. The main content area is titled 'WebGoat (.Net)' and 'Resumen de aplicaciones'. It features a navigation bar with tabs: 'Resumen de aplicaciones' (selected), 'Atributos de aplicación', 'Seguimiento de errores', and 'Control de código fuente'. The configuration form includes the following fields:

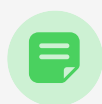
- Nombre de la aplicación:** A text input field containing 'WebGoat (.Net)'.
- Importancia para el negocio:** A dropdown menu currently set to 'Medio'.
- Tipo de aplicación:** A text input field containing 'Web/Cliente pesado'.
- Descripción de aplicación:** A large text area for additional details.
- Correos electrónicos de notificación:** A large text area for specifying notification email addresses, with a note below stating 'Separe las direcciones de correo electrónico mediante punto y coma o coma.'

At the top right of the configuration area, there are two buttons: 'GUARDAR' (Save) and 'X ELIMINAR APLICACIÓN' (Delete Application).

4. Seleccione la pestaña que corresponda a la configuración de la aplicación que quiera editar.

Campo	Descripción
Nombre de la aplicación	Nombre de la aplicación
Importancia para el negocio	Nivel de importancia para el negocio
Tipo de aplicación	Tipo de aplicación (no se podrá editar para aplicaciones de microservicios)
Descripción de aplicación	(Opcional) Descripción de la aplicación que le ayudará a administrar varias aplicaciones.
Correos electrónicos adicionales	(Opcional) Direcciones de correo electrónico a las que se enviarán notificaciones sobre la actividad relacionada con la aplicación.

- La pestaña **Resumen de aplicaciones** muestra detalles de la aplicación.
- (Solo aplicaciones de microservicios) La pestaña **Microservicios** muestra los microservicios existentes. Puede agregar, editar o eliminar los microservicios, así como editar valores de atributos de microservicios.



Note

No puede eliminar los microservicios que estén vinculados con una versión.

☰

🔍

🌐

🔄

🔍

🕒

📄

⚙️

👤

📋

Test App1_Microservice

Resumen de aplicaciones

Microservicios

Atributos de aplicación

Seguimiento de errores

Control de código fuente

✖ ELIMINAR APLICACIÓN

+ AGREGAR

NOMBRE DE MICROSERVICIO

M1	EDITAR
M2	EDITAR ELIMINAR
M3	EDITAR ELIMINAR
M4	EDITAR ELIMINAR

- La pestaña **Atributos de aplicación** muestra los atributos del sistema, así como los atributos personalizados.

- La pestaña **Seguimiento de errores** muestra los parámetros de configuración para la integración del seguimiento de errores. Para obtener más información, consulte [Integración con el seguimiento de errores](#).
 - La pestaña **Application Defender** muestra los parámetros de configuración para la integración de Application Defender. Para obtener más información, consulte Integración de Fortify Application Defender.
 - La pestaña **Control de código fuente** muestra los parámetros de configuración para la integración del control de código fuente. Para obtener más información, consulte [Integración de control de código fuente](#).
5. Edite la configuración de la aplicación como desee.
 6. Haga clic en **Guardar**.

Se guardarán los parámetros de configuración de la aplicación.

1.4.2.4. Administración de la asignación de usuarios a una aplicación

Los usuarios con el permiso **Administrar usuarios** pueden administrar el acceso de un usuario a una aplicación específica en el nivel de la aplicación.



Note

Los líderes en seguridad tienen acceso a todas las aplicaciones y ese acceso no se puede eliminar.

Para administrar el acceso de los usuarios a una aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación para que desea editar el acceso del usuario.

Aparecerá la página Versiones de la aplicación.

3. Haga clic en **Acceso**.

Aparecerá la página Usuarios con acceso a las aplicaciones con la lista de los usuarios que tienen acceso a la aplicación.

17.4 Static Application				
Usuarios con acceso a las aplicaciones				
Texto de búsqueda				
1 encontrados				
Mostrar: 25 50 100				
APELLIDO ^	NOMBRE	CORREO ELECTRÓNICO	ROL	MÉTODO DE ACCESO
User	Test	test_user02@h.com	Líder en seguridad	Rol

4. Haga clic en **Editar usuarios**.

Aparecerá la ventana Asignar usuarios.

5. Puede realizar las siguientes tareas:

Tarea	Procedimiento
Asignar usuarios a la aplicación	- Haga clic en Editar usuarios. Aparecerá la ventana Asignar usuarios. - Seleccione la pestaña Disponible. - Realice las siguientes acciones para seleccionar usuarios: ■ Marque las casillas situadas junto a cada usuario. ■ Seleccione la casilla de verificación ASIGNAR para seleccionar los usuarios mostrados. ■ Marque la casilla Asignar todos los usuarios de inquilinos para seleccionar todos los usuarios. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones.

Tarea	Procedimiento
Quitar usuarios de la aplicación	- Haga clic en Editar usuarios. Aparecerá la ventana Asignar usuarios. - Seleccione la pestaña Seleccionados.  - Realice las siguientes acciones para quitar usuarios: - Desactive la casilla de verificación situada junto a cada usuario. - Desactive la casilla de verificación ASIGNAR para quitar los usuarios mostrados. - Seleccione la casilla de verificación Anular las asignaciones de todos los usuarios de inquilinos para quitar todos los usuarios. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones.

Tarea	Procedimiento

6. Haga clic en **Guardar**.

Se guardan los cambios de los usuarios asignados a la aplicación.

Temas relacionados:

Para administrar el acceso de los usuarios a las aplicaciones a nivel de usuario, consulte [Administrar la asignación de aplicaciones para un usuario](#).

1.4.2.5. Visualización del registro de eventos de aplicaciones

Los usuarios con el permiso **Administrar aplicaciones** pueden ver el registro de eventos de una aplicación. El registro de eventos de una aplicación registra todos los eventos relacionados con la aplicación:

- creación, actualización y eliminación de aplicaciones
- creación, actualización y eliminación de versiones
- adición y eliminación del acceso de grupos y usuarios a la aplicación
- iniciación, actualización y finalización de análisis
- uso de derechos
- creación, publicación, descarga y eliminación de informes
- Descargas de FPR
- exportaciones de datos
- creación, actualización y eliminación de configuraciones de auditoría avanzadas

Para ver el registro de eventos de una aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación cuyo registro de eventos desee ver.

3. Haga clic en **Registro de eventos**.

Aparecerá la página Registro de eventos.

WebGoat (.NET)

Registro de eventos ⓘ

Texto de búsqueda 🔍 **EXPORTAR** ▼

FECHA DEL EVENTO DESDE: 2022/11/28 X FECHA DEL EVENTO HASTA: 2022/11/29 X BORRAR FILTROS expandir todo | contraer todo

2 encontrados Mostrar: 25 50 100

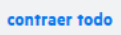
FECHA DEL EVENTO	TIPO	USUARIO	NOTAS
2022/11/29 07:27:09	Proyecto actualizado	HuangTam	ApplicationName = "WebGoat (.NET)"; ApplicationType = "Web/Thick-Client"; ApplicationBusinessCriticality = "1"; ApplicationRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Applications/4521"; Origin = "WebUI"
2022/11/29 07:26:43	Proyecto actualizado	HuangTam	ApplicationName = "WebGoat (.NET)"; ApplicationType = "Web/Thick-Client"; ApplicationBusinessCriticality = "1"; ApplicationRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Applications/4521"; Origin = "WebUI"

FECHA DEL EVENTO

De: 2022/11/28

Para: 2022/11/29

4. Puede realizar las siguientes tareas:

Tarea	Acción
Exportar el registro de eventos de los últimos 13 meses	Haga clic en Exportar . El archivo .csv se guarda en forma local en la carpeta especificada en la configuración del navegador.
Buscar en el registro de eventos	Escriba una palabra clave o una frase en el campo de texto de búsqueda y pulse Intro .
Mostrar u ocultar la lista de filtros	Haga clic en  .
Expandir o contraer filtros	Haga clic en    o en la flecha junto al nombre del filtro.
Quitar los filtros aplicados	Haga clic en X o en Borrar filtros en la parte superior de la página. El filtro está configurado para las últimas 24 horas de forma predeterminada.

Temas relacionados

Para obtener información sobre cómo ver los eventos que se producen en su portal, consulte [Acceso al registro de eventos de administración](#).

1.4.2.6. Eliminación de una aplicación

Al eliminar una aplicación, también se eliminarán todos los datos relacionados con ella, lo cual no se puede deshacer. Los datos de la aplicación se purgan desde OpenText Core Application Security después de 72 horas. Si una aplicación se eliminó por error, comuníquese con el soporte dentro de las 72 horas de haberla eliminado.



Note

Si necesita reutilizar el nombre de una aplicación eliminada, espere 72 horas después de la eliminación antes de crear una aplicación nueva.

Para eliminar una aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página **Sus aplicaciones**.

2. Haga clic en la aplicación que desea eliminar.

3. Haga clic en **Configuración**.

Aparecerá la página **Resumen de aplicaciones**.

The screenshot shows the 'Resumen de aplicaciones' page for 'WebGoat (.Net)'. The page has a sidebar on the left with navigation icons. The main content area has a header with 'WebGoat (.Net)' and 'Resumen de aplicaciones'. Below the header, there are tabs: 'Resumen de aplicaciones', 'Atributos de aplicación', 'Seguimiento de errores', and 'Control de código fuente'. The 'Resumen de aplicaciones' tab is active. It contains several form fields: 'Nombre de la aplicación' (WebGoat (.Net)), 'Importancia para el negocio' (Medio), 'Tipo de aplicación' (Web/Cliente pesado), and 'Descripción de aplicación'. There is also a section for 'Correos electrónicos de notificación' with a text area and a note: 'Separe las direcciones de correo electrónico mediante punto y coma o coma.' At the top right, there are two buttons: 'GUARDAR' (Save) and 'X ELIMINAR APLICACIÓN' (Delete Application).

4. Haga clic en **X Eliminar aplicación**.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí** para eliminar la aplicación.

Se le redirigirá a la página **Sus aplicaciones**.

1.4.3. Administración de una versión

Puede crear, visualizar y editar las versiones según sus permisos de usuario.

Esta sección aborda los siguientes temas:

- [Creación de una versión](#)
- [Visualización de los detalles de la versión](#)
- [Reemplazo de la directiva de seguridad de una versión](#)
- [Edición de la configuración de la versión](#)
- [Eliminación de una versión](#)

1.4.3.1. Creación de una versión

Puede crear una nueva versión para una aplicación existente. Cuando cree una versión nueva, tendrá la opción de empezar desde cero o de conservar las vulnerabilidades y otros detalles de una versión anterior.

Para crear una nueva versión:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en la aplicación para la que desea crear una nueva versión.

3. Haga clic en **+ Nueva versión**.

Aparece el asistente para crear versiones.

Create a Release

Release Details

Release Name

Release Description

SDLC Status

(Choose One) ▼

Release Attributes

RelAttr

(Choose One) ▼

☒ Copy State from Existing Release

NEXT

4. En la página **Información de la versión**, complete los campos necesarios. Los siguientes campos son obligatorios a menos que se indique lo contrario:

Campo	Descripción
Nombre de la versión	Escriba el nombre de su versión.
Descripción de la versión	(Opcional) Escriba una descripción que ofrezca información sobre la versión.
Estado de SDLC	Seleccione la etapa del ciclo de vida de desarrollo del software de la versión: Desarrollo, Control de calidad/Prueba, Producción . La opción Retirado no está disponible.
Atributos de versión	Especifique los atributos de la versión.
Microservicio (solo aplicaciones de microservicios)	En la lista desplegable, seleccione el microservicio que se vinculará con la versión. Una versión debe vincularse con un microservicio; un microservicio puede vincularse con varias versiones.

Campo	Descripción
Copiar estado desde una versión existente	(Opcional, seleccionado de forma predeterminada) Active Copiar estado desde la versión existente para conservar los datos de una versión anterior en la versión nueva. Se copian los siguientes datos: propietario de la versión, configuración de análisis para todos los tipos de análisis, clasificación por estrellas, recuento de problemas y detalles del problema (incluido el historial de problemas, los enlaces de seguimiento de errores y las capturas de pantalla adjuntas). Note Se copian los datos de los análisis completados e importados. Los datos de los análisis en pausa y en curso, incluida la configuración del análisis, no se copian. Los problemas con soluciones validadas no se copian.

5. Si ha activado **Copiar estado desde la versión existente**, haga clic en **Siguiente**. De lo contrario, vaya al paso [7](#).

Crear una versión

Copiar estado desde la versión existente

2 encontrados

Mostrar: 25 **50** 100

	NOMBRE DE LA VERSIÓN	ESTADO DE SDLC
☐	1	Producción
☐	2	Producción

☐ Retirar versión seleccionada

Texto de búsqueda

Q X

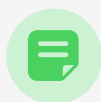
ATRÁS

GUARDAR

6. En la página **Copiar estado desde la versión existente**, seleccione la versión de la que desee transferir las vulnerabilidades y otra información de la lista.

7. Haga clic en **Guardar**.

Se le redirigirá a la página Información general de la versión nueva.



Note

Si eligió copiar los datos desde una versión anterior, el proceso de copia de datos de la versión puede demorar la actualización de la pantalla, por lo que es posible que no vea la página Información general de inmediato.

1.4.3.2. Visualización de los detalles de la versión

La página Información general de la versión muestra un panel con información general sobre la versión y ofrece un resumen rápido e integral sobre la seguridad de la versión. Gracias a una serie de imágenes fáciles de interpretar, podrá ver las métricas clave relacionadas con su versión. Es posible hacer clic en muchos de los elementos visuales para obtener detalles adicionales sobre los conjuntos de datos mostrados.

Para ver los detalles de una versión:

1. Seleccione la vista **Aplicaciones**.

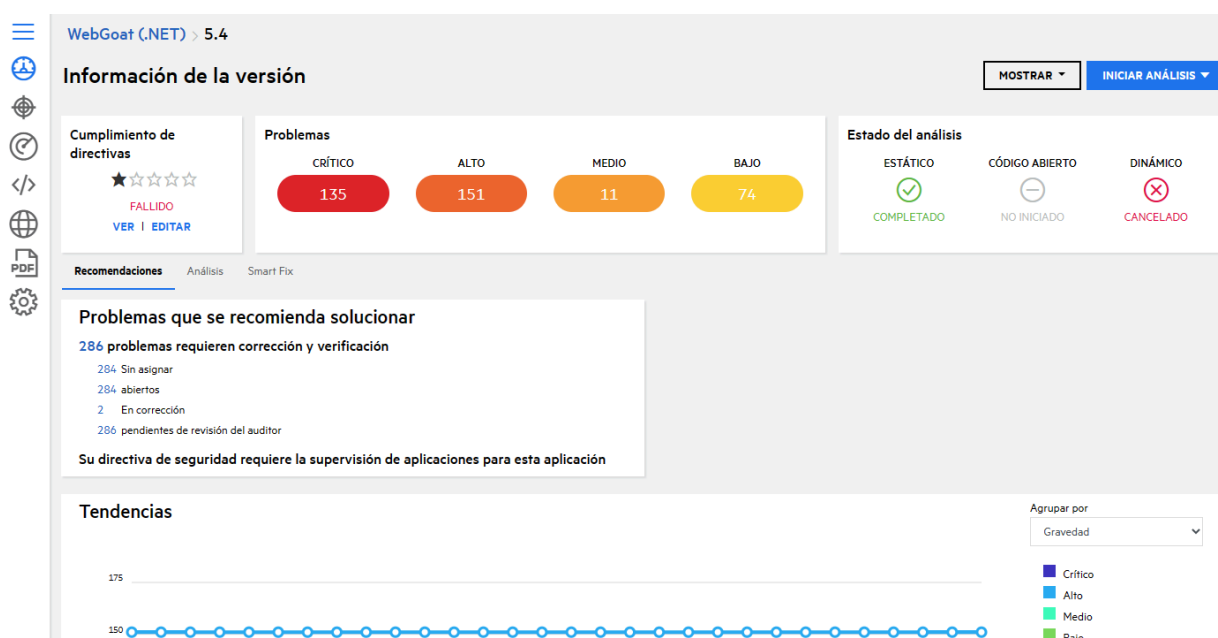
Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

3. Haga clic en el nombre de la versión que desea ver.

Aparecerá la página Información general de versión.



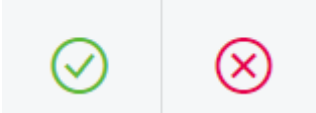
En la sección superior de la página Información general de versión, se resumen los resultados del análisis de la versión.

- El cuadro Cumplimiento de directivas muestra la Clasificación por estrellas y el estado de Aprobados/Fallidos.

- El cuadro Problemas enumera las vulnerabilidades de cada nivel de gravedad. Haga clic en **Crítico**, **Alto**, **Medio** o **Bajo** para ver los detalles de los problemas por prioridad. También puede buscar un problema por su **id. de instancia** específico en la página Problemas de versión.
- El cuadro Estado del análisis muestra los estados de análisis más recientes de la versión.
- Las pestañas muestran representaciones visuales de los resultados del análisis e incluyen vínculos para obtener más información sobre los problemas.

En la siguiente tabla, se describe cómo desplazarse por la página Información general de versión.

Tarea	Acción
Ver el origen del estado de la copia (si corresponde)	Haga clic en el vínculo debajo del nombre de la versión. Debricked Scan > AA 2.0 Información de la versión Copiado desde "Webgoat.net"
Mostrar u ocultar los problemas solucionados	Seleccione Mostrar > Solucionados para mostrar y ocultar los problemas con el estado Solución validados.
Mostrar u ocultar los problemas suprimidos	Seleccione Mostrar > Suprimidos para mostrar y ocultar los problemas con el estado Falso positivo confirmado y Suprimido.
Iniciar un análisis	Haga clic en Iniciar análisis y seleccione el tipo de análisis de la lista. El botón está deshabilitado para las versiones con el estado de SDLC Retirado .
Ver la directiva de seguridad aplicada a la aplicación	Haga clic en Ver en el cuadro Cumplimiento de directivas.
Sobrescribir el cumplimiento de directivas	Haga clic en Editar en el cuadro Cumplimiento de directivas.

Tarea	Acción
Ver los estados de análisis más recientes de la versión	Coloque el cursor sobre el icono de estado relevante. Haga clic en él para acceder directamente a los detalles del estado del análisis. ESTÁTICO DINÁMICO  - Los análisis programados muestran la fecha de inicio programada. - La fecha de finalización se calcula sumando la fecha de inicio, el SLO del tipo de evaluación elegido, el periodo de pausa y los fines de semana. En caso de que un análisis se realice después del SLO, la fecha de finalización prevista mostrará un mensaje que indica: "Análisis de larga ejecución en <versión>. Póngase en contacto con nosotros para obtener más información".
Detalles sobre los problemas filtrados por gravedad del problema o por tipo de análisis	Haga clic en los elementos visuales en los recuadros Problema y Estado del análisis.
Seleccione una representación visual de los resultados del análisis para un análisis más detallado.	Seleccione una pestaña. Para obtener más información, consulte Gráficos de información general de la versión.

1.4.3.2.1. Gráficos de información general de la versión

Las pestañas de la página Información general de versión muestran representaciones gráficas de los resultados del análisis con vínculos para obtener detalles adicionales de los problemas

- [Recomendaciones](#)
- [Análisis](#)
- [Smart Fix \(análisis estáticos\)](#)
- [Información de la aplicación \(análisis móviles\)](#)
- [Reputación \(análisis móviles\)](#)



Note

Mostrar los problemas solucionados y suprimidos aumenta la cantidad de vulnerabilidades en el recuento. El recuento actualizado también se reflejará en los gráficos de vulnerabilidad.

Recomendaciones

La sección **Problemas que se recomienda solucionar** indica por qué la versión no cumple la directiva de seguridad. Si existen problemas específicos que impiden que la versión cumpla los requisitos, puede examinar directamente los detalles de esos problemas. Si su política requiere una frecuencia de análisis mínima, esta información también se mostrará aquí. Las versiones aprobadas, pero que no tienen requisitos de frecuencia de análisis, no tendrán esta sección.

Recomendaciones
Análisis
Smart Fix

Problemas que se recomienda solucionar

286 problemas requieren corrección y verificación

- 284 Sin asignar
- 284 abiertos
- 2 En corrección
- 286 pendientes de revisión del auditor

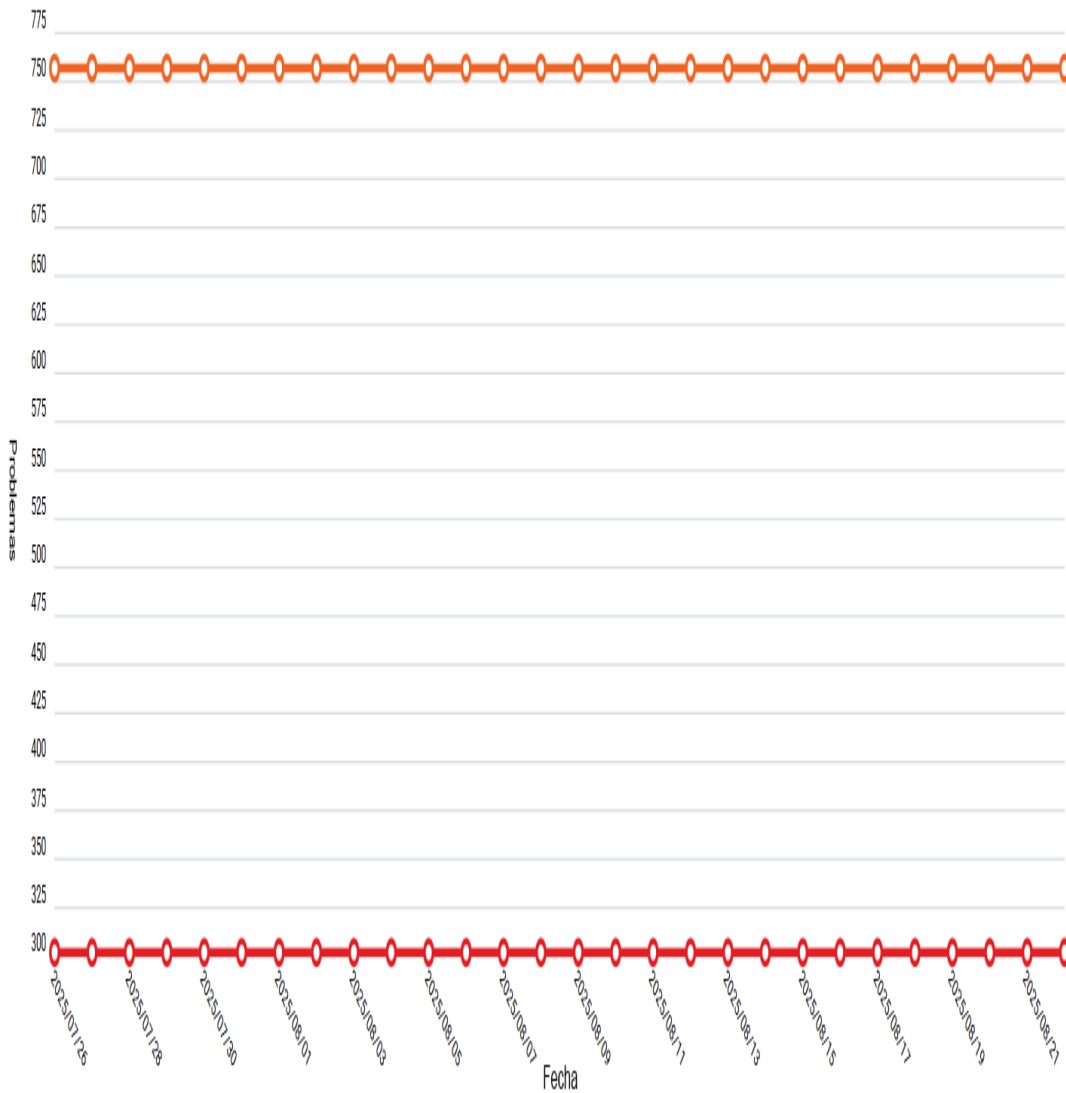
Su directiva de seguridad requiere la supervisión de aplicaciones para esta aplicación

La sección **Tendencias** muestra un gráfico de líneas de las tendencias de vulnerabilidad de la versión a lo largo del tiempo, medidas en términos de la faceta seleccionada. Coloque el cursor sobre un punto de datos para ver el recuento y tipo. Haga clic en una etiqueta para alternar entre mostrar u ocultar los conjuntos de datos.

Tendencias

Agrupar por

Gravedad



Faceta	Descripción
Estado del auditor	Estado del auditor de los problemas
Top 25 de CWE 2023	Clasificación de las 25 principales debilidades comunes
Estado del desarrollador	Estado del desarrollador de los problemas
FISMA (obsoleto)	Clasificación de FISMA
RGPD	Clasificación del RGPD de Fortify Software Security Research (SSR)
Asignado	Estado de la asignación de los problemas: Falso y Verdadero
Cerrado	Estado de la resolución de los problemas: Falso y Verdadero
Estado del problema	Estado del problema: Nuevo, Existente, Reabierto y Solucionado
Se ha suprimido	Estado de la supresión de los problemas: Falso y Verdadero
Kingdom	Clasificación Siete reinos perniciosos
NIST SP 800-53 Rev 5	Publicación especial 800-53 del Instituto Nacional de Estándares y Tecnología
OWASP ASVS 4.0	Clasificación OWASP ASVS 4.0
OWASP ASVS 5.0	Clasificación OWASP ASVS 5.0
OWASP 2017	Clasificación según el Top 10 de OWASP 2017

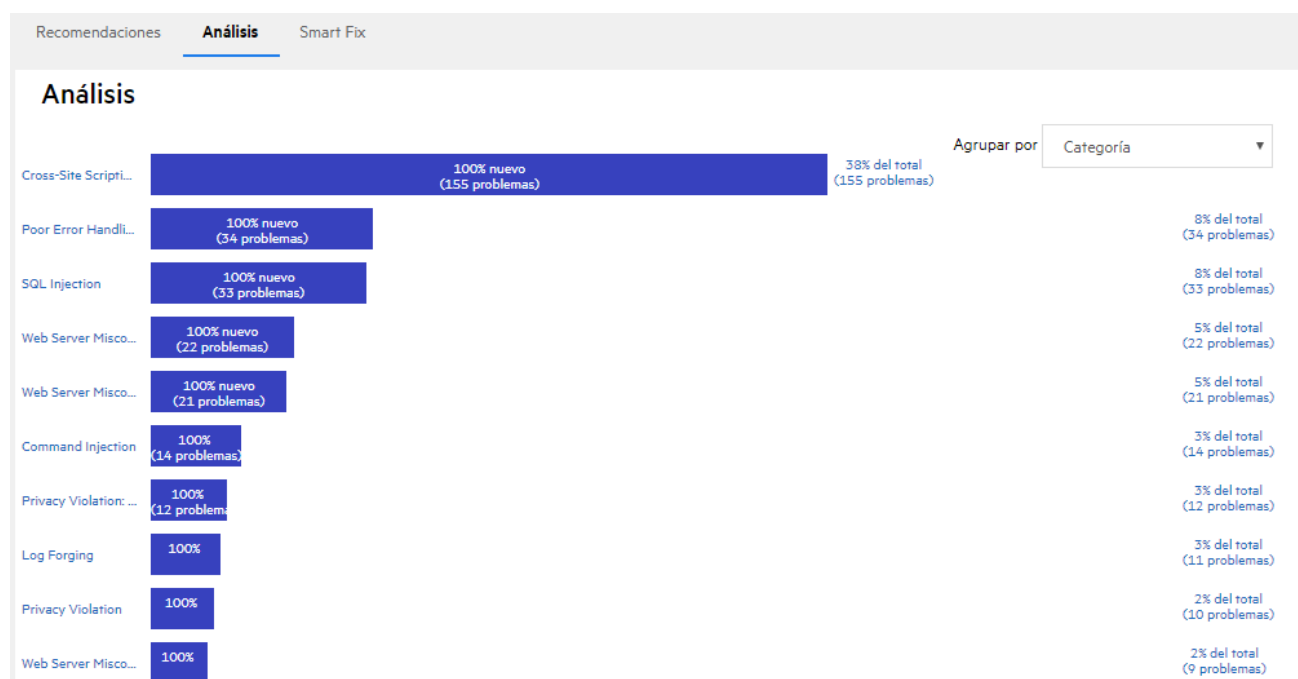
Faceta	Descripción
OWASP 2021	Clasificación según el Top 10 de OWASP 2021
OSWAP 2023	Clasificación OWASP API Top 10 2023
OWASP 2014 Mobile Top 10, OWASP 2024 Mobile Top 10	Clasificación OWASP Mobile Top 10
PCI40	Clasificación de PCI 4.0
PCIDSS401	Clasificación de PCI 4.0.1
PCISSF12	PCI SSF versión 1.2
Tipo de análisis	Tipo de problema de análisis: Estático, Dinámico, Móvil
Gravedad	Gravedad del problema: Crítico, Alto, Medio, Bajo
STIG52	Clasificación DISA STIG 5.2
STIG53	Clasificación DISA STIG 5.3
STIG61	Clasificación DISA STIG 6.1
STIG62	Clasificación DISA STIG 6.2
STIG63	Clasificación DISA STIG 6.3

Análisis

La pestaña **Análisis** muestra un gráfico de barras de las vulnerabilidades de la versión divididas por grupos. Las categorías mostradas dependen de la faceta de agregación seleccionada: **Asignación, Estado del auditor, Categoría, Estado del desarrollador, Tipo de Análisis y OWASP 13**.

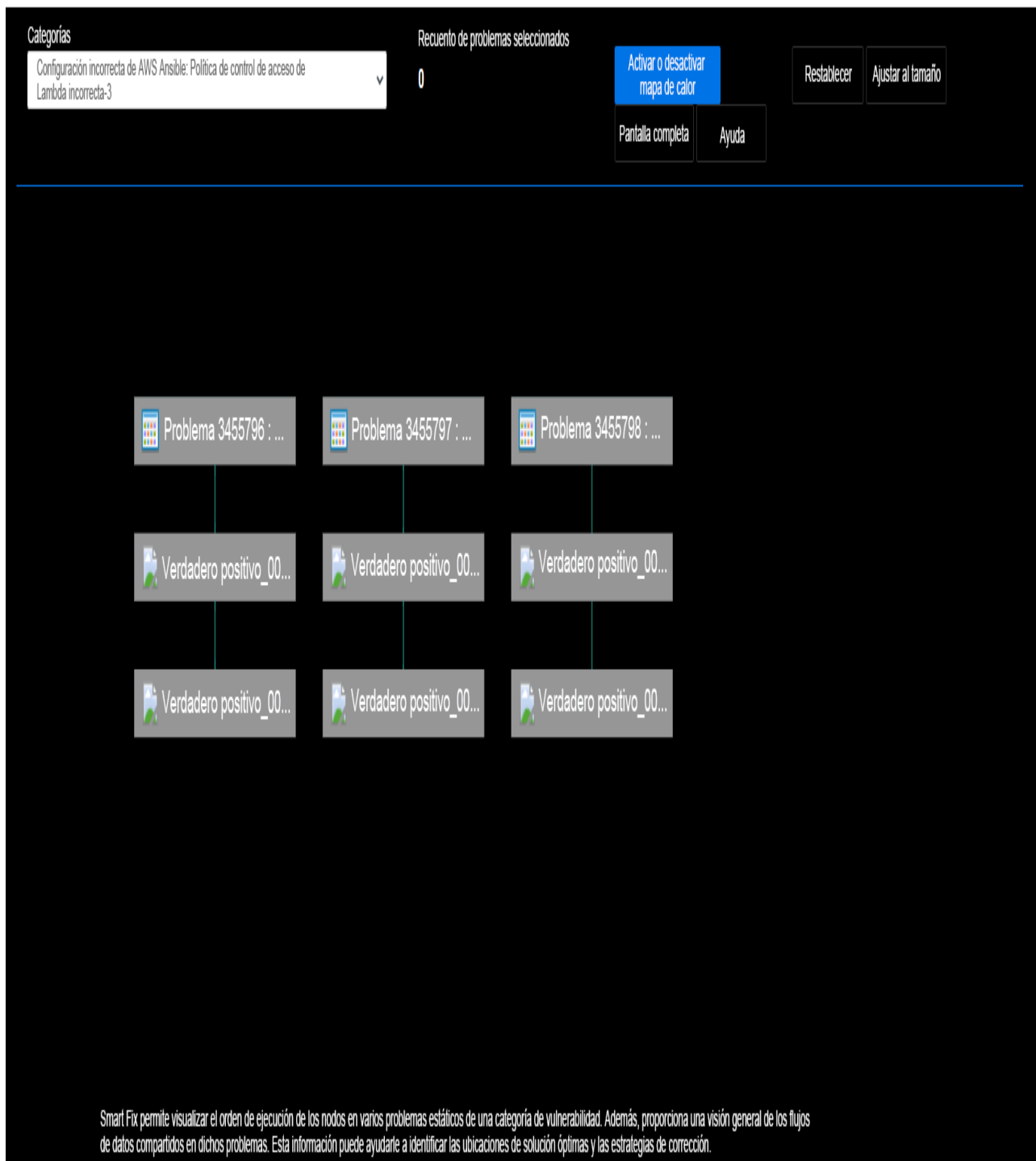
Para profundizar en un grupo, haga clic en cualquiera de las barras del gráfico. Por ejemplo, si hace clic en la barra **que representa las infracciones de seguridad** de la

faceta **Categoría**, se le redirigirá a la página filtrada Problemas, en la que se muestran las vulnerabilidades relacionadas con infracciones de privacidad.



Smart Fix (análisis estáticos)

La pestaña **Smart Fix** está disponible en cuanto se realiza un análisis estático. Muestra un diagrama de seguimiento de análisis donde se visualiza el orden de ejecución de los nodos en problemas estáticos de una categoría de vulnerabilidad y se proporciona información de los flujos de datos compartidos por dichos problemas. Esta información puede ayudarle a identificar las ubicaciones de solución óptimas y las estrategias de corrección.



Seleccione una categoría de vulnerabilidad en la lista **Categorías** para ver su diagrama del seguimiento de análisis. Puede interactuar con el diagrama de las siguientes formas:

- Desplácese hacia arriba y hacia abajo para acercarse y alejarse, según corresponda.
- Haga clic en un nodo para resaltar las rutas compartidas.
- Haga clic en un icono de problema para obtener detalles adicionales..

- Manipule el diagrama usando los comandos de la barra de herramientas:
 - **Activar o desactivar mapa de calor:** activa o desactiva que los flujos de datos aparezcan resaltados.
 - **Recortar** (disponible al seleccionar un nodo): limita el diagrama al flujo de datos combinado de los problemas seleccionados.
 - **Restablecer:** se restablece el diagrama a la vista predeterminada de la categoría de problema seleccionada.
 - **Ajustar al tamaño:** cambia el tamaño de todo el diagrama de manera que se ajuste a la pantalla sin tener que restablecerlo o recortarlo.
 - **Pantalla completa:** amplía el diagrama al modo de pantalla completa.

Información de la aplicación (análisis móviles)

La pestaña **Información de la aplicación** muestra la siguiente información sobre un archivo binario de una aplicación móvil: la plataforma, el nombre de la aplicación, el identificador (nombre del paquete), la versión, el tamaño de archivo, los requisitos mínimos del sistema operativo y los requisitos del dispositivo.

Reputación (análisis móviles)

El servicio de reputación móvil de OpenText Core Application Security realiza un análisis de reputación de los extremos de tráfico detectados al probar una aplicación móvil. En la pestaña **Reputación** se muestran los resultados del análisis. En ella se detallan todos los hosts identificados y se especifican los que se encuentran en buena posición. Los resultados de los análisis móviles también incluyen las vulnerabilidades dedicadas para los hosts identificados en mala posición.

Recomendaciones Análisis Tendencias **Reputación**

NOMBRE DEL HOST	BUENA POSICIÓN
http://%@ordn.playkidsapp.com/	✓
http://%@rdn.playkidsapp.com/	✓
http://127.0.0.1:%d/	✓
http://adlog.flurry.com/	✓
http://ads.flurry.com/	✓
http://br.ordn.playkidsapp.com/	✓
http://data.flurry.com/	✓
http://id.loc.gov/	✓
http://idpf.org/	✓

1.4.3.3. Reemplazo de la directiva de seguridad de una versión

Los líderes en seguridad pueden reemplazar de forma manual la directiva de seguridad de una versión configurándola como aprobada o suspendida. Esta capacidad permite reflejar mejor el proceso de excepción del mundo real en el portal, sin necesidad de suprimir los problemas de forma artificial. La justificación de la excepción aparece en el registro de eventos de la aplicación. El estado de la versión revierte automáticamente a la directiva oficial de seguridad en el siguiente análisis.

Para reemplazar la directiva de seguridad de una versión:

1. Seleccione la vista **Aplicaciones**.

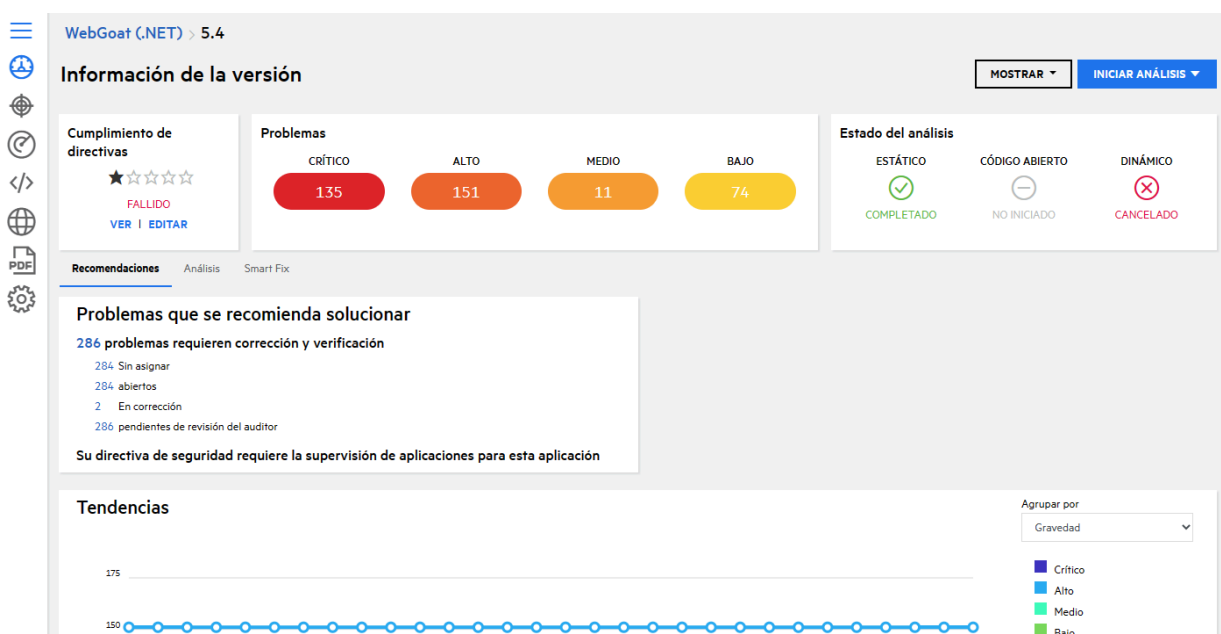
Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación que contenga la versión que desee editar.

Aparecerá la página Información general de la aplicación.

3. Haga clic en el nombre de la versión para la cual desee reemplazar la directiva de seguridad.

Aparecerá la página Información general de versión.



4. Haga clic en **Editar** en el cuadro Cumplimiento de directivas.

Se muestra la ventana modal Reemplazo de cumplimiento.

5. Escriba la justificación para el cambio de los resultados de cumplimiento de directivas en el campo.

Reemplazo de cumplimiento



Escriba un comentario para definir el estado de cumplimiento de esta versión de forma manual.

ESTABLECER COMO APROBADO

ESTABLECER COMO FALLIDO

CANCELAR

6. Haga clic en **Establecer como Aprobado** o en **Establecer como Error**.

Se le redirigirá a la página Información general de versión. El reemplazo de la directiva se mostrará en el cuadro Cumplimiento de directivas.

Temas relacionados:

- Para obtener información sobre las clasificaciones por estrellas, consulte [Clasificación de la evaluación de cinco estrellas](#).
- Para obtener información sobre la administración de directivas de seguridad, consulte [Administración de directivas](#).

1.4.3.4. Edición de la configuración de la versión

Puede editar la configuración de la versión después de crearla.

Para editar la configuración de la versión:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Se mostrará la página Sus versiones con una lista de sus versiones.

3. Seleccione la versión que desea editar.

4. Haga clic en **Configuración**.

Aparecerá la página Resumen de versiones.



The screenshot shows a web interface for managing application versions. On the left is a sidebar with icons for navigation. The main content area is titled '17.4 Static Application' and 'Resumen de versiones'. It contains several form fields: 'Nombre de la versión' (Version Name) with the value '2', 'Estado de SDLC' (SDLC State) with a dropdown menu showing 'Producción' (Production), and 'Propietario' (Owner) with a dropdown menu showing '(Elija uno)' (Choose one). There is also a large text area for 'Descripción de la versión' (Version Description). At the top right of the form area are two buttons: 'GUARDAR' (Save) and 'ELIMINAR VERSIÓN' (Delete Version).

5. Edite la página Resumen de versiones como desee. Todos los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Nombre de la versión	Nombre de la versión
Microservicio	(Solo aplicaciones de microservicios) Nombre del microservicio vinculado con la versión
Estado de SDLC	Etapas del ciclo de vida de desarrollo del software de la versión
Propietario	Propietario de la versión que recibe notificaciones por correo electrónico de las actualizaciones de estado del análisis de la versión

Campo	Descripción
Ejecutar análisis de código abierto con Debricked	(Disponible para inquilinos con derechos de Sonatype) Seleccione la casilla de verificación para cambiar la herramienta de análisis de composición de software de Sonatype a OpenText Core SCA. La configuración no se puede revertir una vez que se ha guardado. El inquilino debe tener derechos activos de OpenText Core SCA para ejecutar correctamente los análisis de OpenText Core SCA después del cambio.  Note Si su inquilino tiene derechos de Sonatype inactivos y derechos activos de OpenText Core SCA, sus análisis de código abierto funcionan con OpenText Core SCA.
Descripción de la versión	(Opcional) La descripción de la versión que ofrece información sobre ella.

6. Haga clic en **Guardar** para guardar los cambios.

1.4.3.5. Eliminación de una versión

Los usuarios con el permiso **Crear aplicaciones** pueden eliminar una versión. Al eliminar una versión, también se eliminarán todos los datos relacionados con ella, lo cual no se puede deshacer. Los datos de la versión se purgan desde OpenText Core Application Security después de 72 horas. Si una versión se eliminó por error, comuníquese con el soporte dentro de las 72 horas de haberla eliminado.



Note

Si necesita reutilizar el nombre de una versión eliminada, espere 72 horas después de la eliminación antes de crear una versión nueva.

Para eliminar una versión:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Se mostrará la página Sus versiones con una lista de sus versiones.

3. Haga clic en la versión que desea eliminar.

4. Haga clic en **Configuración**.

5. Haga clic en **x Eliminar versión**.

6. Haga clic en **Sí**.

Se le redirigirá a la página Información general de versión.

1.4.4. Visualización de aplicaciones del inquilino

Puede revisar el estado de seguridad de varias aplicaciones simultáneamente. La página Sus aplicaciones es la página de destino predeterminada tras iniciar sesión en OpenText Core Application Security. Muestra información general de alto nivel de sus aplicaciones, centrándose en el riesgo y el cumplimiento de directivas de las versiones de producción.

Para ver la página Sus aplicaciones:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones. En la cuadrícula, se muestra la siguiente información de cada aplicación: nombre de la aplicación, número de versiones, importancia para el negocio, clasificación por estrellas combinada y cantidad de problemas detectados en las versiones de producción, así como el estado de análisis más reciente de todas las versiones y el cambio más relevante en relación al riesgo.

Sus aplicaciones

Texto de búsqueda

q

+ Nueva aplicación

10 encontrado

Mostrar: 2550100

expandir todo | contraer todo

Seleccionar todo

Ordenar

Riesgo de producción

Tipo de aplicación

Web/Cliente pesado

Móvil

Cambio más reciente

Tipo de análisis

Clasificación por estrellas

aplicar a todo lo seleccionado

	Nombre		Riesgo de producción y cumplimiento de directivas					Estado de seguridad y análisis				
☐	WebGoat (JAVA) 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 245	Alto 100	Medio 18	Bajo 21	Estático ✓	Código abierto ⊖	Dinámico ✓	Ataques (		
☐	Juice Shop 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 181	Alto 24	Medio 14	Bajo 23	Estático ✓	Código abierto ⊖	Dinámico ✓	Ataques (		
☐	Fortify-IWA (Java) 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 57	Alto 88	Medio 38	Bajo 67	Estático ✓	Código abierto ✓	Dinámico ✓	Ataques (		
☐	iGoat (Swift) 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 56	Alto 150	Medio 8	Bajo 70	Estático ✓	Código abierto ⊖	Dinámico ✓	Ataques (		
☐	Fortify-IWA (.Net) 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 51	Alto 59	Medio 138	Bajo 180	Estático ✓	Código abierto ✓	Dinámico ✓	Ataques (		
☐	Bricks 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 42	Alto 14	Medio 0	Bajo 2	Estático ✓	Código abierto ⊖	Dinámico ⊖	Ataques (		
☐	Go-Test-Bench 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 28	Alto 129	Medio 42	Bajo 3	Estático ✓	Código abierto ✓	Dinámico ⊖	Ataques (		
☐	CloudGoat (IaC) 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 7	Alto 6	Medio 4	Bajo 2	Estático ✓	Código abierto ⊖	Dinámico ⊖	Ataques (		
☐	WebGoat (.Net) 1 VERSIONES Importancia para el negocio: MEDIA	Suspender ★☆☆☆☆	Crítico 5	Alto 36	Medio 0	Bajo 5	Estático ✓	Código abierto ⊖	Dinámico ⊖	Ataques (		

1.4.4.1. Desplazamiento por la página Sus aplicaciones

En la siguiente tabla se describe cómo desplazarse por la página Sus aplicaciones.

Tarea	Acción
Creación de una aplicación	Haga clic en + Nueva aplicación .
Buscar en la lista de aplicaciones	Escriba una palabra clave o una frase en el cuadro de texto de búsqueda y pulse Intro. Para quitar los resultados de búsqueda, elimine el texto del cuadro de búsqueda y pulse Intro o quite el filtro aplicado. Para obtener más información sobre cómo usar el cuadro de texto de búsqueda, consulte Búsqueda de aplicaciones y versiones.
Mostrar u ocultar listas de filtros	Haga clic en  .
Expandir o contraer filtros	Haga clic en expandir todo o contraer todo en la flecha junto al nombre del filtro.
Aplicar filtros	Seleccione los valores de filtro deseados debajo del nombre del filtro. La página se actualizará automáticamente con los resultados filtrados. Para algunos filtros, haga clic en aplicar para actualizar la página.
Quitar los filtros aplicados	Haga clic en la X que se encuentra junto a cada filtro que se haya aplicado o haga clic en Borrar filtros .
Filtrar aplicaciones por designación de microservicio	Seleccione la pestaña que desee. Todo 12 Microservicio 0 No microservicio 12

Tarea	Acción
Editar atributos de aplicación para varias aplicaciones	1. Active la casilla que aparece junto a las aplicaciones individuales o haga clic en seleccionar todo para seleccionar todas las aplicaciones de la página. 2. Haga clic en Editar atributos. Se abrirá la ventana Editar atributo. Editar atributos (2 elementos) ✕ Importancia para el negocio (Elija uno) ▾ 11 GUARDAR CANCELAR 3. Actualice los campos según sea necesario. 4. Haga clic en Guardar. Para obtener más información sobre los atributos de aplicación, consulte Creación de una aplicación.

Tarea	Acción																		
Editar grupos de usuarios para varias aplicaciones	1. Active la casilla que aparece junto a las aplicaciones individuales o haga clic en seleccionar todo para seleccionar todas las aplicaciones de la página. 2. Haga clic en Editar grupos. Se abrirá la ventana Editar grupos. Editar grupos (2 elementos) ⓘ × Seleccione grupos que deberían tener acceso a las aplicaciones seleccionadas. Buscar <table><thead><tr><th></th><th>NOMBRE DEL GRUPO</th><th>USUARIOS ASIGNADOS</th></tr></thead><tbody><tr><td>☐</td><td>group 1</td><td>2</td></tr><tr><td>☐</td><td>group 2</td><td>0</td></tr><tr><td>☐</td><td>group 3</td><td>1</td></tr><tr><td>☐</td><td>group 4 empty</td><td>0</td></tr><tr><td>☐</td><td>group 5</td><td>1</td></tr></tbody></table> ADJUNTAR Y GUARDAR SOBRESCRIBIR Y GUARDAR CANCELAR 3. Seleccione los grupos que se asignarán a las aplicaciones. 4. Haga clic en Adjuntar y guardar para agregar los grupos seleccionados a los grupos asignados existentes, o bien haga clic en Sobrescribir y guardar para reemplazar los grupos asignados existentes por los grupos seleccionados (si no se selecciona ningún grupo de usuarios, se eliminan todos los grupos asignados existentes).		NOMBRE DEL GRUPO	USUARIOS ASIGNADOS	☐	group 1	2	☐	group 2	0	☐	group 3	1	☐	group 4 empty	0	☐	group 5	1
	NOMBRE DEL GRUPO	USUARIOS ASIGNADOS																	
☐	group 1	2																	
☐	group 2	0																	
☐	group 3	1																	
☐	group 4 empty	0																	
☐	group 5	1																	

Tarea	Acción
	 Note Los usuarios deben tener los permisos Administrar aplicaciones y Acceso a todas las aplicaciones para usar Sobrescribir y guardar. Para obtener más información sobre los grupos, consulte Grupos.
Ver los detalles de una aplicación	Haga clic en el nombre de la aplicación.
Ver la directiva de seguridad aplicada a una aplicación	Haga clic en la clasificación por estrellas.
Ver métricas combinadas en las versiones de producción de una aplicación	En la columna Riesgo de producción y cumplimiento de directivas , se muestra la clasificación por estrellas combinada y la cantidad de problemas en las versiones de producción de una aplicación.

Tarea	Acción
Ver los estados de análisis más recientes en las versiones de una aplicación	Coloque el cursor sobre el icono de estado relevante. Haga clic en él para acceder directamente a los detalles del estado del análisis. • Los análisis programados muestran la fecha de inicio programada. • La fecha prevista de finalización se calcula en función de la fecha de inicio del análisis + SLO del tipo de evaluación elegido + período de pausa + fines de semana. En caso de que se realice un análisis posterior al SLO, la fecha de finalización prevista mostrará el mensaje: "Análisis largo en ejecución. Póngase en contacto con nosotros para obtener más información".

Tarea	Acción
Ver los cambios relevantes al riesgo más recientes correspondientes a una aplicación	La columna Cambio más reciente muestra el cambio más reciente de la siguiente lista: • Perfil de riesgo actualizado • Versión creada • Versión implementada en producción • Nuevas vulnerabilidades dinámicas detectadas • Nuevas vulnerabilidades estáticas detectadas • Nuevas vulnerabilidades móviles detectadas • Importancia para el negocio actualizada • Versión que ha aprobado la política de seguridad • Versión que no cumple la política de seguridad

1.4.4.2. Filtrado de la página Sus aplicaciones

De forma predeterminada, la página Sus aplicaciones muestra todas sus aplicaciones, ordenadas de arriba abajo en función de los siguientes criterios:

- El grupo al que pertenece la aplicación, ordenado de forma descendente según la prioridad:
 - producción: aplicación con una o más versiones de producción (ordenada por estado aprobado/suspenso, donde suspendida > no evaluada > aprobada)
 - preproducción: aplicación con una o varias versiones en fase de desarrollo o control de calidad
 - retirado: aplicación sin versiones de producción, desarrollo ni control de calidad
- En cada grupo (producción, preproducción y retirado), las aplicaciones se ordenan por su importancia para el negocio (de alta a baja), seguida del número de problemas por gravedad.

Puede limitar las aplicaciones que se muestran, así como cambiar el orden, mediante filtros. Los siguientes filtros están disponibles en la página Sus aplicaciones:



Note

Un filtro aparece en la lista de filtros solamente cuando los resultados contienen varios valores para ese filtro.

Filtro	Descripción	Valores
Tipo de aplicación	El tipo de aplicación, seleccionado durante el proceso de creación de la aplicación	Móvil o Web/Cliente pesado
Importancia para el negocio	Importancia para el negocio de una aplicación	Alto, Medio, Bajo
Tiene microservicios	Si la aplicación tiene microservicios o no	falso, verdadero
Estado de análisis dinámico	Estado de análisis dinámicos	Programado, En curso, Completado, Cancelado, En espera
Estado del análisis móvil	Estado de análisis móviles	Programado, En curso, Completado, Cancelado, En espera
Cambio más reciente	Categoría del cambio más reciente detectado en una aplicación	Nuevas vulnerabilidades de supervisión detectadas, Versión que ha aprobado la política de seguridad, Importancia para el negocio actualizada, Versión creada, Nuevas vulnerabilidades dinámicas detectadas, Versión que no cumple la política de seguridad
Aprobar/Suspender	Clasificación Aprobar/Suspender definida por el usuario	Fallido, Aprobado, Sin evaluar

Filtro	Descripción	Valores
Tipo de análisis	Tipo de análisis	Estático, Dinámico, Móvil, Código abierto
Ordenar	Orden de clasificación	Riesgo de producción (predeterminado), Cambio más reciente, Nombre de la aplicación (A-Z) y Nombre de la aplicación (Z-A).
Clasificación por estrellas	Sistema de clasificación de 5 estrellas	1, 2, 3, 4, 5
Estado del análisis estático	Estado de análisis estáticos	En curso, Completado, Cancelado, En espera
<Atributo de la aplicación personalizado>	Atributos de aplicación que son listas de selección	Definido por el usuario
<Atributo del microservicio personalizado>	Atributos de microservicios que son listas de selección	Definido por el usuario

1.4.5. Visualización de versiones del inquilino

Además de revisar varias aplicaciones a la vez, también puede revisar los detalles de las versiones individuales en varias aplicaciones simultáneamente. La página Sus versiones muestra información general de alto nivel de las versiones en OpenText Core Application Security.

Para ver la página Sus versiones:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones. La cuadrícula muestra los siguientes detalles sobre cada versión: nombre de la aplicación, nombre de la versión asociada, cantidad de problemas encontrados en la versión, clasificación por estrellas y estados de análisis actuales.

</

3. Seleccione las pestañas para filtrar las versiones en función de sus estados de SDLC. El estado de SDLC predeterminado es **Todo**, que muestra todas las versiones. Puede cambiar el estado de SDLC predeterminado en la configuración de su cuenta.

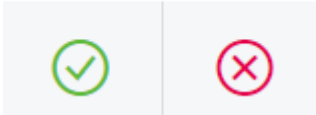
1.4.5.1. Desplazamiento por la página Sus versiones

En la siguiente tabla, se describe cómo desplazarse por la página Sus versiones.

Tarea	Acción
Creación de una aplicación	Haga clic en + Nueva aplicación .
Buscar en la lista de versiones	Escriba una palabra clave o una frase en el cuadro de texto de búsqueda y pulse Intro. Para quitar los resultados de búsqueda, elimine el texto del cuadro de búsqueda y pulse Intro o quite el filtro aplicado. Para obtener más información, consulte Búsqueda de aplicaciones y versiones.
Exportar datos como archivo .csv	Haga clic en Exportar. Un archivo .csv que contiene información detallada sobre todas las vulnerabilidades se guarda en una carpeta local especificada en la configuración del navegador.  Note Las funcionalidades de exportación en las páginas Panel de inquilino, Sus versiones y Problemas de versión muestran los mismos campos para las columnas. Los filtros aplicados actualmente también se aplican a la exportación.
Cambiar las columnas de la cuadrícula	- Haga clic en . - Use las casillas de verificación para hacer las selecciones. - Haga clic en Guardar.

Tarea	Acción
Mostrar u ocultar la lista de filtros	Haga clic en  .
Expandir o contraer filtros	Haga clic en expandir todo contraer todo  o en la flecha junto al nombre del filtro.
Aplicar filtros	Seleccione los valores de filtro deseados debajo del nombre del filtro. La página se actualizará automáticamente con los resultados filtrados. Para algunos filtros, haga clic en aplicar para actualizar la página.
Quitar los filtros aplicados	Haga clic en X o en Borrar filtros en la parte superior de la página.
Filtrar versiones por el estado de SDLC	Seleccione una pestaña que corresponda a un estado de SDLC. El estado de SDLC seleccionado se conserva al pasar de una vista a otra. 
Ordenar la lista de versiones por columna	Haga clic en un encabezado de columna. La flecha junto al encabezado indica el orden de clasificación de los datos. Para invertir el orden, haga clic otra vez en el encabezado.

Tarea	Acción
Editar atributos de la versión para múltiples versiones	1. Active la casilla que aparece junto a las versiones individuales o haga clic en seleccionar todo para seleccionar todas las versiones de la página. 2. Haga clic en Editar atributos. Se abrirá la ventana Editar atributo.  3. Actualice los campos según sea necesario. 4. Haga clic en Guardar. Para obtener más información sobre los atributos de la versión, consulte Creación de una versión
Iniciar un análisis	Haga clic en Iniciar análisis y seleccione el tipo de análisis.
Ver detalles adicionales de una aplicación o versión	Haga clic en el nombre de una aplicación o de una versión.

Tarea	Acción
Ver los estados de análisis más recientes de una versión	Coloque el cursor sobre un icono de estado. Haga clic en él para acceder directamente a los detalles del estado del análisis. ESTÁTICO DINÁMICO  • Los análisis programados muestran la fecha de inicio programada. • La fecha de finalización se calcula sumando la fecha de inicio, el SLO del tipo de evaluación elegido, el periodo de pausa y los fines de semana. En caso de que un análisis se realice después del SLO, la fecha de finalización prevista mostrará un mensaje que indica: "Análisis de larga ejecución en <versión>. Póngase en contacto con nosotros para obtener más información".
Ver la directiva de seguridad aplicada a una aplicación principal de la versión	Haga clic en una clasificación por estrellas.

1.4.5.2. Filtrado de la página Sus versiones

La página Sus versiones muestra todas sus versiones de forma predeterminada. Puede aplicar filtros para limitar las versiones que se muestran. Los siguientes filtros están disponibles en la página Sus versiones:



Note

Un filtro únicamente aparece en la lista de filtros cuando las versiones tienen varios valores para ese filtro.

Filtro	Definición	Valores
Fecha de creación de la aplicación	Fecha de creación de la aplicación	< 7 días, < 30 días, < 90 días, < 180 días
Tipo de aplicación	El tipo de aplicación, seleccionado durante el proceso de creación de la aplicación	Móvil o Web/Cliente pesado
Importancia para el negocio	Importancia de las aplicaciones	Alto, Medio, Bajo
Estado de análisis dinámico	Estado de análisis dinámicos	No iniciado, Cancelado, Completado, En curso, Esperando
MicroserviceName	Nombres de microservicios	Definido por el usuario
Estado del análisis móvil	Estado de análisis móviles	No iniciado, Cancelado, Completado, En curso, Esperando
Aprobar/Suspender	Clasificación Aprobar/Suspender definida por el usuario	Suspender, Aprobar
Tipo de análisis	Tipo de análisis	Estático, Dinámico, Móvil
Estado de SDLC	Estado de SDLC de las versiones	Producción, Control de calidad/Prueba, Desarrollo, Retirado
Clasificación por estrellas	Sistema de clasificación de 5 estrellas	1, 2, 3, 4, 5
Estado del análisis estático	Estado de análisis estáticos	En curso, Completado, Cancelado, En espera

Filtro	Definición	Valores
<Atributo de versión personalizado>	Atributos de versión que son listas de selección	Definido por el usuario

1.4.6. Búsqueda de aplicaciones y versiones

Además del cuadro de búsqueda de nivel superior disponible en la barra de herramientas del portal, también puede utilizar el cuadro **Texto de búsqueda** disponible en cada cuadrícula para buscar nombres de aplicaciones, nombres de versiones, palabras clave y direcciones URL en el contexto de visualización de la cuadrícula.

Búsqueda de texto

Para buscar una aplicación o una versión en una cuadrícula:

1. Escriba la cadena que desee buscar en el cuadro **Texto de búsqueda**.



No es necesario escribir toda la cadena en el cuadro. Por ejemplo, si busca una aplicación llamada *Aplicación de prueba 1*:

- Si escribe **Prueba** en el cuadro, los resultados de la búsqueda **incluirán** *Aplicación de prueba 1*.
- Si escribe **Prueb** en el cuadro, los resultados de la búsqueda **no** incluirán *Aplicación de prueba 1*.
- Si escribe **Prueb*** en el cuadro, los resultados de la búsqueda **incluirán** *Aplicación de prueba 1*.

2. Haga clic en **Intro**.

La página se actualizará con los resultados de la búsqueda.

3. Haga clic en el nombre de aplicación o versión que desee. La página se actualizará para mostrar la página de la aplicación o versión seleccionada y se borrará el contenido del cuadro de búsqueda.

Eliminación de los resultados de búsqueda

Para quitar el filtro de búsqueda aplicado, realice una de las siguientes acciones:

- Quite la cadena de búsqueda del cuadro de búsqueda.
- Haga clic en la flecha **Atrás** del navegador.

1.4.7. Creación de vínculos en profundidad

OpenText Core Application Security es compatible con la vinculación en profundidad a aplicaciones, versiones, análisis y problemas.

Para crear vínculos en profundidad, use los siguientes formatos de ruta:

- Aplicaciones: `https://<dominio_de_fod>/redirect/Applications/<id_aplicación>`
- Versiones: `https://<dominio_de_fod>/redirect/Releases/<id_versión>`
- Análisis: `https://<dominio_de_fod>/redirect/Scans/<id_análisis>`
- Problemas: `https://<dominio_de_fod>.com/redirect/Issues/<id_problema>`



Note

En la parte superior del panel de detalles del problema aparece el identificador del problema.

236127 <http://zero.webappsecurity.com:80/forge>

donde `<dominio_de_fod>` es el dominio del centro de datos de OpenText Core Application Security:

- EE. UU.: `ams.fortify.com`
- EMEA: `emea.fortify.com`
- APAC: `apac.fortify.com`
- FedRAMP: `fed.fortify.com`

1.5. Ejecución de evaluaciones

OpenText Core Application Security ofrece pruebas integrales de seguridad en tres tipos de evaluación: dinámica, estática y móvil.

Esta sección contiene los siguientes temas:

- [Evaluaciones estáticas](#)
- [Análisis de composición de software de código abierto](#)
- [Evaluaciones dinámicas](#)
- [Evaluaciones móviles](#)
- [Uso de derechos](#)
- [Administración de análisis](#)

1.5.1. Evaluaciones estáticas

Una evaluación estática analiza el código fuente, el código de bytes o los archivos binarios de una aplicación para identificar vulnerabilidades de seguridad potenciales. Las evaluaciones estáticas funcionan con OpenText SAST. Las pruebas estáticas con OpenText SAST implican:

1. Traducir el código fuente a un formato traducido intermedio
2. Analizando el código traducido

Esta sección contiene los siguientes temas:

- [Requisitos de OpenText SAST](#)
- [Preparación de archivos en evaluaciones estáticas](#)
- [Configuración de un análisis estático](#)
- [Carga de una carga de evaluación estática](#)
- [Validación de la carga de una evaluación estática](#)

1.5.1.1. Requisitos de OpenText SAST



Note

Pueden darse actualizaciones de OpenText SAST en OpenText Core Application Security entre versiones principales. Los requisitos de OpenText SAST se actualizan en la documentación para la versión principal. Para obtener más información sobre las versiones de OpenText SAST, consulte la [Documentación de herramientas y pruebas de seguridad de aplicaciones estáticas de OpenText](#).

Esta sección contiene los siguientes temas:

- [Lenguajes admitidos](#)
- [Compiladores admitidos](#)
- [Bibliotecas, marcos y tecnologías compatibles](#)

1.5.1.1.1. Lenguajes admitidos

OpenText SAST admite los lenguajes de programación que figuran en la siguiente tabla.

Lenguaje/Marco	Versiones
.NET (Core)	2.0.x–9.x
.NET Framework	2.0–4.8
ABAP/BSP	6.x, 7.x
ActionScript	3.0
Apex	55–61
Bicep	0.12.x–0.15.31
C#	5–13
C	C11, C17, C23 (consulte Compiladores)
C++	C++11, C++14, C++17, C++20 (consulte Compiladores)
Classic ASP (con VBScript)	2.0, 3.0
COBOL	IBM Enterprise COBOL para z/OS 6.1–6.3 (CICS, IMS, DB2 y IBM MQ) Visual COBOL 6.0–8.0
ColdFusion	8–10
Dart	2.12–3.1
Docker (Dockerfiles)	cualquiera

Lenguaje/Marco	Versiones
Flutter	2.0-3.13
Go	1.12-1.23
HCL	2.0  Note La compatibilidad con el lenguaje HCL es específica para Terraform y las configuraciones compatibles de infraestructura como código (IaC) del proveedor de nube.
HTML	5 o anteriores
Java (incluido Android)	7-21
JavaScript	ECMAScript 2015–2023
JSON	ECMA-404
JSP	1.2-2.1
Kotlin	1.3-2.0
MXML (Flex)	4
Objective-C/C++	2.0 (consulte Compiladores)

Lenguaje/Marco	Versiones
PHP	7.3-8.3
PL/SQL	8-23
Python	2.6–2.7, 3.0–3.12
Ruby	1.x
Scala	2.11–2.13, 3.3–3.4
Solidity	0.4.12–0.8.21
Swift	5.0–5.10, 6.0 (consulte Compiladores para ver las versiones de swiftc compatibles)
T-SQL	SQL Server 2005, 2008, 2012
TypeScript	3.6-5.4
VBScript	2.0, 5.0
Visual Basic (VB.NET)	15.0-16.9
Visual Basic	6.0
XML	1.0

Lenguaje/Marco	Versiones
YAML	1.2

1.5.1.1.2. Compiladores admitidos

<<topic is shared with FoD>>

OpenText SAST admite los compiladores que figuran en la siguiente tabla.

Compilador	Versiones	Sistemas operativos
gcc	GNU gcc 6.x–10.4, 11, 12, 13	Windows, Linux, macOS
	GNU gcc 4.9, 5.x	Windows, Linux, macOS, AIX
g++	GNU g++ 6.x–10.4, 11, 12, 13	Windows, Linux, macOS
	GNU g++ 4.9, 5.x	Windows, Linux, macOS, AIX
OpenJDK javac	9, 10, 11, 12, 13, 14, 17, 21	Windows, Linux, macOS, AIX
Oracle javac	7, 8, 9	Windows, Linux, macOS
cl (MSVC)	2015, 2017, 2019, 2022	Windows
Clang	14.0.3, 15.0.0, 16.0.0	macOS
Swiftc	5.8, 5.8.1, 5.9, 5.9.2, 5.10, 6.0, 6.0.2, 6.0.3 ¹	macOS

¹OpenText SAST admite las aplicaciones generadas con las siguientes versiones de Xcode: 14.3, 14.3.1, 15, 15.0.1, 15.1, 15.2, 15.3, 15.4, 16, 16.1, 16.2 .

1.5.1.1.3. Bibliotecas, marcos y tecnologías compatibles

OpenText SAST es compatible con las bibliotecas, los marcos y las tecnologías que se enumeran en esta sección con Fortify Secure Coding Rulepacks dedicado y cobertura de vulnerabilidades más allá de los principales lenguajes admitidos.

Java

Adobe Flex	Apache Slide	iBatis	Mozilla Rhino	Spring AI
Blaze DS	Apache	IBM MQ	MyBatis	Spring MVC
Ajanta	Spring	IBM	MyBatis-Plus	Spring Boot
Amazon Web	Security	WebSphere	Netscape	Spring Data
Services	(Acegi)	Jackson	LDAP API	Commons
(AWS) SDK	Apache	Jakarta	OkHttp	Spring Data
Android	Struts	Activation	OpenCSV	JPA
Android	Apache	Jakarta EE	Oracle	Spring Data
Jetpack	Tapestry	(Java EE)	Application	MongoDB
Apache	Apache	Jasypt	Development	Spring Data
Axiom	Tomcat	Java	Framework	Redis
Apache Axis	Apache	Annotations	(ADF)	Spring
Apache	Torque	Java Excel	Oracle BC4J	HATEOAS
Beam	Apache Util	API	Oracle JDBC	Spring JMS
Apache	Apache	JavaMail	Oracle OA	Spring JMX
Beehive	Velocity	JAX-RS	Framework	Spring
NetUI	Apache	JAXB	Oracle	Messaging
Apache	Wicket	Jaxen	tcDataSet	Spring
Catalina	Apache Xalan	JBoss	Oracle XML	Security
Apache	Apache	JDesktop	Developer Kit	Spring
Cocoon	Xerces	JDOM	(XDK)	Webflow
Apache	ATG Dynamo	Jetty	OWASP	Spring
Commons	SDK de	JGroups	Enterprise	WebSockets
Apache ECS	Azure	json-simple	Security API	Spring WS
Apache	Castor	JTidy Servlet	(ESAPI)	Stripes
Hadoop	Display Tag	JXTA	OWASP HTML	Sun
Apache	Dom4j	JYaml	Sanitizer	JavaServer
HttpCompon	GDS AntiXSS	Liferay Portal	OWASP Java	Faces (JSF)
ents	Google Cloud		Encoder	Tungsten
Apache				Weblogic
Jasper				

Apache Log4j	Google Dataflow	MongoDB	Plexus Archiver	WebSocket
Apache Lucene	Google Guava		Realm	XStream
Apache MyFaces	Google Web Toolkit		Restlet	YamlBeans
Apache OGNL	gRPC		SAP Web Dynpro	ZeroTurnaround ZIP
Apache ORO	Gson		Saxon	Zip4J
Apache POI	Hibernate		SnakeYAML	
Apache SLF4J			Spring	

Kotlin

El soporte de Kotlin incluye todas las bibliotecas cubiertas para Java y las siguientes bibliotecas de Kotlin.

Biblioteca estándar de Kotlin				

Scala

El soporte de Scala incluye todas las bibliotecas cubiertas para Java y las siguientes bibliotecas de Scala.

Akka HTTP	Scala Slick			
Scala Play				

.NET

.NET Framework, .NET Core y .NET Estándar	SDK de Azure	Hot Chocolate	MongoDB	SharePoint Services
.NET WebSockets	Castle ActiveRecord	IBM Informix .NET Provider	MySQL Connector/NET	SharpCompress
ADO.NET Entity Framework	CsvHelper	Json.NET	NHibernate	SharpZipLib
ADODB	Dapper	Log4Net	NLog	SQLite .NET Provider
Amazon Web Services (AWS) SDK	DB2 .NET Provider	Microsoft ApplicationBlocks	Npgsql	SubSonic
ASP.NET MVC	DotNetZip	Microsoft My Framework	Open XML SDK	Sybase ASE ADO.NET Data Provider
ASP.NET SignalR	Entity Framework	Microsoft Practices Enterprise Library	Oracle Data Provider for .NET	Xamarin
ASP.NET Web API	Entity Framework Core	Microsoft Web Protection Library	OWASP AntiSamy	Xamarin Forms
	fastJSON		Saxon	YamlDotNet
	gRPC			

C

ActiveDirectory LDAP	CURL Library	MySQL	OpenSSL	Sun RPC
Apple System Logging (ASL)	GLib	Netscape LDAP	POSIX Threads	WinAPI
	JNI	ODBC	SQLite	

C++

Boost Smart Pointers MFC	STL WMI			

SQL

Oracle ModPLSQL			

PHP

ADODB Advanced PHP Debugging CakePHP PHP Debug	PHP DOM PHP Extension PHP Hash PHP JSON PHP Mcrypt	PHP Mhash PHP Mysql PHP OCI8 PHP OpenSSL PHP PostgreSQL	PHP Reflection PHP Simdjson PHP SimpleXML PHP Smarty PHP Sodium	PHP WordPre ss PHP XML PHP XMLReader PHP Zend PHP Zip

JavaScript/TypeScript/HTML5

Angular	API de Gemini	JS-YAML	React	Sequelize
Anthropic Claude	GraphQL.js	LangChain	React Native	Underscore.js
Apollo Server	Handlebars	Mustache	React Native Async Storage	Vue
Bluebird	Helmet	Node.js Azure Storage	React Router	
child-process-promise	iOS JavaScript Bridge	Node.js Core	SAPUI5/Open UI5	
Exprés	jQuery	OpenAI		

Python

aiopg	Graphene	_mysql	pycrypto	requests
Amazon Web Services (AWS) Lambda	gRPC	MySQL Connector/Python	PyCryptodome	simplejson
Amazon SageMaker	httplib2	MySQLdb	pycurl	six
Anthropic Claude	Jinja2	OpenAI	pylibmc	TensorFlow
Azure Functions	LangChain	oslo.config	PyMongo	Twisted Mail
Django	libxml2	Paramiko	PySpark	urllib3
Flask	lxml	psycopg2	PyYAML	WebKit
Google Cloud	memcache-client			

Ruby

MySQL pg	Rack SQLite	Thor		

Objective-C

AFNetworking Apple AddressBook Apple AppKit Apple CFNetwork Apple ClockKit Apple CommonCrypto Apple CoreData	Apple CoreFoundation Apple CoreLocation Apple CoreServices Apple CoreTelephony Apple Foundation Apple HealthKit	Apple LocalAuthentication Apple MessageUI Apple Security Apple Social Apple UIKit	Apple WatchConnectivity Apple WatchKit Apple WebKit Hpple Objective-Zip Realm	SBJson SFHFKeychainUtils SSZipArchive ZipArchive ZipUtilities ZipZap

Swift

Alamofire	Apple CoreFoundati on	Apple MessageUI	Apple WatchKit	Zip
Apple AddressBook	Apple CoreLocation	Apple Security	Apple WebKit	ZipArchive
Apple CFNetwork	Apple Foundation	Apple Social	Hpple	ZIPFoundatio n
Apple ClockKit	Apple HealthKit	Apple SwiftUI	Realm	ZipUtilities
Apple CommonCry pto	Apple LocalAuthenti cation	Apple UIKit	SQLite	ZipZap
Apple CoreData		Apple WatchConne ctivity	SSZipArchive	

COBOL

Auditor	Micro Focus COBOL Run- time System	POSIX		
CICS		SQL		
DLI	MQ			

Go

GORM				
logrus				
gRPC				

Configuración

.NET Configuration	Docker Configuration (Dockerfiles)	Java Apache Struts	Java OWASP AntiSamy	OpenAPI Specification
Adobe Flex (ActionScript) Configuration	GitHub Actions	Java Apache Tomcat Configuration	Java Spring and Spring MVC	Oracle Application Development Framework (ADF)
Ajax Frameworks	Google Android Configuration	Java Blaze DS	Java Spring Boot	PHP Configuration
Amazon Web Service (AWS)	iOS Property List	Java Hibernate Configuration	Java Spring Mail	PHP WordPress
Ansible	J2EE Configuration	Java iBatis Configuration	Java Spring Security	Silverlight Configuration
AWS CloudFormation	Java Apache Axis	Java IBM WebSphere	Java Spring WebSockets	Terraform (AWS, Azure, GCP)
Azure Resource Manager (ARM)	Java Apache Log4j Configuration	Java MyBatis Configuration	Java Weblogic	WS-SecurityPolicy
Build Management	Java Apache Spring Security (Acegi)		Kubernetes	XML Schema
			Mule	

Infraestructura como código: Amazon Web Services

API Gateway	Database Migration Service (DMS)	ElastiCache	Lightsail	Rekognition
AppSync		EMR	Location Service	Route 53
Athena		FinSpace	Mainframe Modernization	SageMaker
Aurora	DocumentDB	FSx		Secrets Manager
Backup	DynamoDB	Global Accelerator	Transmisiones gestionadas para Apache Kafka (MSK)	Servicio de notificación simple (SNS)
Batch	EC2	Glue	MemoryDB para Redis	Servicio de cola simple (SQS)
Certificate Manager	Elastic Block Store (EBS)	GuardDuty	MQ	Servicio de almacenamiento simple (S3)
CloudFormation	Elastic Container Registry (ECR)	Identity and Access Management (IAM)	Neptune	Timestream
CloudFront		Image Builder	Servicio de OpenSearch	Transfer Family
CloudTrail	Elastic Container Service (ECS)	Key Management Service (KMS)	Base de datos de Quantum Ledger (QLDB)	VPC
CloudWatch	Elastic File System (EFS)	Kinesis	RDS	WorkSpaces Family
CodeStar	Elastic Kubernetes Service (EKS)	Kinesis Video Streams	Redshift	
Cognito				
Config	Elastic Load Balancing (ELB)			

Infraestructura como código: Microsoft Azure

App Service	Batch	Base de datos para MySQL	Hub de IoT	Servicio SignalR
Automation	Almacenamiento de blobs	Base de datos para PostgreSQL	Key Vault	Recuperación de sitios
Microsoft Entra Domain Services	Caché para Redis	Databricks	Aplicaciones lógicas	Aplicaciones Spring
Azure Health Data Services	Búsqueda cognitiva	Defender para usar en la nube	Servicios de medios	SQL
Azure Kubernetes Service (AKS)	Registro de contenedores	Event Hubs	Monitor	Cuentas de almacenamiento
	Cosmos DB	Front Door	Archivos NetApp	Conjuntos de escalado de máquinas virtuales (Virtual Machine Scale Sets)
	Base de datos para MariaDB	Centro de IoT	Política	Máquinas virtuales
			Portal	Web PubSub

Infraestructura como código: Google Cloud

Gestión de API de Apigee Motor de aplicaciones BigQuery Cloud Bigtable	Cloud DNS Cloud Functions Cloud Key Management Cloud Load Balancing Cloud Logging	Cloud Spanner Cloud SQL Cloud Storage Compute Engine	Filestore Google Cloud Platform Google Kubernetes Engine (GKE)	Identity and Access Management (IAM) Media CDN Pub/Sub Secret Manager

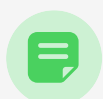
Secretos

.netrc	Definido	HashiCorp (Terraform, Vault)	New Relic	Sendbird
1Password	DES	Heroku	npm	SendGrid
Actually Good Encryption (AGE)	DigitalOcean	HexChat	NuGet	Sentry
Adafruit	Docker	HubSpot	Okta	SHA1
Adobe	Doppler	Intercom	OpenVPN	SHA256
Airtable	Droneci	Java	Contraseña en el comentario	SHA512
Algolia	Dropbox	JFrog (Artifactory)	Contraseña en la cadena de conexión	Shippo
Alibaba (Aliyun)	Duffel	JSON Web Token	Contraseña en el script de PowerShell	Shopify
Amazon (AWS, MWS)	Dynatrace	Monedero de KDE (Kwallet)	Contraseña en URI	Sidekiq
Apple (macOS)	EasyPost	KeePass	Contraseña en URI	Slack
Apache HTTP	Etsy	Kraken	Password Safe	SonarQube
Asana	Facebook	Kucoin	PayPal (Braintree)	Square
Atlassian	Fastly	LaunchDarkly	Pidgin	Squarespace
Authress	Finicity	Linear	Plaid	StackHawk
Autenticación de acceso básico	Finnhub	LinkedIn	Planetscale	Stripe
bcrypt	Flickr	Lob	PostgreSQL	Sumologic
Beamer	Flutterwave	Mailchimp	Postman	Telegram
Token de bearer	Frame.io	Mailgun	Prefect	Travis
Bitbucket	Freshbooks	Mapbox	Pulumi	Trello
Bittrex	Git	Mattermost	PuTTY	Twilio
	GitHub	MD5		Twitch
	GitLab	MessageBird		Twitter
	Gitter			Typeform
	GNOME			Yandex
				Zendesk

Brevo (Sendinblue)	GNU (Bash)	Microsoft (Az	PyPI	
Clojars	GoCardless	ure App	RapidAPI	
Code Climate	Google (API,	Storage,	Readme	
Codecov	Google	Cosmos DB,	RSA Security	
Coinbase	Cloud,	Functions	Ruby (Ruby	
Confluent	OAuth)	and Bitlocker,	on Rails,	
Contentful	Grafana	PowerShell,	RubyGems)	
Databricks		RDP,	Sauce Labs	
Datadog		VBScript)	Clave secreta	
		Microsoft	Secure Shell	
		(Outlook)	Protocol	
		Mutt	(SSH)	
		MySQL		
		Netlify		

1.5.1.2. Preparación de archivos en evaluaciones estáticas

El primer paso en una evaluación estática es preparar los archivos compilados o el código fuente de la aplicación. Para evitar el rechazo de la evaluación estática y obtener resultados de análisis completos y precisos, prepare los archivos de acuerdo con las instrucciones proporcionadas para el lenguaje de programación o el componente tecnológico de la aplicación.



Note

Para obtener información sobre cómo preparar archivos para el análisis de composición de software de código abierto, consulte [Preparación de archivos de evaluación de código abierto](#).

Esta sección contiene los siguientes temas:

- [Requisitos del archivo de evaluación estática](#)
- [Instalación y uso del cliente Fortify ScanCentral SAST](#)
- [Preparación de los archivos de aplicaciones .NET](#)
- [Preparación de archivos de aplicaciones Java](#)
- [Preparación de los archivos JavaScript Technology/HTML/XML](#)
- [Preparación de archivos de aplicaciones Kotlin](#)
- [Preparación de los archivos de aplicación de ABAP \(SAP\)](#)
- [Preparación de archivos de aplicaciones C y C++](#)
- [Preparación de archivos de aplicaciones Classic ASP, VBScript y Visual Basic](#)
- [Preparación de archivos de aplicación Dart y Flutter](#)
- [Preparación de archivos de aplicaciones ColdFusion Markup Language \(CFML\)](#)
- [Preparación de archivos de aplicaciones COBOL](#)
- [Preparación de archivos Dockerfiles e infraestructura como código \(IaC\)](#)
- [Preparación de archivos de aplicaciones Go](#)
- [Preparación de los archivos de aplicaciones PHP](#)
- [Preparación de los archivos de aplicaciones Python](#)
- [Preparación de archivos de aplicaciones Ruby](#)
- [Preparación de archivos de aplicaciones Solidity](#)
- [Preparación de los archivos de aplicaciones de Salesforce \(Apex y Visualforce\)](#)
- [Preparación de archivos de aplicaciones Scala](#)
- [Preparación de archivos de aplicación de Android \(código fuente\)](#)
- [Preparación de archivos de aplicaciones iOS \(código fuente\)](#)

1.5.1.2.1. Requisitos del archivo de evaluación estática

Las aplicaciones enviadas para evaluaciones estáticas deben cumplir con los siguientes requisitos de archivo:

- Los archivos de la aplicación se deben empaquetar en un archivo zip no protegido con contraseña. No se admiten otras extensiones de archivo como tarball, rar, tar y 7z.
- El tamaño de carga máximo es de 5 GB para una aplicación monolítica y de 100 MB para una aplicación de microservicios; las pruebas gratuitas están restringidas a un tamaño máximo de carga de 150 MB.
- La carga debe contener al menos uno de los siguientes tipos de archivos:
 - Archivos binarios/compilados: los archivos binarios y compilados son los archivos ejecutables compilados con depuración que se producen al compilar los archivos de código fuente de su aplicación y los archivos ejecutables de bibliotecas y recursos producidos por las dependencias de terceros que se usan en la aplicación.
 - Archivos de código fuente: los archivos de código fuente son los archivos de texto que se compilan para producir archivos de aplicación.
- Los archivos de aplicación deben cumplir los requisitos específicos para el componente tecnológico bajo el cual se presenta la solicitud. Asegúrese de preparar los archivos de aplicación según las instrucciones del componente tecnológico.
- En general, el código enviado se tiene que poder implementar completamente. Por ejemplo, esto significa que un archivo JAR debe contener código ejecutable.

1.5.1.2.2. Instalación y uso del cliente Fortify ScanCentral SAST

Fortify ofrece un cliente Fortify ScanCentral SAST independiente para empaquetar automáticamente todas las dependencias necesarias y el código fuente requerido para el análisis estático y los archivos requeridos para el análisis de código abierto de OpenText. Se admiten los siguientes lenguajes: .NET y .NET Core (proyectos MSBuild), Apex, Classic ASP, ColdFusion, Dockerfiles, Go, Java (proyectos Gradle y Maven), Javascript/Typescript, PHP, Python y Ruby.



Important

El cliente independiente Fortify ScanCentral SAST es un componente del software local Fortify ScanCentral SAST y se utiliza para empaquetar el código y enviarlo a un controlador para su análisis. OpenText Core Application Security solo usa la función de empaquetado del cliente Fortify ScanCentral SAST. Se han proporcionado detalles que son relevantes para empaquetar su código fuente.

La última versión del cliente Fortify ScanCentral SAST está disponible en la página Herramientas del portal. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

Para obtener más información sobre el uso del cliente de Fortify ScanCentral SAST, consulte la [Fortify Documentación de Software Security Center](#). Seleccione la versión de la documentación que se corresponda con su versión instalada.

- Requisitos de software: "Requisitos de software del cliente Fortify ScanCentral SAST" en *Requisitos del sistema de software de seguridad de las operaciones OpenText™*
- Herramientas de compilación compatibles: "Lenguajes de los sensores de Fortify ScanCentral SAST y herramientas de compilación" en *Requisitos del sistema de software de OpenText™ Application Security*
- Opciones de línea de comandos: "Opciones de comando Package" en *Guía de instalación, configuración y uso de Fortify ScanCentral SAST de OpenText™*

1.5.1.2.3. Preparación de los archivos de aplicaciones .NET

Para las implementaciones de .NET (.NET, .NET Core, .NET Framework y las aplicaciones Xamarin para Android e iOS), use uno de los siguientes métodos para preparar los archivos de aplicación:

- Empaquetado de código automatizado con Fortify ScanCentral SAST (recomendado)
- Empaquetado de código con herramientas IDE
- Empaquetado de código manual



Important

El código fuente se analiza de forma predeterminada. OpenTextEl Portal de MSP recomienda que se proporcione el código fuente, ya que produce resultados de análisis más precisos y completos. Adicionalmente, dado que el proceso de análisis puede devolver falsos positivos, los auditores pueden utilizar el código fuente para revisar manualmente los problemas. Si el análisis de código fuente no es una opción, comuníquese con el soporte técnico para habilitar el análisis de código binario/compilado.

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CICD.

Ejemplos adicionales del comando `package` para .NET:

- Proyecto dotnet en Windows: `scancentral package -bt dotnet -o mypayload.zip`
- Proyecto MSBuild en Windows con archivo CSPROJ: `scancentral package -bt dotnet -o mypayload.zip`

Empaquetado de código con herramientas IDE

Los complementos IDE permiten la selección de archivos de proyecto y las dependencias necesarias para el empaquetado. Para obtener más información sobre cómo utilizar las herramientas IDE, consulte [Herramientas IDE](#).

Empaquetado de código manual

El empaquetado del código manual consta de:

- Preparación de archivos de código fuente
- Preparación de archivos compilados (para código binario/compilado)
- Crear un archivo zip que contenga el código fuente y los archivos compilados

Preparación de archivos de código fuente

El código fuente consta de todos los proyectos para la aplicación. Un proyecto completo contiene lo siguiente:

- Todos los archivos de código fuente necesarios (C/C++, C# o VB.NET)
- Todas las bibliotecas de referencia necesarias

Aquí se incluyen aquellas de los marcos correspondientes, paquetes NuGet y bibliotecas de terceros.

- Para los proyectos C/C++, se incluyen todos los archivos de encabezado necesarios que no pertenecen a la instalación de Visual Studio o de MSBuild.
- Para los proyectos de ASP.NET y ASP.NET Core, se incluyen todos los archivos de páginas ASP.NET necesarios.

Los tipos de páginas ASP.NET compatibles son ASPX, ASCX, ASAX, ASHX, ASMX, AXML, Master, CSHTML, VBHTML, BAML y XAML.

Además, asegúrese de realizar las siguientes tareas para ayudar a reducir los resultados de análisis no deseados:

- Incluya solo una copia de sus dependencias que estén dirigidas a su versión de .NET especificada.
- No incluya las carpetas `obj` y `bin/release` para evitar la duplicación de código en la carga.

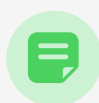


Note

Si está trabajando en el símbolo del sistema para desarrolladores de Visual Studio, asegúrese de que ejecuta el comando `dotnet restore` para asegurarse de que se han descargado e instalado todas las bibliotecas de referencia necesarias en el proyecto. Debe ejecutar este comando desde la carpeta de nivel superior del proyecto.

Preparación de archivos compilados (para código binario/compilado)

- Limpie y compile la aplicación en el modo de depuración **completa**. Los resultados del análisis de los archivos compilados solo incluyen los nombres de archivo y los números de línea si existen los archivos PDB correspondientes. Los archivos binarios y los archivos PDB correspondientes deben ubicarse en la misma carpeta; se excluye un archivo binario si no está presente el archivo PDB correspondiente.



Note

Si va a incluir bibliotecas de terceros en los resultados del análisis, se requieren los archivos PDB correspondientes.

- Proporcione los archivos compilados con depuración, incluidas todas las dependencias. No incluya las carpetas `obj` y `bin/release` para evitar la duplicación de código en la carga.

Creación de un archivo zip

Empaquete los archivos de código fuente y de compilación de depuración en un único archivo comprimido. Coloque los archivos de código fuente en un directorio raíz separado.

Si la aplicación contiene componentes de JavaScript, HTML y/o XML, simplemente incluya los archivos JavaScript, HTML y/o XML en la carga para analizarlos.

1.5.1.2.4. Preparación de archivos de aplicaciones Java

Para aplicaciones Java, use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código con herramientas IDE
- Empaquetado de código manual



Important

El código fuente se analiza de forma predeterminada. OpenTextEl Portal de MSP recomienda que se proporcione el código fuente, ya que produce resultados de análisis más precisos y completos. Adicionalmente, dado que el proceso de análisis puede devolver falsos positivos, los auditores pueden utilizar el código fuente para revisar manualmente los problemas. Si el análisis de código fuente no es una opción, comuníquese con el equipo de soporte técnico para habilitar el análisis de código binario.

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.

Ejemplos adicionales del comando `package` para Java:

- Proyecto Maven con un archivo POM personalizado: `scancentral package -bf myCustomPom.xml -o mypayload.zip`
- Proyecto Gradle con parámetro de compilación personalizado: `scancentral package -bc clean build -o mypayload.zip`

Empaquetado de código con herramientas IDE

Los complementos IDE permiten la selección de archivos de proyecto y las dependencias necesarias para el empaquetado. Para obtener más información sobre cómo utilizar las herramientas IDE, consulte [Herramientas IDE](#).

Empaquetado de código manual

El empaquetado del código manual consta de:

- Preparación de archivos de código fuente
- Preparación de archivos compilados
- Crear un archivo zip que contenga el código fuente y los archivos compilados

Preparación de archivos de código fuente

Proporcione el código fuente, junto con cualquier código fuente de Kotlin relevante al que haga referencia la aplicación Java.

Preparación de archivos compilados

- Compile la aplicación en el modo de depuración (por ejemplo, ejecute `javac -g` si utiliza el compilador javac). Los resultados del análisis de los archivos compilados solo incluyen los nombres de archivo y los números de línea si se proporciona información de la depuración.
- Los archivos JSP deben formar parte de un archivo WAR. No precompile los archivos JSP.
- Cree un paquete de la aplicación en forma de archivo JAR, WAR o EAR.

- Proporcione solo una copia de los archivos compartidos para evitar la duplicación de código en la carga.
- Si se va a usar el análisis de código fuente, proporcione solo las dependencias de los archivos compilados para minimizar la duplicación de problemas en los resultados del análisis. Las dependencias normalmente se encuentran en las carpetas `WEB-INF/lib` (WAR) y `lib` o `APP-INF/lib` (EAR).
- Si se va a usar el análisis de modo mixto, proporcione todos los archivos compilados, incluidas las dependencias.

Creación de un archivo zip

Empaquete los archivos de código fuente y los compilados en un único archivo comprimido. Puede incluir varios archivos JAR, WAR y EAR en el archivo comprimido. No incluya código fuente en archivos JAR; coloque los archivos de código fuente en un directorio raíz separado.

Si la aplicación contiene componentes de JavaScript, HTML y/o XML, simplemente incluya los archivos JavaScript, HTML y/o XML en la carga para analizarlos.

1.5.1.2.5. Preparación de los archivos JavaScript Technology/HTML/XML

Los archivos JavaScript, HTML y XML se pueden enviar como cargas útiles independientes en el componente tecnológico **JS/TS/HTML**. **JS/TS/HTML** es una opción general para aplicaciones web simples y aplicaciones web que principalmente emplean tecnologías relacionadas con JavaScript. Las aplicaciones móviles React Native se envían en el componente tecnológico **React Native**

Para las aplicaciones compiladas con diferentes lenguajes o componentes tecnológicos, y que contienen archivos Javascript, HTML o XML, empaque la aplicación de acuerdo con las instrucciones proporcionadas para el lenguaje o el componente tecnológico, e incluya los archivos JavaScript, HTML o XML en el paquete.

Use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código con herramientas IDE
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.

Empaquetado de código manual

Para las aplicaciones que constan de archivos de JavaScript, TypeScript, HTML o XML, empaquete los archivos en un archivo comprimido .zip. Incluya todas las dependencias de producción. Por ejemplo, ejecute `npm install --only=prod` si utiliza npm.

Además, asegúrese de hacer lo siguiente:

- Incluya el archivo `package.json`.
- Proporcione solo el código fuente TypeScript, no el TypeScript transpilado. Por ejemplo, no proporcione la carpeta `dist` generada al compilar un proyecto de Angular.
- No incluya archivos JavaScript minificados del código fuente, ya que el código minificado reduce considerablemente la calidad de los resultados del análisis.

1.5.1.2.6. Preparación de archivos de aplicaciones Kotlin

Para las aplicaciones Kotlin, empaquete los archivos de código fuente en un archivo ZIP, junto con cualquier código fuente de Java relevante al que haga referencia la aplicación Kotlin. Incluya todas las dependencias; normalmente se encuentran en las carpetas `WEB-INF/lib` (WAR) y `lib` o `APP-INF/lib` (EAR).



Important

El análisis de archivos de origen de Kotlin es compatible.

1.5.1.2.7. Preparación de los archivos de aplicación de ABAP (SAP)

El código ABAP se debe extraer de la base de datos SAP y prepararlo para el análisis. Se proporciona la herramienta Extractor de ABAP de Fortify para la descarga de archivos de código fuente en el servidor de presentación.

Importación de la solicitud de transporte

El extractor de ABAP Fortify está disponible en la página Herramientas del portal (consulte [Visualización de herramientas](#)). El archivo zip del Extractor de ABAP de Fortify contiene los siguientes archivos:

- K900XXX.S9S (donde "XXX" representa el número de versión)
- R900XXX.S9S (donde "XXX" representa el número de versión)

Estos archivos conforman la solicitud de transporte de SAP que debe importar al sistema SAP desde fuera del dominio de transporte local. Solicite la importación de la solicitud de transporte al administrador de SAP o a un individuo autorizado para instalar solicitudes de transporte en el sistema.

Los archivos NSP contienen un programa, una transacción (YSCA) y la interfaz de usuario del programa. Después de importarlos al sistema, puede extraer el código de la base de datos SAP.

Nota sobre la instalación

La solicitud de transporte del Extractor de ABAP de Fortify se creó con un sistema que ejecuta la versión SAP 7.02, nivel de SP 0006. Si se ejecuta una versión de SAP diferente y se produce el error de importación de solicitud de transporte: **La versión de instalación no coincide con la versión actual**, significa que la instalación de la solicitud de transporte no se realizó correctamente.

Realice lo siguiente para solucionar este problema:

1. Vuelva a ejecutar la importación de la solicitud de transporte.

Se abrirá el cuadro de diálogo Importar solicitud de transporte.

2. Haga clic en la pestaña **Opciones**.
3. Active la casilla **Ignorar versión de componente no válida**.
4. Complete el procedimiento de importación.

Si esto no resuelve el problema o si el sistema se está ejecutando en una versión de SAP con una estructura de tablas diferente, OpenText le recomienda exportar la estructura de archivos de ABAP con su propia tecnología, de manera que OpenText Core Application Security pueda analizar el código ABAP.

Ejecución del Extractor de ABAP de Fortify

Debe usar una cuenta que tenga permiso para descargar archivos en el sistema local y ejecutar comandos del sistema operativo.

Haga lo siguiente para ejecutar el Extractor de ABAP de Fortify:

1. Inicie el programa a partir del código de transacción o inicie el objeto Extractor de forma manual.

Objects			
Software Component			
Package		bis	
Program		bis	
BSP Application		bis	

Sourceanalyzer parameters	
FPR File Path	
Working Directory	
Build-ID	
Translation Parameters	
Scan Parameters	
ZIP File Name	
Maximum Call-chain Depth	1

Actions	
☒	Download
☐	Build
☐	Scan
☐	Launch AWB
☐	Create ZIP File
☐	Export SAP standard code

2. Indique el nombre de inicio y finalización del rango de componentes de software, paquetes, programas o aplicaciones BSP que desea analizar.



Note

Puede especificar varios objetos o rangos.

3. Especifique las preferencias para la extracción del código fuente. Los campos son obligatorios a menos que se indique lo contrario.

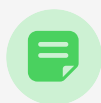


Note

Algunos campos no se aplican al uso de OpenText Core Application Security. Solo se enumeran los campos aplicables.

Campo	Descripción
Directorio de trabajo	Escriba o seleccione el directorio en el que desea almacenar el código fuente extraído.
Nombre del archivo ZIP	(Opcional) Escriba el nombre de un archivo ZIP si desea que la salida se incluya en un paquete comprimido.
Profundidad máxima de la cadena de llamada	No se descarga una F de función SAP global a menos que F se seleccione explícitamente o que se pueda acceder a F a través de una cadena de llamadas de función que se inicie en un código seleccionado explícitamente y cuya longitud sea igual o inferior a este número. No debe especificar un valor superior a 2 a menos que soporte técnico le haya indicado que lo haga.

4. Especifique las acciones que se deben ejecutar. Los campos son obligatorios a menos que se indique lo contrario.



Note

Algunos campos no se aplican al uso de OpenText Core Application Security. A continuación solo se enumeran los campos aplicables.

Campo	Descripción
Descargar	Active esta casilla de verificación para descargar el código fuente extraído de la base de datos SAP.
Crear archivo ZIP	(Opcional) Active esta casilla de verificación para comprimir la salida. También puede comprimir manualmente la salida después de haber extraído el código fuente de la base de datos de SAP.
Exportar código estándar de SAP	(Opcional) Active esta casilla de verificación para exportar el código estándar de SAP además del código personalizado.

5. Haga clic en **Ejecutar**.

Notas sobre el Extractor de ABAP de Fortify

Dado que el programa Extractor de ABAP de Fortify se ejecuta en línea, podría recibir la excepción **Se alcanzó el tiempo máximo para el proceso de trabajo del cuadro de diálogo** si el volumen de los archivos de origen seleccionados para la extracción supera el tiempo de ejecución permitido para el proceso. Para solucionar este problema, descargue los proyectos grandes como una serie de tareas más pequeñas del Extractor. Por ejemplo, si el proyecto consta de cuatro paquetes distintos, descargue cada uno por separado en el mismo directorio de proyecto. Si la excepción

se produce con frecuencia, contacte con su administrador de SAP Basis para incrementar el límite máximo de tiempo (`rdisp/max_wprun_time`).

Cuando un paquete se extrae de ABAP, el Extractor de ABAP de Fortify extrae todo de `TDEVC` con un campo `parentcl` que coincide con el nombre del paquete. A continuación extrae de forma recursiva todo lo demás de `TDEVC` con un campo `parentcl` igual a los que ya se extrajeron de `TDEVC` . El campo extraído de `TDEVC` es `devclass` .

Los valores de `devclass` se consideran un conjunto de nombres de programa y se tratan de la misma manera que un nombre de programa, el cual puede proporcionar.

Los programas se extraen de `TRDIR` comparando el campo de nombre con uno de los siguientes elementos:

- El nombre del programa especificado en la pantalla de selección
- La lista de valores extraídos de `TDEVC` si se proporcionó un paquete

Las filas de `TRDIR` son aquellas para las que el campo de nombre tiene el nombre del programa dado y la expresión `LIKE programname` se usa para extraer filas.

Esta lista final de nombres se usa con `READ REPORT` para extraer código del sistema SAP. Para que conste, este método lee clases y métodos, así como simplemente `REPORTs` .

Cada llamada a `READ REPORT` produce un archivo en la carpeta temporal del sistema local.

A medida que se descarga el código fuente, el Extractor de ABAP de Fortify detecta instrucciones `INCLUDE` en el origen. Cuando las encuentra, descarga los destinos de `INCLUDE` en el sistema local.

Empaquetado del código fuente de ABAP

Si no especificó que el Extractor de ABAP de Fortify debe comprimir la salida, empaquete los archivos de código fuente descargados en un archivo ZIP.

1.5.1.2.8. Preparación de archivos de aplicaciones C y C++

OpenText Core Application Security no admite el análisis directo de código fuente C/C++ o sus binarios. El código C/C++ se debe traducir y empaquetar en un archivo del entorno. De este modo, se garantiza la coherencia de la traducción en relación con las variables del entorno y los compiladores utilizados, y se elimina la necesidad de que el equipo de pruebas reproduzca el entorno de compilación. Se ofrece una versión de OpenText SAST de solo traducción para traducir código C/C++ y empaquetarlo para el análisis.

Instalando OpenText SAST

La última versión de OpenText SAST está disponible en la página Herramientas del portal. Puede descargar instaladores para los sistemas operativos Windows, macOS y Linux. Se requiere un archivo de licencia válido para traducir el código fuente. Póngase en contacto con el equipo de soporte para obtener una licencia, que estará disponible en la página Herramientas.

Para obtener instrucciones de instalación y uso, consulte en [Documentación de herramientas y pruebas de seguridad de aplicaciones estáticas de OpenText](#).

Traducción del código

1. En una interfaz de línea de comandos, cambie el directorio por el directorio de compilación normal.
2. Ejecute el siguiente comando:

```
sourceanalyzer -debug -verbose -logfile translate.log -b <build-id> touchless
<build_command>
```

donde `<build_command>` es su secuencia de comandos de compilación.

Ejemplo:

```
sourceanalyzer -debug -verbose -logfile translate.log -b my_proj touchless
make all
```

3. Compruebe que el proyecto se compila correctamente verificando que la salida de la consola se haya completado y que no haya errores en `translate.log`.

Empaquetado del código traducido

Una sesión de compilación móvil de OpenText SAST le permite traducir un proyecto en un equipo y analizarlo en otro. Un archivo de sesión de compilación móvil (archivo MBS) incluye todos los archivos necesarios para el análisis.

Siga estos pasos para generar y empaquetar un archivo MBS:

1. En el equipo en el que se realizó la traducción, ejecute el siguiente comando para generar una sesión de compilación móvil:

```
sourceanalyzer -b <build-id> -export-build-session <file.mbs>
```

En el comando anterior, `<file.mbs>` es el nombre de archivo que se proporciona para la sesión de compilación móvil.

2. Empaquete el archivo MBS en la raíz de un archivo zip. No incluya otros archivos (como los archivos MBS adicionales) o directorios, ya que esto provocaría la cancelación del análisis.
3. Cargue el archivo comprimido en OpenText Core Application Security en la opción de componente tecnológico **MBS/C/C++/Scala**.

Para obtener más información acerca del uso de OpenText SAST, consulte en [Documentación de herramientas y pruebas de seguridad de aplicaciones estáticas de OpenText](#).

1.5.1.2.9. Preparación de archivos de aplicaciones Classic ASP, VBScript y Visual Basic

Para aplicaciones de Classic ASP, VBScript, y Visual Basic (VB6), use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código con herramientas IDE
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CICD.

Empaquetado de código manual

Empaquete los archivos de código fuente en un único archivo comprimido.

1.5.1.2.10. Preparación de archivos de aplicación Dart y Flutter

Empaquete los archivos de código fuente en un archivo zip. Incluya todas las dependencias.

Descargue las dependencias ejecutando uno de los siguientes comandos:

- Para proyectos de Flutter, use `flutter pub get` .
- Para proyectos solo de Dart, use `dart pub get` .

Por ejemplo, para descargar las dependencias de un proyecto Flutter que tiene la raíz del proyecto `myproject` , ejecute los siguientes comandos:

```
cd myproject flutter pub get
```



Important

Si el proyecto incluye paquetes anidados con diferentes archivos `pubspec.yaml` , debe ejecutar `dart pub get` o `flutter pub get` para cada raíz del paquete.



Important

Asegúrese de que lo siguiente esté incluido en el directorio del proyecto:

- El archivo `pubspec.yaml` , que especifica las dependencias
- El directorio `dart_tool` , que incluye el archivo `package_config.json` generado automáticamente por la herramienta `pub`

1.5.1.2.11. Preparación de archivos de aplicaciones ColdFusion Markup Language (CFML)

Para aplicaciones CFML, use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.

Empaquetado de código manual

Empaquete los archivos de código fuente en un único archivo comprimido.

1.5.1.2.12. Preparación de archivos de aplicaciones COBOL

Para aplicaciones de COBOL, use uno de los siguientes métodos para preparar sus archivos de aplicación:

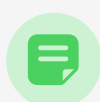
- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package -targs "-copydirs <copybooks>" -targs "-dialect <cobol_dialect> o <output_zip>`; por ejemplo, `scancentral package -targs "-copydirs copybooks" -targs "-dialect COBOL390 o mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CICD.

Empaquetado de código manual

Empaquete el código fuente de COBOL, los archivos de cuaderno que utiliza el código fuente de COBOL y los archivos SQL INCLUDE a los que hace referencia dicho código en un archivo ZIP. Los archivos de cuaderno y SQL INCLUDE deben mantener los nombres que se utilizan en las instrucciones `COPY` del código fuente de COBOL.

No incluya los archivos de cuaderno ni SQL INCLUDE en el directorio ni el subdirectorio en el que reside el código fuente de COBOL. Coloque el código fuente de COBOL en una carpeta denominada `sources/` y los cuadernos en una carpeta denominada `copybooks/`. Coloque estas carpetas al mismo nivel en la raíz del archivo ZIP.

1.5.1.2.13. Preparación de archivos Dockerfiles e infraestructura como código (IaC)

Los archivos de configuración de infraestructura como código (IaC) y los Dockerfiles se pueden enviar como cargas independientes en el componente tecnológico **Infrastructure-As-Code/Dockerfile**.

Para las aplicaciones en contenedor, empaquete la aplicación de acuerdo con las instrucciones proporcionadas para el lenguaje o componente tecnológico de la aplicación e incluya los Dockerfiles en el paquete.



Note

OpenText SAST traduce los siguientes archivos como Dockerfiles: `Dockerfile`, `dockerfile`, `*.Dockerfile`, y `*.dockerfile`.

OpenText SAST acepta los siguientes caracteres de escape en Dockerfiles: barra invertida (`\`) y comillas invertidas (```). Si en el Dockerfile el carácter de escape no está establecido, OpenText SAST supone que la barra diagonal inversa lo es.

Use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.

Empaquetado de código manual

Empaquete los archivos en un archivo zip y envíelo al componente tecnológico **Infrastructure-As-Code/Dockerfile**.

1.5.1.2.14. Preparación de archivos de aplicaciones Go

Para aplicaciones de Go, use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código con herramientas IDE
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.

Empaquetado de código con herramientas IDE

Los complementos IDE permiten la selección de archivos de proyecto y las dependencias necesarias para el empaquetado. Para obtener más información sobre cómo utilizar las herramientas IDE, consulte [Herramientas IDE](#).

Empaquetado de código manual

Empaquete los archivos de código fuente de Go en un archivo zip. Incluya dependencias que no estén en la biblioteca estándar de Go. Asegúrese de que estas dependencias estén en la carpeta del proveedor.

Son compatibles los siguientes sistemas de administración de dependencias integrados en Go:

- Módulos de Go (recomendados)

Si su proyecto usa módulos de Go, los archivos del proyecto (incluyendo el archivo go.mod) deben estar en la raíz del archivo zip. No coloque los archivos del proyecto en directorios anidados.

- GOPATH (obsoleto eSn Go 1.13)



Note

Las siguientes entidades se excluyen del análisis:

- Carpeta del proveedor
- Todos los proyectos definidos por cualquier archivo go.mod en subcarpetas
- Todos los archivos con el sufijo _test.go (pruebas de unidad)

1.5.1.2.15. Preparación de los archivos de aplicaciones PHP

Para aplicaciones PHP, use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código con herramientas IDE
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.

Empaquetado de código con herramientas IDE

Los complementos IDE permiten la selección de archivos de proyecto y las dependencias necesarias para el empaquetado. Para obtener más información sobre cómo utilizar las herramientas IDE, consulte [Herramientas IDE](#).

Empaquetado de código manual

Empaquete los archivos de código fuente en un único archivo comprimido. Asegúrese de incluir el archivo `php.ini` en el paquete. Este archivo ayuda a identificar dónde residen las dependencias.

1.5.1.2.16. Preparación de los archivos de aplicaciones Python

Para las aplicaciones de Python, use uno de los siguientes métodos para preparar los archivos de su aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)



Important

Los microservicios de Python se deben empaquetar con el cliente Fortify ScanCentral SAST.

- Empaquetado de código con herramientas IDE
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CICD.

Empaquetado de código con herramientas IDE

Los complementos IDE permiten la selección de archivos de proyecto y las dependencias necesarias para el empaquetado. Para obtener más información sobre cómo utilizar las herramientas IDE, consulte [Herramientas IDE](#).

Empaquetado de código manual

OpenText SAST procesa archivos PY como código fuente Python. Los archivos PYC (archivos Python compilados) no son compatibles. OpenText SAST admite la traducción de los marcos Django y Flask.

Empaquete los archivos de código fuente en un único archivo comprimido. Incluya todos los paquetes y los módulos estándares y de terceros; se encuentran en la carpeta `lib` del entorno virtual Python (proporcione al menos la carpeta `site-packages`).



Note

Si la aplicación utiliza una versión de Python que no aparece en [Lenguajes admitidos](#), póngase en contacto con el soporte para conocer las opciones disponibles.

1.5.1.2.17. Preparación de archivos de aplicaciones Ruby

Para aplicaciones de Ruby, use uno de los siguientes métodos para preparar sus archivos de aplicación:

- Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)
- Empaquetado de código con herramientas IDE
- Empaquetado de código manual

Empaquetado de código automatizado con el cliente Fortify ScanCentral SAST (recomendado)

El cliente Fortify ScanCentral SAST empaqueta automáticamente el código fuente y todas las dependencias necesarias en su proyecto. Debe descargar el cliente Fortify ScanCentral SAST desde la página Herramientas e instalarlo en el equipo de compilación. Las instrucciones de instalación están disponibles en el archivo README.txt almacenado en el archivo zip.

En una interfaz de línea de comandos, navegue hasta el directorio de trabajo del proyecto y ejecute el comando `package`. La sintaxis básica es: `scancentral package` o `<output_zip>`; por ejemplo, `scancentral package` o `mypayload.zip`.

Para obtener más información sobre el cliente Fortify ScanCentral SAST y las opciones de empaquetado adicionales, consulte [Instalación y uso del cliente Fortify ScanCentral SAST](#).



Note

El empaquetado Fortify ScanCentral SAST está integrado en las herramientas de IDE OpenText Core Application Security y las herramientas CI/CD.

Empaquetado de código manual

Empaquete la aplicación completa tal como se implementaría y todos los archivos de código fuente en un archivo ZIP.

1.5.1.2.18. Preparación de archivos de aplicaciones Solidity

Empaquete los archivos de código fuente en un archivo zip. Incluya todas las dependencias.

OpenText SAST descarga compiladores a los que se hace referencia en el código con la declaración pragma del repositorio del compilador de Solidity. Si un archivo no contiene una declaración pragma, se utiliza el valor predeterminado ^0.8.0.

1.5.1.2.19. Preparación de los archivos de aplicaciones de Salesforce (Apex y Visualforce)

Realice lo siguiente para preparar aplicaciones de Salesforce (Apex y Visualforce):

- Utilice la herramienta de migración Ant disponible en el sitio web de Salesforce para descargar su aplicación a su ordenador local desde su organización de Salesforce (org) donde la desarrolla e implementa. Asegúrese de que los archivos de manifiesto del proyecto estén configurados correctamente para el destino especificado en su archivo `build.xml`.
- La versión descargada de la aplicación contiene:
 - Clases de Apex en archivos con la extensión `.cls`
 - Páginas web de Visualforce en archivos con la extensión `.page`
 - Archivos de código de Apex denominados funciones "desencadenadoras" de base de datos en archivos con la extensión `.trigger`
 - Archivos de componentes de Visualforce con la extensión `.component`
 - Objetos con la extensión `.object`
- Configure los objetivos de recuperación utilizando la documentación de la herramienta de migración Ant. Si su organización utiliza alguna aplicación del intercambio de aplicaciones, asegúrese de que se descargue como destino empaquetado.
- Empaquete los archivos de código fuente en un único archivo comprimido.

1.5.1.2.20. Preparación de archivos de aplicaciones Scala

El código Scala se debe traducir y empaquetar en un archivo del entorno. El complemento de Scala Fortify y la versión de solo traducción de OpenText SAST se encuentran disponibles para traducir el código de Scala y empaquetarlo para su análisis.

Instalando OpenText SAST

La última versión de OpenText SAST está disponible en la página Herramientas del portal. Puede descargar instaladores para los sistemas operativos Windows, macOS y Linux. Se requiere un archivo de licencia válido para traducir el código fuente. Póngase en contacto con el equipo de soporte para obtener una licencia, que estará disponible en la página Herramientas.

Para obtener instrucciones de instalación y uso, consulte en [Documentación de herramientas y pruebas de seguridad de aplicaciones estáticas de OpenText](#).

Traducción del código

Para traducir código Scala, debe tener la siguiente licencia estándar de Lightbend Enterprise Suite y el complemento Scala de Fortify de Lightbend. Póngase en contacto con el soporte de OpenText Core Application Security para obtener una clave de licencia. Para obtener instrucciones sobre cómo descargar el complemento y traducir código Scala, consulte la documentación de Lightbend en <https://developer.lightbend.com/guides/fortify/>.



Important

Si la aplicación contiene código fuente en un lenguaje distinto de Scala, envíe el otro código fuente en una evaluación independiente.

Empaquetado del código traducido

Una sesión de compilación móvil de OpenText SAST le permite traducir un proyecto en un equipo y analizarlo en otro. Un archivo de sesión de compilación móvil (archivo MBS) incluye todos los archivos necesarios para el análisis.

Siga estos pasos para generar y empaquetar un archivo MBS:

1. En el equipo en el que se realizó la traducción, ejecute el siguiente comando para generar una sesión de compilación móvil:

```
sourceanalyzer -b <build-id> -export-build-session <file.mbs>
```

En el comando anterior, `<file.mbs>` es el nombre de archivo que se proporciona para la sesión de compilación móvil.

2. Empaquete el archivo MBS en la raíz de un archivo zip. No incluya otros archivos (como los archivos MBS adicionales) o directorios, ya que esto provocaría la cancelación del análisis.
3. Cargue el archivo comprimido en OpenText Core Application Security en la opción de componente tecnológico **MBS/C/C++/Scala**.

Para obtener más información acerca del uso de OpenText SAST, consulte en [Documentación de herramientas y pruebas de seguridad de aplicaciones estáticas de OpenText](#).

1.5.1.2.21. Preparación de archivos de aplicación de Android (código fuente)

Para las aplicaciones de Android, empaquete los archivos de código fuente de Java o Kotlin en un archivo ZIP. Incluya todas las dependencias necesarias para compilar el código Android en el proyecto de la aplicación.



Note

OpenText SAST es compatible con Xamarin. Para obtener instrucciones sobre la preparación de archivos de aplicación de Xamarin, consulte [Preparación de archivos de aplicación de .NET](#). No se admiten otras bibliotecas de desarrollo de terceros, como Cordova, Ionic Framework, PhoneGap y Unity.

Temas relacionados:

Para obtener información sobre cómo preparar archivos binarios de Android para evaluaciones móviles, consulte [Preparación de archivos de aplicaciones Android \(binarios\)](#).

1.5.1.2.22. Preparación de archivos de aplicaciones iOS (código fuente)

Para las aplicaciones iOS, prepare los archivos de código fuente conforme a las siguientes instrucciones:

- Las aplicaciones deben poder crearse mediante xcodebuild desde la línea de comandos.
- Asegúrese de que cualquier dependencia que se requiera para crear el proyecto se encuentre en la carga y no se acceda a ella a través de administradores de dependencias como una instancia de GitHub protegida por contraseña. La carga debe poder crearse aislada.
- Quite de la aplicación toda configuración específica del desarrollador o del entorno.
- Si el proyecto incluye archivos de lista de propiedades en formato binario, primero debe convertirlos al formato XML. Para ello, puede utilizar el comando `plutil Xcode`.
- Asegúrese de que los encabezados de las bibliotecas de terceros estén disponibles.
- Los proyectos de Objective-C++ deben usar el tiempo de ejecución de Objective-C no frágil (ABI 2 o 3).

Empaquete los archivos de código fuente en un único archivo comprimido.



Note

OpenText SAST es compatible con Xamarin. Para obtener instrucciones sobre la preparación de archivos de aplicación de Xamarin, consulte [Preparación de archivos de aplicación de .NET](#). No se admiten otras bibliotecas de desarrollo de terceros, como Cordova, Ionic Framework, PhoneGap y Unity.

Temas relacionados:

Para obtener información sobre cómo preparar archivos binarios de iOS para evaluaciones móviles, consulte [Preparación de archivos de aplicaciones iOS \(binarios\)](#).

1.5.1.3. Configuración de un análisis estático

Después de preparar los archivos de aplicación para una evaluación estática, debe configurar el análisis estático. Solo necesita configurar los ajustes de análisis estático una vez por versión, ya que la configuración se guardará para el próximo análisis. Puede editar la configuración como considere necesario en evaluaciones posteriores.

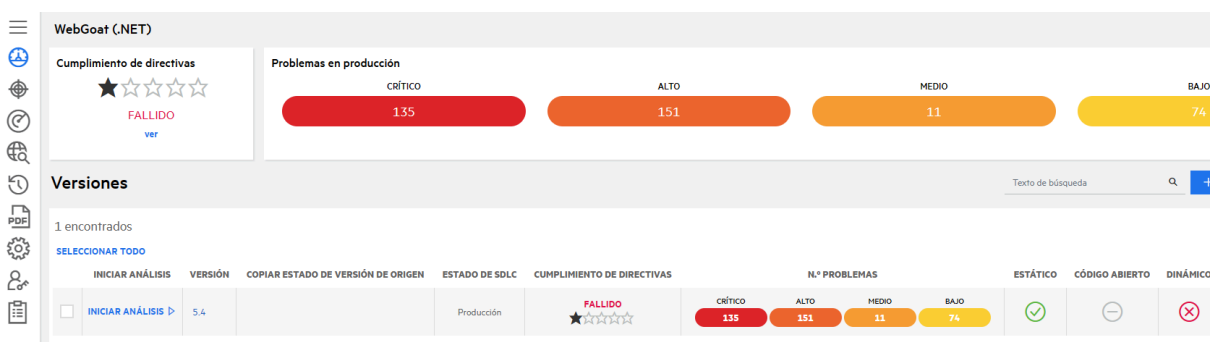
Para configurar un análisis estático:

1. Seleccione la vista **Aplicaciones**.

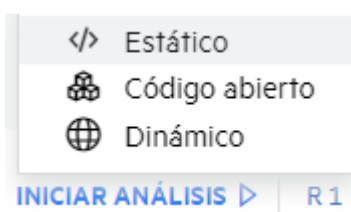
Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación.

Aparecerá la página Información general de la aplicación.



3. Haga clic en Iniciar análisis para la versión que desea evaluar y seleccione Estático.



Aparecerá la página Configuración de análisis estático.

4. Rellene los campos según sea necesario.

Campo	Necesario	Descripción
Tipo de evaluación	Sí	Seleccione un tipo de evaluación. Solo se muestran los tipos de evaluación que permite la directiva de seguridad de la organización. El SLO del tipo de evaluación seleccionado aparece debajo del campo.

Campo	Necesario	Descripción
Derecho	Sí	Seleccione el derecho que la evaluación utilizará. El campo muestra los derechos que son válidos para el tipo de evaluación seleccionado, incluidos los que pueden comprarse. Tenga en cuenta que las aplicaciones de microservicios están restringidas a las suscripciones. Si la versión tiene una suscripción activa, solo se muestran las opciones que no usan derechos.

Campo	Necesario	Descripción
		 Note Si selecciona un derecho que se ofrece mediante una evaluación Dinámico premium y Móvil premium, la evaluación se activa y se deduce el costo completo del derecho.

Campo	Necesario	Descripción
Preferencia de auditoría	Sí	Seleccione la preferencia de auditoría. ◦ Manual: los falsos positivos identificados por Fortify Audit Assistant con alta confianza se suprimen automáticamente. A continuación, un experto en seguridad revisa manualmente los resultados del análisis. ◦ Automatizado: los falsos positivos identificados por Fortify Audit Assistant con alta confianza se suprimen automáticamente, y los resultados se publican sin revisión manual.

Campo	Necesario	Descripción
		 Note Fortify Audit Assistant solo se aplica a nuevos problemas encontrados en un análisis. Desafío de falso positivo no está disponible para los nuevos problemas detectados en un análisis mediante una auditoría automatizada. La capacidad de seleccionar una preferencia de auditoría depende del tipo de evaluación: ◦ Un análisis único Estático solo

Campo	Necesario	Descripción
		permite la opción Automatizado. - Una suscripción Estática permite una auditoría Manual por aplicación (no por versión o microservicio). - Un análisis único Estático+ solo permite la opción Manual. - Una suscripción Estática+ permite una auditoría Automatizada o Manual para cada evaluación.

Campo	Necesario	Descripción
SAST Aviator	No	Para los análisis que utilizan una auditoría automatizada, seleccione la casilla de verificación para que SAST Aviator audite los resultados y proporcione asistencia de corrección mejorada. Esta opción está seleccionada de forma predeterminada si se permite SAST Aviator en la directiva de seguridad; si no es así, la opción está deshabilitada. Este servicio consume 1 unidad de evaluación adicional. No se deduce ningún derecho si no se realiza el servicio SAST Aviator. Para obtener más información sobre SAST Aviator, consulte Auditoría y corrección con SAST Aviator.

Campo	Necesario	Descripción
Análisis de composición de software	No	Active la casilla para incluir el análisis de composición del software de código abierto. Ningún código sale del entorno de OpenText Core Application Security. Para obtener más información sobre la inclusión de análisis de composición de software como parte de un análisis estático, consulte Análisis de composición de software de código abierto.

Campo	Necesario	Descripción
Analizar bibliotecas de terceros para la evaluación de seguridad estática	No	 Note Póngase en contacto con el soporte para habilitar la opción. (Opcional) Active la casilla de verificación para analizar las bibliotecas de terceros en busca de vulnerabilidades, que se incluirán en los resultados del análisis. Esto aumenta considerablemente el tiempo de respuesta. Esta opción no está disponible para aplicaciones de microservicios.

Campo	Necesario	Descripción
		 Note Al seleccionar esta opción, se infiere que su organización recibió el consentimiento de todos los terceros proveedores para analizar sus bibliotecas.

5. Si fuera necesario, puede establecer parámetros de análisis adicionales en las secciones que aparecen debajo de los campos obligatorios.

Haga clic en **Configuración avanzada** y complete los campos según sea necesario.

Campo	Descripción
Componente tecnológico	Seleccione el componente tecnológico de la aplicación. Los lenguajes que pueden seleccionarse dependen del tipo de aplicación (web/cliente pesado o móvil) y de si la aplicación es una aplicación de microservicios. Si la función de detección automática está habilitada, al seleccionar Detección automática, los OpenText Core Application Security determinan el componente tecnológico en función del contenido de la carga útil.
Nivel de lenguaje	Si corresponde, seleccione el nivel de lenguaje del componente tecnológico en la lista.

Haga clic en **Configuración heredada** y complete el campo según sea necesario.

Campo	Descripción	Nota sobre obsolescencia
Integración del servidor de compilación	Una vez configuradas las opciones de análisis estático (tipo de evaluación, componente tecnológico, nivel de idioma, preferencia de auditoría, análisis de composición de software), un token se incluye de manera automática en el campo Integración del servidor de compilación. El token puede utilizarse para enviar una evaluación estática mediante herramientas externas.  Note El token de BSI persiste en todas las evaluaciones de una versión.	El id. de versión reemplaza el token de BSI. Migre las configuraciones de compilación al id. de versión lo antes posible.

Campo	Descripción	Nota sobre obsolescencia
Control de código fuente	Seleccione el método de carga. ◦ Carga manual (predeterminado): realice la carga de forma manual desde el sistema local. ◦ Control de código fuente: realice la carga desde una plataforma de control de versiones. Esta opción estará disponible si se ha configurado el control de código fuente. Para obtener más información, consulte Integración de control de código fuente.	Está previsto que esta función quede obsoleta. Debe migrar las integraciones de control de código fuente heredadas a las canalizaciones en las plataformas de control de versiones aplicables lo antes posible. Para obtener más información, consulte Herramientas de CICD.

Campo	Descripción	Nota sobre obsolescencia
Análisis binario	 Note Póngase en contacto con el soporte para habilitar la opción. (componentes tecnológicos Java/J2EE/Kotlin, .NET y .NET Core) Seleccione la casilla para compilar y analizar archivos de código fuente. El análisis de archivos binarios no es compatible con cargas empaquetadas por Fortify ScanCentral SAST.	

Campo	Descripción	Nota sobre obsolescencia
	 Note Si está habilitado el requisito de inclusión de código fuente, y esta opción no está seleccionada, el análisis se cancelará cuando la carga no contenga código fuente.	

6. Hacer clic **Integración de DevOps e IDE** para ver el id. de versión. El id. de versión puede utilizarse para enviar un análisis estático mediante herramientas CI/CD. El id. de versión actúa como un token que recupera la configuración de análisis guardada más recientemente en el portal.

7. Haga clic en **Guardar**.

La configuración de análisis estático se guardará.

8. Si tiene el permiso Consumir derechos y seleccionó un derecho de suscripción, haga clic en **Iniciar suscripción** para iniciar la suscripción de evaluación estática y consumir el derecho de forma inmediata. El costo de evaluación se deduce del derecho cuando un usuario comienza el análisis inicial.

**Note**

Póngase en contacto con el soporte para habilitar la opción.

1.5.1.4. Carga de una carga de evaluación estática

Una vez que haya empaquetado los archivos de la aplicación y configurado los ajustes de análisis estático, suba la carga para analizar. El límite máximo de tamaño de carga es de 5 GB. Los navegadores web tienen sus propios límites máximos de tamaño (consulte la documentación del navegador para obtener detalles). Como pueden producirse agotamientos del tiempo de espera del portal al cargar archivos grandes, se recomienda cargar a través de este solo si el tamaño de archivo es menor a 500 MB. Si le resulta complicado realizar la carga mediante el portal, consulte [Temas relacionados](#) para obtener información acerca de otros métodos de carga de archivos. También puede ponerse en contacto con el soporte técnico para determinar la opción de carga más adecuada.

Puede tener un solo análisis estático en curso para una versión. Puede enviar varios análisis para una aplicación, incluidos los que son para la misma versión. Los análisis adicionales se ponen en cola y, luego, se ejecutan en el orden en que aparecen allí. Cada aplicación puede tener hasta 30 análisis en la cola.

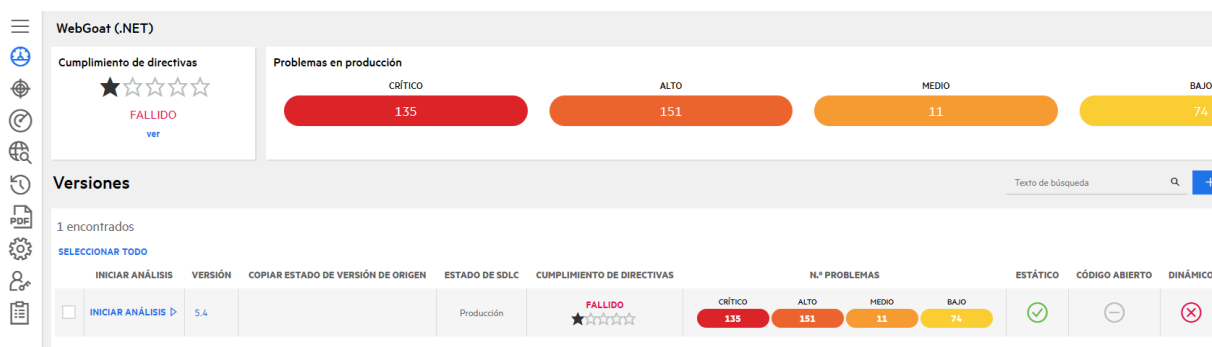
Para realizar una carga de evaluación estática a través del portal, haga lo siguiente:

1. Seleccione la vista **Aplicaciones**.

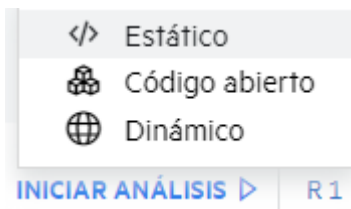
Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación.

Aparecerá la página Información general de la aplicación.



3. Haga clic en Iniciar análisis para la versión que desea evaluar y seleccione Estático en el menú.



Aparecerá la página Configuración de análisis estático.

4. Haga clic en **Iniciar análisis**.

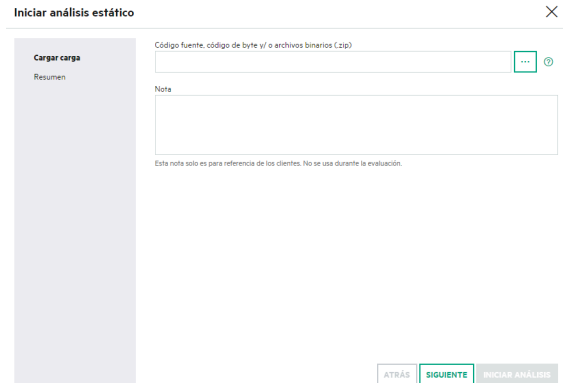


Note

Si ya existe un análisis estático activo en la aplicación, no podrá iniciar otro análisis.

Se abrirá la ventana Iniciar análisis estático.

5. Realice la tarea relevante en función del método de carga:

Método de carga	Procedimiento
Carga manual	 1. Haga clic en 2. Desplácese a su archivo comprimido y selecciónelo.
Control de código fuente	 1. Seleccione Rama o Versión de la lista Ubicación de fuente. 2. Seleccione la rama o la versión concreta.

6. En el campo, escriba una descripción de la aplicación.

7. Haga clic en **Siguiente**.

Aparecerá un resumen de los valores de la configuración de análisis estáticos.

8. Revise el resumen. Si es necesario, haga clic en **Atrás** y realice las correcciones. Si los valores son correctos, haga clic en **Iniciar análisis**.

Una vez que se completa la carga del archivo zip, se le redirige a la página Análisis de versión; su nuevo estado del análisis es **Puesto en cola**. El análisis comenzará una vez que se mueva al frente de la cola.

Temas relacionados

Además de utilizar el portal, puede enviar una evaluación estática utilizando los siguientes métodos:

- Herramientas del complemento de IDE: Visual Studio Extension, Eclipse Plugin, complemento de IntelliJ, extensiones de Fortify para código de Visual Studio.

Para obtener más información, consulte [Herramienta de IDE](#).

- Herramientas de integración del servidor de compilación: FoDUploader, Fortify extensión de Azure DevOps, complemento OpenText Core Application Security de Jenkins. Para obtener más información, consulte [Herramienta de CI/CD](#).
- API de OpenText Core Application Security. Para obtener más información, consulte [OpenText Core Application Security API](#).

1.5.1.5. Validación de la carga de una evaluación estática

Después de realizar una carga, OpenText Core Application Security realiza las siguientes validaciones de carga con el fin de garantizar que se hayan cumplido los requisitos para que el equipo de pruebas estáticas pueda iniciar una evaluación estática:

- El archivo comprimido es válido y no está dañado.
- La carga contiene extensiones de archivo compatibles con OpenText SAST. Las extensiones de archivo admitidas son: ABAP, abap, appxmanifest, as, asax, ascx, ashx, asmx, asp, aspx, baml, bas, bicep, BSP, bsp, cbl, cfc, cfm, cfml, class, cls, cob, conf, Config, config, cpx, cs, cscfg, csdef, cshtml, ctl, ctp, dart, dll, Dockerfile, dockerfile, erb, exe, frm, go, hcl, htm, html, inc, ini, jar, java, jmod, js, jsff, json, jsp, jspf, jsp, jsx, kt, kts, Master, master, mbs, mxml, page, php, phtml, pkb, pkh, pks, plist, properties, py, razor, rb, scala, settings, sol, sql, swift, tag, tagx, tf, tld, trigger, ts, tsx, vb, vbhtml, vbs, vbscript, wadcfg, wadcfgx, winmd, wsdd, wsdl, xaml, xcfg, xhtml, xmi, xml, xsd, yaml, yml.
- Para las aplicaciones .NET, la carga contiene archivos .dll o .exe.
- Para aplicaciones Java y Kotlin, la carga útil contiene archivos .class, .java, .jar, .jsp, .kt, .ktm o .kts.
- Una carga empaquetada con Fortify ScanCentral SAST no tiene habilitada la configuración de análisis **Analizar binarios**.
- Para las aplicaciones de microservicio de Python, la carga se empaqueta utilizando el cliente de Fortify ScanCentral SAST.
- Para componentes tecnológicos que requieren que se envíe un archivo de sesión de compilación móvil (MBS), la carga contiene solo un archivo .mbs.
- Para los inquilinos que hayan habilitado el requisito de inclusión de código fuente, la carga contiene archivos en los siguientes formatos:

Componente tecnológico	Extensión del archivo de origen
.NET	.cs, .vb
ABAP	.abap
ASP	.asp
CFML	.cfm, .cfml, .cfc
COBOL	.cbl, .cob, .ccp, .cb2
Dockerfile/Infraestructura como código	.dockerfile, .json, .xml, .tf, .yaml, dockerfile
Go	.go
JAVA/J2EE/Kotlin	.java, .kt, .ktm, .kts
JS/TS/HTML	.xsd, .xmi, .wsdd, .config, .cpx, .xcfg, .js, .ts
PHP	.php
PYTHON	.py
VB6	.vbs, .bas, .frm, .ctl, .cls
VBScript	.vbscript
Ruby	.rb

Si alguno de los requisitos no se cumple, el análisis se cancelará automáticamente y se enviará un correo electrónico en el que se indicará el motivo de la cancelación. Tras la aceptación del archivo, el código se transfiere a un servidor seguro y se analiza.

1.5.2. Análisis de composición de software de código abierto

OpenText Core Application Security ofrece análisis de composición de software de código abierto en combinación con una evaluación estática o como una evaluación separada. Las aplicaciones se analizan utilizando una de las siguientes herramientas de análisis de composición de software:

- OpenText Core SCA (se ofrece con evaluaciones estáticas y como evaluación separada)
- Sonatype (se ofrece con evaluaciones estáticas, no disponible para su compra)

Son compatibles los lenguajes siguientes: C# (.NET), Go, Java, JavaScript, Kotlin, Objective-C, PHP, Python, Ruby y Swift.

Compre derechos de OpenText Core SCA para permitir el análisis de composición de software de código abierto. Un derecho se canjea para una suscripción de OpenText Core SCA por aplicación. Al enviar un análisis de código abierto, la herramienta de análisis de composición de software comprueba si hay componentes de código abierto en la carga útil. Los resultados del análisis de código abierto identifican dependencias directas y transitivas junto con problemas de seguridad y licencias asociadas

Los inquilinos que no tienen derechos de Sonatype activos reciben cinco análisis Debricked complementarios por cada suscripción estática. Los análisis complementarios están limitados al período de suscripción. Los análisis complementarios se anulan una vez que los inquilinos adquieren derechos de escaneo de código abierto.

Si le interesa comprar derechos de OpenText Core SCA, póngase en contacto con su representante de ventas.

Esta sección contiene los siguientes temas:

- [Preparación de archivos de evaluación de código abierto](#)
- [Realización de una carga de evaluación de código abierto a través del portal](#)
- [Visualización de componentes de código abierto en una versión](#)
- [Visualización de componentes de código abierto en un inquilino](#)

1.5.2.1. Preparación de archivos de evaluación de código abierto

Para el análisis de código abierto, los archivos que se necesitan en la carga dependen de la herramienta de análisis de composición de software que se esté utilizando.

Requisitos de archivos de OpenText Core SCA para el análisis de archivos bloqueados

Para detectar dependencias de manera fiable, OpenText Core SCA utiliza uno de los siguientes enfoques según el sistema de compilación o el administrador de paquetes:

- Algunos administradores de paquetes usan un archivo de bloqueo para describir las dependencias en un proyecto (como npm). Los administradores de paquetes suelen generar de forma automática archivos de bloqueo. OpenText Core SCA admite el análisis de dependencias mediante archivos nativos de bloqueo.
- Para sistemas de compilación o administradores de paquetes o sistemas de compilación que no usan un archivo de bloqueo (como Maven y Gradle), OpenText Core SCA requiere un archivo que describa el árbol de dependencia que se va a generar utilizando la funcionalidad del sistema de compilación o el administrador de paquetes. Este archivo se conoce como archivo de bloqueo de OpenText Core SCA.

Puede utilizar uno de los siguientes métodos para generar archivos de bloqueo nativos y archivos de bloqueo de OpenText Core SCA:

- (Recomendado) Utilice el cliente de Fortify ScanCentral SAST (22.1.2 o posterior) para generar los archivos de bloqueo junto con los archivos de la aplicación. Añada la opción `-oss` al comando `package` para invocar la CLI de OpenText Core SCA y agregar los archivos de bloqueo al paquete. Tenga en cuenta que la generación de paquetes no depende de que se empaqueten correctamente los archivos de bloqueo.
- (Recomendado) Ejecute la CLI de OpenText Core SCA para generar los archivos de bloqueo independientemente de los archivos de la aplicación. Para obtener instrucciones de instalación y uso, consulte [README.FoD.md](#).
- Genere manualmente los archivos de bloqueo. Puede automatizar este proceso agregando el comando adecuado a su canalización de CI/CD.

La siguiente tabla describe los requisitos de los archivos para el análisis con OpenText Core SCA en OpenText Core Application Security.



Important

Se cancelará un análisis de OpenText Core SCA si el archivo de bloqueo necesario no se encuentra en la carga.

Idioma	Administrador de paquetes	Archivo necesario	Notas (si no se utiliza el Fortify ScanCentral SAST client)
C#	NuGet	packages.lock.json	Utilice uno de los siguientes métodos para generar el archivo de bloqueo: • Ejecute <code>debricked resolve</code> desde la CLI de Debricked. Para obtener más información, consulte Paquete C# - Nuget. • Ejecute <code>dotnet restore --use-lock-file</code> desde la CLI de .NET. Para obtener más información, consulte Habilitar restauración de paquetes repetibles

Idioma	Administrador de paquetes	Archivo necesario	Notas (si no se utiliza el Fortify ScanCentral SAST client)
			con un archivo de bloqueo. • Ajuste la propiedad de MSBuild RestorePackagesWithLockFile a true en el archivo de proyecto .csproj y ejecute el comando Nuget restore . Para obtener más información, consulte Habilitar restauracion es de paquetes repetibles con un archivo de bloqueo.

Idioma	Administrador de paquetes	Archivo necesario	Notas (si no se utiliza el Fortify ScanCentral SAST client)
	Paket	<code>paket.lock</code>	Packet genera <code>paket.lock</code> automáticamente.
Go	Go Dep	<code>gopkg.lock</code>	dep genera <code>gopkg.lock</code> automáticamente.  Note Las actualizaciones de Go Dep no se realizarán, ya que Go Dep está obsoleto.

Idioma	Administrador de paquetes	Archivo necesario	Notas (si no se utiliza el Fortify ScanCentral SAST client)
	Módulos Go	gomod.debricked.lock	Para obtener instrucciones sobre cómo generar el archivo de árbol de dependencias resuelto, consulte Go - Módulos Go, Go Dep, Bazel .
Java/Kotlin	Bazel	WORKSPACE	WORKSPACE se genera automáticamente por Bazel.
		(Recomendado) maven_install.json	Usar <code>rules_jvm_external</code> para generar <code>maven_install.json</code> , donde todas las dependencias están ancladas a sus respectivas versiones. Para más información, ver Una regla de repositorio para calcular las dependencias transitivas de Maven .

Idioma	Administrador de paquetes	Archivo necesario	Notas (si no se utiliza el Fortify ScanCentral SAST client)
	Gradle	<code>gradle.debricked.lock</code>	Para obtener instrucciones sobre cómo generar el archivo de árbol de dependencias resuelto, consulte Java & Kotlin - Gradle, Maven and Bazel .
	Maven	<code>maven.debricked.lock</code>	Para obtener instrucciones sobre cómo generar el archivo de árbol de dependencias resuelto, consulte Java & Kotlin - Gradle, Maven and Bazel .
JavaScript	Bower	<code>bower.debricked.lock</code>	Para obtener instrucciones sobre cómo generar el archivo de dependencia resuelto, consulte JavaScript - NPM, Yarn, Bower .

Idioma	Administrador de paquetes	Archivo necesario	Notas (si no se utiliza el Fortify ScanCentral SAST client)
	npm	package-lock.json	El comando <code>npm install</code> genera automáticamente <code>package-lock.json</code> , a menos que esté deshabilitado en un archivo <code>.npmrc</code> . El comando <code>npm install --package-lock-only</code> genera <code>package-lock.json</code> sin comprobar <code>node_modules</code> y descargar dependencias.
	Yarn	yarn.lock	Yarn genera <code>yarn.lock</code> automáticamente.
Objective-C	Cocoapods	podfile.lock	Cocoapods genera automáticamente <code>podfile.lock</code> .

Idioma	Administrador de paquetes	Archivo necesario	Notas (si no se utiliza el Fortify ScanCentral SAST client)
PHP	Composer	composer.lock	Composer genera automáticamente composer.lock .
Python	pip	<file_name>.pip.debricked.lock	Para obtener instrucciones sobre cómo generar el archivo de árbol de dependencia resuelto, consulte Python - Pip, Pipenv .
	Pipenv	Pipfile.lock	Pipenv genera automáticamente Pipfile.lock en función del entorno virtual del proyecto.
Ruby	RubyGems	Gemfile.lock	RubyGems genera automáticamente Gemfile.lock .
Swift	Cocoapods	podfile.lock	Cocoapods genera automáticamente podfile.lock .

De acuerdo con los mejores procedimientos de la industria, debería enviar los archivos de bloqueo al repositorio de control de código fuente. Esto simplifica el proceso de preparación de los archivos de la aplicación, especialmente si no está utilizando el cliente Fortify ScanCentral SAST para empaquetar la carga.

Requisitos de archivos de OpenText Core SCA para el análisis de huellas dactilares

OpenText Core SCA admite el análisis de dependencias no administradas que no están definidas en los archivos de manifiesto mediante el examen de huellas digitales de los archivos de la aplicación, incluidos los archivos binarios (con algunas exclusiones para los archivos no pertinentes). Se debe proporcionar el archivo `debricked.fingerprints.txt` ; este archivo es generado automáticamente por OpenText Core Application Security al enviar un análisis de OpenText Core SCA. Un análisis OpenText Core SCA incluye tanto el análisis de huellas dactilares como el análisis del archivo de bloqueo. Para obtener más información sobre la huella digital de archivos OpenText Core SCA, incluidos los idiomas compatibles actualmente, consulte [Huella digital de archivos](#).

En algunos casos, el paquete y/o la versión resultante de la toma de huellas digitales de archivos pueden diferir de la dependencia utilizada en su aplicación. Puede asegurarse de que los resultados sean correctos al excluir la toma de huellas digitales de un determinado archivo o ruta. Para ello, agregue la dependencia correcta a un archivo de manifiesto. CycloneDX SBOM utilizando el CLI de OpenText Core SCA. Como alternativa, genere un archivo `debricked-config.yaml` para anular los resultados. Para obtener más información sobre la exclusión de dependencias, consulte [Administrar o sobrescribir resultados](#).

Requisitos de archivos Sonatype

Para obtener información sobre los requisitos de archivo para los análisis de Sonatype, consulte <https://help.sonatype.com/iqserver/analysis>.

1.5.2.2. Realización de una carga de evaluación de código abierto a través del portal

El método para cargar una carga de código abierto depende de si la evaluación de código abierto se incluye con la evaluación estática o se ejecuta por separado:

- Para incluir la evaluación de código abierto con la evaluación de análisis estático, configure los parámetros del análisis estático para incluir un análisis de código abierto. Incluya los archivos de origen de código abierto necesarios en su carga útil de evaluación estática. Este método está disponible tanto con OpenText Core SCA como con Sonatype. Para obtener más información, consulte [Configuración de un análisis estático](#).
- Para ejecutar por separado la evaluación de código abierto, cargue un archivo de bloqueo nativo o de OpenText Core SCA. Las siguientes instrucciones describen cómo enviar el análisis solo con OpenText Core SCA.



Note

Puede enviar evaluaciones de OpenText Core SCA en la lista de materiales de software de terceros. Para obtener más información, consulte [Importación de una lista de materiales de software](#).

Para enviar el análisis solo con OpenText Core SCA:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación.

Aparecerá la página Información general de la aplicación.

WebGoat (.NET)

Cumplimiento de directivas
★☆☆☆☆
FALLIDO
ver

Problemas en producción

CRÍTICO	ALTO	MEDIO	BAJO
135	151	11	74

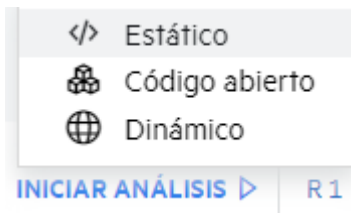
Versiones

1 encontrados

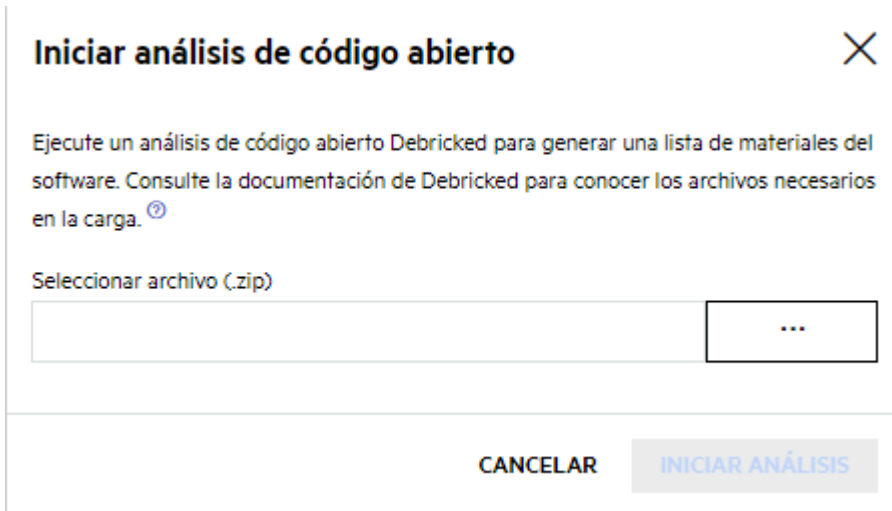
[SELECCIONAR TODO](#)

INICIAR ANÁLISIS	VERSIÓN	COPIAR ESTADO DE VERSIÓN DE ORIGEN	ESTADO DE SDLC	CUMPLIMIENTO DE DIRECTIVAS	N.º PROBLEMAS	ESTÁTICO	CÓDIGO ABIERTO	DINÁMICO
☐ INICIAR ANÁLISIS ▶	5.4		Producción	★☆☆☆☆ FALLIDO	CRÍTICO: 135 ALTO: 151 MEDIO: 11 BAJO: 74	✓	⊖	⊗

- Haga clic en Iniciar análisis para la versión que desea evaluar y seleccione Código abierto.



Aparecerá la ventana de análisis de código abierto.



- Haga clic en
- Diríjase al archivo comprimido que contiene el archivo de bloqueo y selecciónelo. El archivo comprimido puede contener la carga de la evaluación estática o solo el archivo de bloqueo.
- Haga clic en **Iniciar análisis**.

Una vez que se completa la carga del archivo zip, se le redirige a la página Análisis de versión; su nuevo estado del análisis es **Puesto en cola**. El análisis comenzará una vez que se mueva al frente de la cola.

1.5.2.3. Visualización de componentes de código abierto en una versión

Puede ver los componentes de código abierto encontrados en el análisis más reciente de una versión.

Realice lo siguiente para ver los componentes de código abierto de una versión:

1. Seleccione la vista **Aplicaciones**.

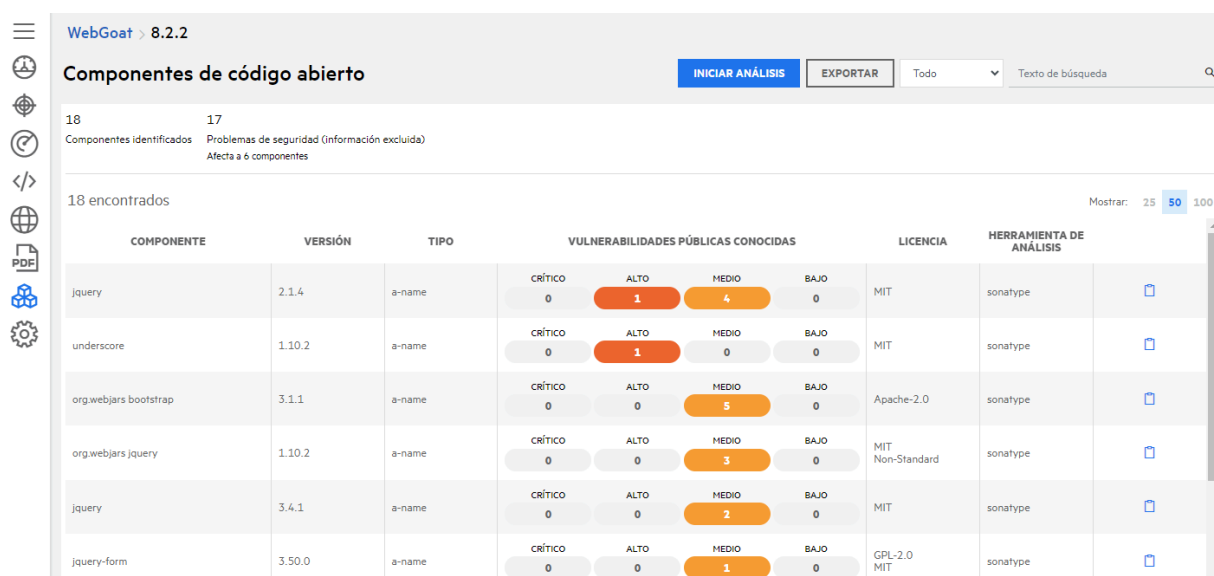
Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

3. Haga clic en **Componentes de código abierto**.

Aparecerá la página Componentes de código abierto.



COMPONENTE	VERSIÓN	TIPO	VULNERABILIDADES PÚBLICAS CONOCIDAS				LICENCIA	HERRAMIENTA DE ANÁLISIS
			CRÍTICO	ALTO	MEDIO	BAJO		
jquery	2.1.4	a-name	0	1	4	0	MIT	sonatype
underscore	1.10.2	a-name	0	1	0	0	MIT	sonatype
org.webjars.bootstrap	3.1.1	a-name	0	0	5	0	Apache-2.0	sonatype
org.webjars.jquery	1.10.2	a-name	0	0	3	0	MIT Non-Standard	sonatype
jquery	3.4.1	a-name	0	0	2	0	MIT	sonatype
jquery-form	3.50.0	a-name	0	0	1	0	GPL-2.0 MIT	sonatype

4. Si hay resultados de varias herramientas de análisis, seleccione el origen cuyos resultados desee ver en la lista desplegable.

La página se actualizará con los resultados del origen seleccionado.

En la siguiente tabla se describe cómo desplazarse por la página Componentes de código abierto.

Tarea	Acción
Exportar la lista de componentes de código abierto	Haga clic en Exportar . Se envía un vínculo para descargar un archivo CSV a la dirección de correo electrónico especificada en la configuración de la cuenta. El vínculo es válido durante 7 días desde el momento en que se envía el correo electrónico.
Ver resultados de una herramienta de análisis específica	En la lista desplegable, seleccione la herramienta de análisis que desea ver.
Buscar en la lista de componentes de código abierto	Escriba una palabra clave o una frase en el campo de texto de búsqueda y pulse Intro .
Filtrar y ordenar por valores de columna	Haga clic en uno de los siguientes encabezados de columna: Componente, Licencia, Herramienta de análisis, Ámbito y Tipo
Ver problemas filtrados por URL del paquete	Haga clic en el recuento de problemas en cada fila de componentes.
Ver la URL del paquete del componente y el enlace de Open Source Select	Haga clic en el icono Detalles .

1.5.2.4. Visualización de componentes de código abierto en un inquilino

Los usuarios que tienen el permiso **Ver aplicaciones de terceros** pueden ver un resumen del inquilino completo de todos los componentes de código abierto identificados, así como las aplicaciones que los utilizan.

Para ver los componentes de código abierto en un inquilino:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Componentes de código abierto**.

Aparecerá la página Componentes de código abierto.

Componentes de código abierto

Sonatype

Texto de búsqueda

14 encontrados

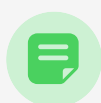
Mostrar:

25

50

100

COMPONENTE	URL DE PAQUETE	VERSIÓN	TIPO	VULNERABILIDADES PÚBLICAS CONOCIDAS				LICENCIA	VERSIONES	
commons-collections:commons-collections		3.1	maven	CRÍTICO 1	ALTO 0	MEDIO 0	BAJO 0	Apache-2.0 Not Declared	3	VER VERSIONES
axis:axis		1.2	maven	CRÍTICO 0	ALTO 3	MEDIO 0	BAJO 0	Apache-1.1 Apache-2.0 Not Declared	3	VER VERSIONES
axis:axis-ant		1.2	maven	CRÍTICO 0	ALTO 0	MEDIO 0	BAJO 0	Not Declared	3	VER VERSIONES
axis:axis-jaxrpc		1.2	maven	CRÍTICO 0	ALTO 0	MEDIO 0	BAJO 0	Apache-2.0	3	VER VERSIONES
axis:axis-saaj		1.2	maven	CRÍTICO 0	ALTO 0	MEDIO 0	BAJO 0	Apache-2.0 Not Declared	3	VER VERSIONES
commons-digester:commons-digester		1.4.1	maven	CRÍTICO 0	ALTO 0	MEDIO 0	BAJO 0	Apache-1.1 Not Declared	3	VER VERSIONES
commons-discovery:commons-discovery		0.2	maven	CRÍTICO 0	ALTO 0	MEDIO 0	BAJO 0	Apache-1.1 Not Declared	3	VER VERSIONES



Note

Los resultados de análisis de código abierto de versiones retiradas no se incluyen.

En la siguiente tabla se describe cómo desplazarse por la página Componentes de código abierto.

Tarea	Acción
Exportar la lista de componentes de código abierto	Haga clic en Exportar . Se envía un vínculo para descargar un archivo CSV a la dirección de correo electrónico especificada en la configuración de la cuenta. El vínculo es válido durante 7 días desde el momento en que se envía el correo electrónico.
Ver resultados de una herramienta de análisis específica	En la lista desplegable, seleccione los resultados de herramienta de análisis que desea ver.
Buscar en la lista de componentes de código abierto	Escriba una palabra clave o una frase en el campo de texto de búsqueda y pulse Intro .
Filtrar y ordenar por valores de columna	Haga clic en uno de los siguientes encabezados de columna: Componente, Licencia, Herramienta de análisis, Ámbito y Tipo
Visualice las aplicaciones y las versiones correspondientes que usa un componente.	Haga clic en Ver versiones en la fila de un componente.
Ver la URL del paquete del componente y el enlace de Open Source Select	Haga clic en el icono Detalles .

1.5.3. Evaluaciones dinámicas

Una evaluación dinámica analiza una aplicación web en ejecución para buscar vulnerabilidades de seguridad. Las evaluaciones dinámicas incluyen pruebas automatizadas con tecnología OpenText DAST y análisis manual.

Las pruebas dinámicas con OpenText DAST abarcan los siguientes modos:

- Rastreo, el proceso mediante el cual OpenText DAST identifica la estructura del sitio web de destino
- Auditoría, el análisis de vulnerabilidades real

Esta sección contiene los siguientes temas:

- [Preparación del sitio web para la prueba dinámica](#)
- [Preparación de archivos de API web](#)
- [Configuración de OpenText Core Application Security Connect](#)
- [Configuración de análisis dinámicos](#)
- [Programación de análisis dinámicos](#)
- [Edición de la configuración de análisis dinámico para análisis en curso y completados](#)

1.5.3.1. Preparación del sitio web para la prueba dinámica

Para todas las evaluaciones dinámicas, realice los siguientes preparativos para facilitar el proceso de pruebas:

- Antes de iniciar la evaluación, confirme que la aplicación web y las credenciales de usuario funcionan. Si la aplicación web utiliza autenticación de certificado de cliente, póngase en contacto con el soporte técnico.
- Deshabilite todos los controles de autenticación multifactor durante el periodo de pruebas. Esto incluye mecanismos de autenticación secundaria como mensajes SMS, verificaciones por email, CAPTCHA, tokens de OATH y tokens físicos. La evaluación también puede realizarse sin autenticación para analizar la seguridad del contenido de la aplicación disponible para usuarios sin autenticación.
- Complete todas las pruebas funcionales y de rendimiento antes de la evaluación e inmovilice el código de la aplicación durante el periodo de pruebas.
- Como medida de precaución estándar, OpenTextel Portal de MSP recomienda que realice una copia de seguridad de todos sus datos antes de comenzar el proceso de pruebas. Una vez completadas las pruebas, restaure los datos a partir de una copia de seguridad que sepa que está en buen estado para evitar que se dañen los datos.
- Agregue las direcciones IP de OpenText Core Application Security a la lista de direcciones permitidas en los firewall, los IPS, los IDS y los WAF para garantizar que el equipo de pruebas dinámicas pueda analizar la aplicación. Puede obtener las direcciones IP de la página Configuración de análisis dinámico del portal. Es posible que se usen direcciones ad hoc con su consentimiento solo cuando las condiciones lo exijan.
- Proporcione las direcciones IP de OpenText Core Application Security a los equipos de operaciones de seguridad y redes, de manera que sepan que no deben bloquearlas si ven que se producen ataques contra el sitio, ya que estos forman parte del análisis de seguridad periódico previsto.
- Siempre y cuando se pueda acceder al sitio web mediante los puertos HTTP/HTTPS predeterminados (80/443), no deberá abrir puertos adicionales para la evaluación.
- Para sitios internos, utilice OpenText Core Application Security Connect para configurar la VPN de sitio a sitio. Para obtener más información, consulte [Configuración de Fortify en Demand Connect](#).

Para evaluaciones dinámicas que utilizan automatización durante el proceso de análisis, haga los siguientes preparativos:

- Cree macros de flujo de trabajo para ejecutar análisis controlados por flujo de trabajo. Una macro de flujo de trabajo es un registro de eventos HTTP cuando navega por un sitio web utilizando una herramienta Web Macro Recorder. Puede crear macros de flujo de trabajo con la Web Macro Recorder de OpenText DAST basada en eventos, disponible en la página Herramientas del portal. Para obtener instrucciones sobre cómo crear macros de flujo de trabajo, consulte la *Guía de herramientas de pruebas de seguridad de aplicaciones dinámicas de OpenText™* en [OpenText DAST Documentación](#).
- Cree macros de inicio de sesión para la autenticación. Una macro de inicio de sesión es un registro de los eventos que ocurren cuando accede e inicia sesión en un sitio web utilizando una herramienta Web Macro Recorder. Puede crear macros de inicio de sesión con la Web Macro Recorder de OpenText DAST basada en eventos, disponible en la página Herramientas del portal. Para obtener instrucciones sobre cómo crear macros de inicio de sesión, consulte la *Guía de herramientas de pruebas de seguridad de aplicaciones dinámicas de OpenText™* en [OpenText DAST Documentación](#).



Note

Si usa la API y cambia de un tipo de evaluación dinámica a un tipo de evaluación de DAST automatizada, cargue la macro de inicio de sesión a través del portal antes de comenzar el análisis.

1.5.3.2. Preparación de archivos de API web

Si una evaluación dinámica incluye pruebas de API web, debe proporcionar archivos de proyecto con datos de muestra funcionales para realizar pruebas de seguridad adecuadas. Prepare los archivos del proyecto de acuerdo con las siguientes instrucciones.



Note

Si no tiene archivos de proyecto con datos de muestra funcionales, solicite ayuda a los equipos de control de calidad o desarrollo para obtenerlos. Suelen tener conjuntos de archivos de este tipo para probar las funciones de las API web.

REST

- Proporcione una definición de API, como una URL o un archivo de documento de OpenAPI, o bien una URL o un archivo de colección Postman.



Note

No se admiten archivos de entorno de Postman.

- Las solicitudes deben incluir valores de parámetros válidos para establecer el comportamiento de la aplicación de línea de base.
- Si la API requiere autenticación, proporcione las credenciales que serán válidas durante el período de prueba.
 - Si proporciona una colección Postman, configure la autenticación en ella.



Note

No se admite la autenticación dinámica.

- Si va a proporcionar un documento de OpenAPI, dé las credenciales en la página Configuración de análisis dinámico.

SOAP

- Proporcione una URL o un archivo de Web Service Definition Language (WSDL).
- Proporcione pares de solicitud y respuesta en formato de texto o XML, o bien como archivo de colección Postman o proyecto de SoapUI.
- Las solicitudes deben incluir valores de parámetros válidos para establecer el comportamiento de la aplicación de línea de base.
- Si la API requiere autenticación, proporcione las credenciales que serán válidas durante el período de prueba.
- Si va a enviar un archivo de colección Postman o proyecto de SoapUI, configure la autenticación en el archivo del proyecto. También puede proporcionar la información en los campos **Notas adicionales** o **Documentación adicional**.

gRPC

- Proporcione un archivo de prototipo. Si se necesitan importaciones adicionales, deben combinarse con el archivo de prototipo principal en un archivo de prototipo "maestro". Los archivos de prototipo de gRPC deben ser autónomos. Cualquier importación debe ser a recursos reconocidos internamente y no a archivos generados por el usuario. OpenText DAST no puede identificar las rutas de archivo de los archivos proto importados.

GraphQL

- Proporcione un archivo o URL de introspección de GraphQL. La API de GraphQL debe tener habilitada la introspección para descargar el contenido del esquema para el análisis.

Ejemplos

Los siguientes ejemplos contienen archivos de proyecto con datos de muestra funcionales.

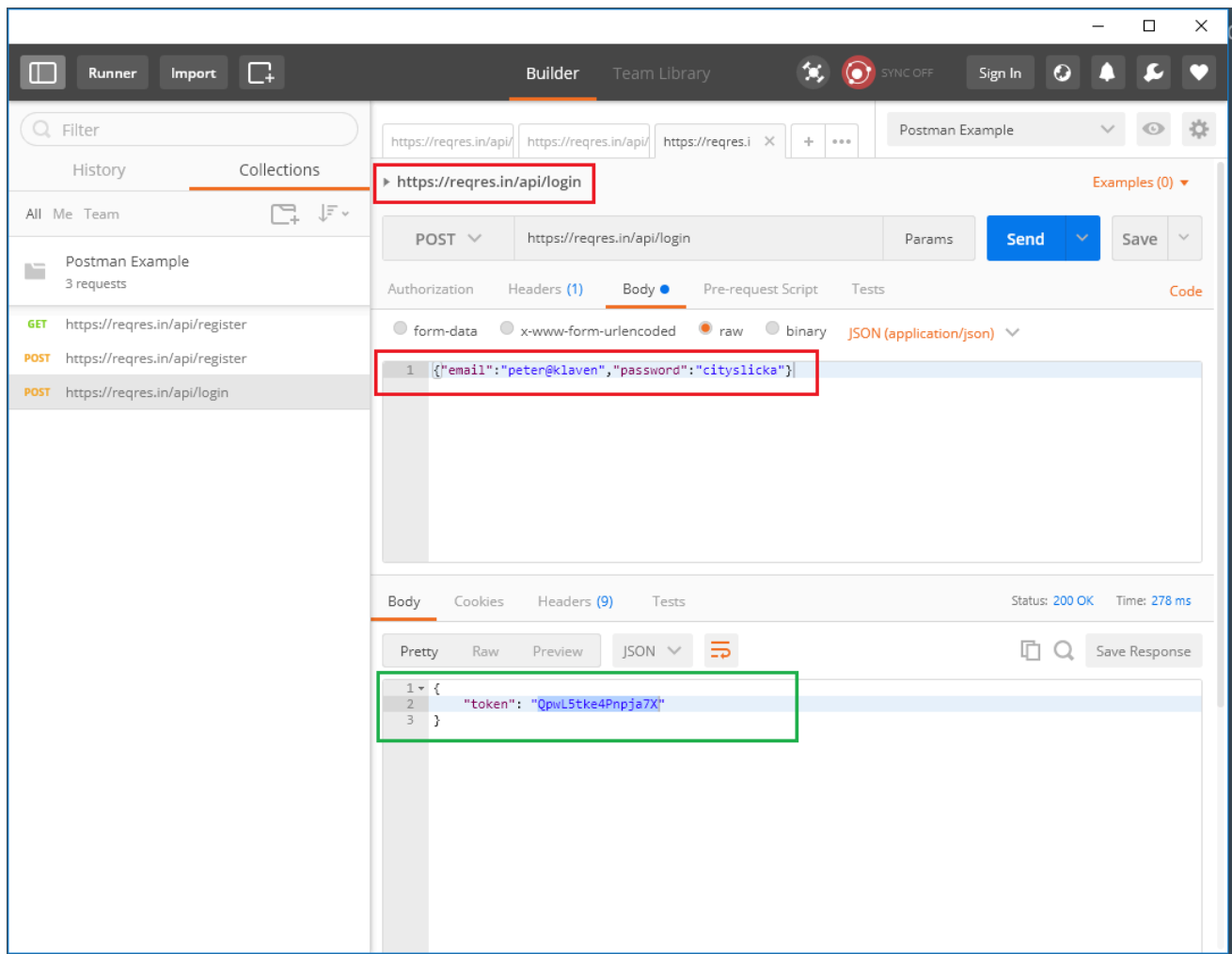


Note

Solo se deben proporcionar valores de parámetro de entrada; las respuestas que se muestran aquí solo tienen valor informativo.

Ejemplo 1 (REST)

El siguiente ejemplo muestra un extremo de API de REST que se ha cargado en la interfaz de usuario de Postman. El extremo gestiona la autenticación de una aplicación. La pantalla muestra una solicitud con los valores de entrada de nombre de usuario y contraseña correctos (en el cuadro rojo) y la respuesta de la aplicación (en el cuadro verde).



Ejemplo 2 (SOAP)

El siguiente ejemplo muestra un archivo WSDL que se cargó en la interfaz de usuario SOAPUI y que se actualizó con valores de parámetro funcionales. La pantalla muestra cuatro solicitudes con los valores de entrada correctos (en el cuadro rojo) y las respuestas correspondientes del servicio web (en el cuadro verde).

SoapUI 5.3.0

File Project Suite Case Step Tools Desktop Help

Empty SOAP REST Import Save All Forum Trial Preferences Proxy

Search Forum

Online Help

Inspector

Projects

- Example WSDL
 - DVWA Web Service Binding
 - check_user_information
 - Request 1
 - owasp_apitop10
 - Request 1
 - population
 - Request 1
 - return_price
 - Request 1

Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

Raw XML

```
<?xml version='1.0' encoding='UTF-8'>
<soapenv:Envelope xmlns:soapenv='http://www.w3.org/2001/XMLSchema-instance' xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>
  <soapenv:Header/>
  <soapenv:Body>
    <population soapenv:encodingStyle='http://schemas.xmlsoap.org/soap/encoding/'>
      <value_one xsi:type='xsd:string'>China</value_one>
    </population>
  </soapenv:Body>
</soapenv:Envelope>
```

SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"

SOAP-ENV:Body

ns1:populationResponse xmlns:ns1="http://schemas.xmlsoap.org/soap/encoding/"

return xsi:type="xsd:integer">1458</return>

ns1:populationResponse

SOAP-ENV:Body

SOAP-ENV:Envelope

Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

Raw XML

```
<?xml version='1.0' encoding='UTF-8'>
<soapenv:Envelope xmlns:soapenv='http://www.w3.org/2001/XMLSchema-instance' xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>
  <soapenv:Header/>
  <soapenv:Body>
    <return_price soapenv:encodingStyle='http://schemas.xmlsoap.org/soap/encoding/'>
      <name xsi:type='xsd:string'>Android</name>
    </return_price>
  </soapenv:Body>
</soapenv:Envelope>
```

SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"

SOAP-ENV:Body

ns1:return_priceResponse xmlns:ns1="http://schemas.xmlsoap.org/soap/encoding/"

return xsi:type="xsd:float">82.8</return>

ns1:return_priceResponse

SOAP-ENV:Body

SOAP-ENV:Envelope

Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

Raw XML

```
<?xml version='1.0' encoding='UTF-8'>
<soapenv:Envelope xmlns:soapenv='http://www.w3.org/2001/XMLSchema-instance' xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>
  <soapenv:Header/>
  <soapenv:Body>
    <check_user_information soapenv:encodingStyle='http://schemas.xmlsoap.org/soap/encoding/'>
      <username xsi:type='xsd:string'>admin</username>
    </check_user_information>
  </soapenv:Body>
</soapenv:Envelope>
```

SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"

SOAP-ENV:Body

ns1:check_user_informationResponse xmlns:ns1="http://schemas.xmlsoap.org/soap/encoding/"

return xsi:type="xsd:string">Admin, admin@comp.xyz, 6676 445</return>

ns1:check_user_informationResponse

SOAP-ENV:Body

SOAP-ENV:Envelope

Request 1

http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php

Raw XML

```
<?xml version='1.0' encoding='UTF-8'>
<soapenv:Envelope xmlns:soapenv='http://www.w3.org/2001/XMLSchema-instance' xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'>
  <soapenv:Header/>
  <soapenv:Body>
    <owasp_apitop10 soapenv:encodingStyle='http://schemas.xmlsoap.org/soap/encoding/'>
      <owaspid xsi:type='xsd:int'>9</owaspid>
    </owasp_apitop10>
  </soapenv:Body>
</soapenv:Envelope>
```

SOAP-ENV:Envelope SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"

SOAP-ENV:Body

ns1:owasp_apitop10Response xmlns:ns1="http://schemas.xmlsoap.org/soap/encoding/"

return xsi:type="xsd:string">Security Misconfiguration</return>

ns1:owasp_apitop10Response

SOAP-ENV:Body

SOAP-ENV:Envelope

Request Properties

Property	Value
Name	Request 1
Description	
Message Size	422
Encoding	UTF-8
Endpoint	http://192.168.81.128/dvws/vulnerabilities/wsdlenum/service.php
Timeout	
Bind Address	

Properties

SoapUI log http log jetty log error log wsrm log memory log

1.5.3.3. Configuración de OpenText Core Application Security Connect

Puede usar OpenText Core Application Security Connect para configurar fácilmente el VPN de sitio a sitio para evaluaciones dinámicas de aplicaciones web internas. OpenText Core Application Security Connect implementa una configuración de servidor y cliente OpenVPN para crear conexiones seguras de sitio a sitio. Debe instalar el cliente OpenVPN, disponible como contenedor Docker.

Las siguientes instrucciones asumen que está familiarizado con la instalación, configuración y uso de Docker.

Para configurar OpenText Core Application Security Connect:

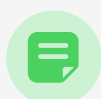
1. Extraiga la imagen de Docker de OpenText Core Application Security Connect en Docker Hub. El acceso al repositorio Fortify de Docker requiere credenciales y se otorga a través de su ID de Docker. Para acceder al repositorio de Docker de Fortify, envíe su ID de Docker por correo electrónico a fortifydocker@opentext.com.
2. Instale el contenedor Docker en un equipo Linux x86_64. El equipo debe cumplir con los siguientes requisitos:
 - Versión de motor Docker mínima admitida: 20.10.17
 - Acceso a la aplicación interna
3. (Líderes en seguridad) Agregar una red OpenText Core Application Security Connect en OpenText Core Application Security. Consulte [Agregar una red de OpenText Core Application Security Connect](#).
4. (Líderes en seguridad) Copie el comando de Docker para la red y ejecútelo en la máquina antes de programar el análisis dinámico. El siguiente es un comando de Docker de ejemplo:

```
docker run --name fdc_client -d \ -e
"FDC_ADDRESS=35.155.176.67:443" \ -e
"FDC_UNAME=fodconnect_username" \ -e
"FDC_UPSWD=fodconnect_password" \ -e "FDC_PROXY=3128" \ --
privileged fortifydocker/fortify-
connect:23.1.0.5.alpine.3.17
```

El ID del contenedor se devuelve si el comando de Docker es correcto.

1.5.3.4. Configuración de análisis dinámicos

Después de preparar la aplicación web para una evaluación dinámica, debe completar la página Configuración de análisis dinámico. Solo necesita configurar los ajustes de análisis dinámico una vez por versión, ya que la configuración se guardará para el próximo análisis. Puede editar la configuración como considere necesario en evaluaciones posteriores.



Note

La configuración de análisis dinámico anterior a la versión 22.4 se guardó a nivel de la aplicación. Guarde o actualice la configuración de análisis dinámico existente para que se guarde a nivel de la versión.

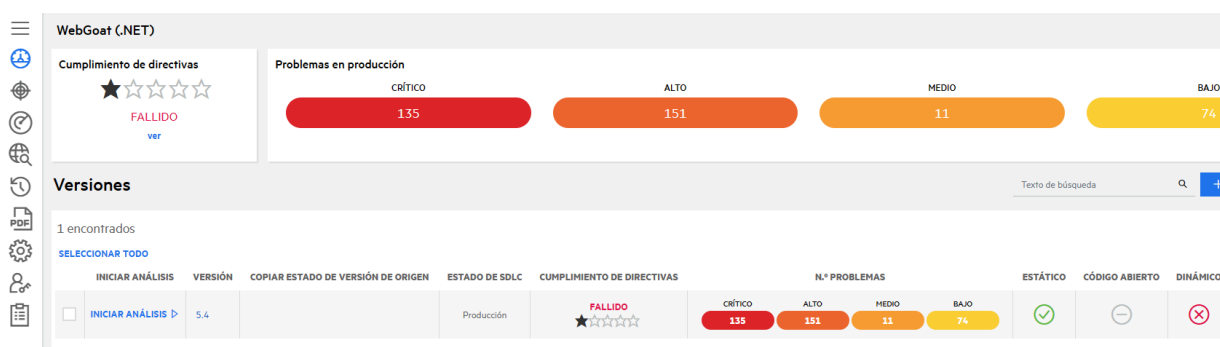
Para configurar un análisis dinámico:

1. Seleccione la vista Aplicaciones.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación.

Aparecerá la página Información general de la aplicación.



3. Haga clic en Iniciar análisis para la versión que desea evaluar y seleccione Dinámico.

Aparecerá la página Configuración de análisis dinámico.

4. Rellene los campos obligatorios. Los demás campos son opcionales o utilizan valores predeterminados.

Campo	Tipo de evaluación	Descripción
Tipo de evaluación		Seleccione un tipo de evaluación. Solo se muestran los tipos de evaluación que permite la directiva de seguridad de la organización. El SLO del tipo de evaluación seleccionado aparece debajo del campo.  Note La evaluación Dynamic+ API se usa para probar una API web donde no está disponible un archivo de definición.

Campo	Tipo de evaluación	Descripción
Tipo de análisis	DAST automatizada	Seleccione el tipo de análisis dinámico: ◦ Sitio web: este análisis es similar al análisis de un sitio web dinámico. ◦ Análisis controlado por flujo de trabajo: este análisis es similar a un análisis de sitio web dinámico que utilice una macro de flujo de trabajo. ◦ API: este análisis es similar a un análisis de API dinámica.
URL de sitio dinámica	◦ Todo tipo de sitios web ◦ API+	Indique la URL del sitio.

Campo	Tipo de evaluación	Descripción
Análisis controlado por flujo de trabajo	◦ Sitio web (opcional) ◦ DAST automatizado: análisis controlado por flujo de trabajo	Un análisis controlado por flujo de trabajo utiliza el modo de solo auditoría (sin rastreo) y está completamente automatizado. OpenText DAST audita solo las URL registradas en la macro y no sigue ningún hipervínculo encontrado durante la auditoría. Para la evaluación del sitio web, debe seleccionar la casilla de verificación para ejecutar el análisis en forma de análisis controlado por flujo de trabajo. Cargue la macro del flujo de trabajo (consulte Preparación del sitio web para la prueba dinámica). Las macros compatibles son archivos <code>.webmacro</code>, capturas de Burp Proxy y archivos <code>.har</code>.

Campo	Tipo de evaluación	Descripción
		 Note La aplicación que se analiza debe estar orientada hacia el exterior. La actividad registrada en una macro anula otra configuración de análisis.

Campo	Tipo de evaluación	Descripción
Derecho		Seleccione el derecho que la evaluación utilizará. El campo muestra los derechos que son válidos para el tipo de evaluación seleccionado, incluidos los que pueden comprarse. Si la versión tiene una suscripción activa, solo se muestran las opciones que no usan derechos.

Campo	Tipo de evaluación	Descripción
		 Note El cambio de evaluación dinámica o dinámica+ a evaluación de DAST automatizada no consume unidades de evaluación. Sin embargo, cambiar de la evaluación de DAST automatizada a otra evaluación consume el coste de la nueva evaluación.
Zona horaria		Seleccione la zona horaria de su ubicación, ya que se utilizará para programar la hora de inicio del análisis.

Campo	Tipo de evaluación	Descripción
Expuesto al entorno		Seleccione si el sitio es interno o externo.

Campo	Tipo de evaluación	Descripción
Solicitar eliminación de falso positivo (opcional)	DAST automatizado	☐ Solicitar eliminación de falso positivo[?] Seleccione la casilla de verificación para solicitar la eliminación de falsos positivos por parte del equipo de pruebas una vez por cada aplicación. Esta opción está seleccionada de forma predeterminada si los complementos de DAST automatizada están permitidos en la directiva de seguridad; si no es así, la opción está deshabilitada.

Campo	Tipo de evaluación	Descripción
		 Important La generación de macros de inicio de sesión y la eliminación de falsos positivos se ofrecen como un servicio opcional que está disponible una vez por cada aplicación y consume 1 unidad de evaluación adicional.

Campo	Tipo de evaluación	Descripción
		 Important Si desea solicitar tanto la generación de macros de inicio de sesión como la eliminación de falsos positivos, debe seleccionar ambas opciones juntas; una vez que se haya completado un análisis que incluya cualquiera de las opciones, ambas se desactivarán para análisis posteriores.

Campo	Tipo de evaluación	Descripción
Usar Fortify on Demand Connect (opcional)		El momento de activación interno cuando configurar una VPN entre el sitio y Fortify on Demand Connect.  (Opcional) Si el sitio es interno, marque la casilla de verificación para usar OpenText Core Application Security Connect para configurar una VPN de sitio a sitio y luego seleccione la red de OpenText Core Application Security Connect que se ha configurado para el sitio. Para obtener más información, consulte Configuración de Fortify en Demand Connect.  Important Se debe inicializar una conexión entre el cliente VPN y el servidor VPN antes de programar el análisis.

Campo	Descripción
Analizar el host completo (<URL>)	Seleccione una de las siguientes opciones: Analizar todo el host (<URL>) (predeterminada): se analizará todo el host. Ejemplo: Para https://foo.com/home, se incluirán las siguientes URL: - https://foo.com/ - https://foo.com/contact-us.html - https://foo.com/folder/ - https://foo.com/folder/folder2/page.aspx - https://foo.com/home/folder/ - https://foo.com/home/index.html Restringir el análisis al directorio y los subdirectorios de la URL: solo se analizarán el directorio indicado por la última barra diagonal de la URL y sus subdirectorios. Si selecciona esta opción, asegúrese de que la última barra diagonal indique el directorio al que desea restringir el análisis. Ejemplo: Para https://foo.com/home/, se excluirán las siguientes URL: - https://foo.com/ - https://foo.com/folder/ - https://foo.com/contact-us.html

Campo	Descripción
Restringir el análisis al directorio y subdirectorios de la URL	■ https://foo.com/folder/folder2/page.aspx

Campo	Descripción
Permitir HTTP (:80) y HTTPS (:443)	Active la casilla para permitir el análisis de HTTP y HTTPS del sitio (predeterminada). Ejemplo: Para https://foo.com/home, si se selecciona la opción Analizar todo el host, se incluirán http://foo.com/ y sus subdirectorios. Si se selecciona la opción Restringir el análisis al directorio y subdirectorios de la URL, solo se incluirán http://foo.com/home y sus subdirectorios.  Important Este campo no es aplicable para evaluación dinámica y evaluación dinámica+ de sitios web.

Campo	Descripción
Permitir el envío de formularios durante el rastreo	Seleccione la casilla de verificación para permitir envíos de formularios durante el rastreo de un sitio (predeterminado). Esto descubre un área de superficie adicional de la aplicación que puede examinarse para que el análisis sea más exhaustivo. No seleccionar la casilla de verificación no evita el envío de formularios durante las comprobaciones de vulnerabilidad. La detección de varias vulnerabilidades críticas, como la inyección de SQL y los scripts entre sitios, requieren el envío de formularios. Para excluir funcionalidades web específicas de los envíos, especifique esas URL en el campo Excluir URL que contengan.  Important Para evaluación dinámica y evaluación dinámica+ de sitios web, este campo está desactivado y no se puede modificar.

Campo	Descripción
Excluir URL que contengan	(Opcional) Escriba una URL completa o parcial, y haga clic en + para excluir las URL que coincidan con la cadena del análisis. Agregue una nueva entrada para cada cadena. El campo no distingue entre mayúsculas y minúsculas. Ejemplo: https://foo.com/login.html, login.html

Campo	Descripción
Incluir URL	(Opcional, evaluaciones dinámica+ de sitios web y dinámica de sitios web) De forma predeterminada, OpenText Core Application Security no analiza las URL fuera del dominio de nivel superior proporcionado. Para auditar recursos vinculados al dominio URL de sitio dinámica, como subdominios, API y recursos externos, escriba la URL y haga clic en +. Agregue una nueva entrada para cada URL adicional. No incluya direcciones URL que estén bajo el dominio URL del sitio dinámica, dominios externos o aplicaciones de terceros. Ejemplo: con https://foo.com/home, las URL válidas incluyen: ◦ www.foo.com (subdominio) ◦ API.aws.com (API) ◦ authfoo.com/login ◦ api.foo.com ◦ api.foo2.com

Ámbito (sitio web dinámico en forma de análisis controlado por flujo de trabajo)

Para editar el ámbito del análisis, haga clic en **Ámbito**. Aparecerá una lista de los hosts definidos en la macro de flujo de trabajo. Seleccione los hosts que se van a analizar.

▼ Ámbito

Cuando una macro se ejecuta, extrae datos de diferentes URL, lo que puede no resultar obvio al compilar la macro. Por ejemplo, cada vez que se muestra un anuncio en una página, se asocia una URL externa a dicho anuncio. Si desea que el análisis realice comprobaciones en ese sitio, debe indicar el nombre de host como host permitido más abajo

☐ zero.webappsecurity.com:80 ☐ zero.webappsecurity.com:443

Ámbito (DAST automatizado)

Para editar el ámbito del análisis, haga clic en **Ámbito** y complete los campos según sea necesario.

▼ Ámbito

Fortify on Demand puede analizar todo el host de la URL designada. Durante la evaluación no se analizarán otros dominios y subdominios.

☒ Analizar todo el host (zero.webappsecurity.com) ☐ Restringir el análisis al directorio y subdirectorios de la URL [?]

Excluir las URL que contienen

+

☐ Habilitar detección de páginas redundantes [?]

Compara la estructura de la página con cada página rastreada para identificar y excluir el procesamiento de recursos redundantes.

Directiva de análisis

Standard ▼

☐ Duración del análisis de Timebox (horas) [?]

Aplicar un límite de tiempo a un análisis limitará la actividad de análisis a esa duración.

Campo	Tipo de análisis	Descripción
Analizar el host completo (<URL>)	Sitio web	Seleccione una de las siguientes opciones: Analizar todo el host (<URL>) (predeterminada): se analizará todo el host. Ejemplo: Para https://foo.com/home, se incluirán las siguientes URL: - https://foo.com/ - https://foo.com/contact-us.html - https://foo.com/folder/ - https://foo.com/folder/folder2/page.aspx - https://foo.com/home/folder/ - https://foo.com/home/index.html Restringir el análisis al directorio y los subdirectorios de la URL: solo se analizarán el directorio indicado por la última barra diagonal de la URL

Campo	Tipo de análisis	Descripción
Restringir el análisis al directorio y subdirectorios de la URL		y sus subdirectorios. Si selecciona esta opción, asegúrese de que la última barra diagonal indique el directorio al que desea restringir el análisis. Ejemplo: Para <code>https://foo.com/home/</code>, se excluirán las siguientes URL: ▪ <code>https://foo.com/</code> ▪ <code>https://foo.com/folder/</code> ▪ <code>https://foo.com/contact-us.html</code> ▪ <code>https://foo.com/folder/folder2/page.aspx</code>

Campo	Tipo de análisis	Descripción
Excluir URL que contengan	Sitio web	(Opcional) Escriba una URL completa o parcial, y haga clic en + para excluir las URL que coincidan con la cadena del análisis. Agregue una nueva entrada para cada cadena. El campo no distingue entre mayúsculas y minúsculas. Ejemplo: https://foo.com/login.html, login.html

Campo	Tipo de análisis	Descripción
Habilitar detección de páginas redundantes	◦ Sitio web ◦ Análisis controlado por flujo de trabajo	Seleccione la casilla de verificación para permitir la comparación de la estructura de la página para determinar el nivel de similitud y permitir al sensor identificar y excluir el procesamiento de recursos redundantes.  Important La detección de páginas redundantes funciona en la fase de rastreo del análisis. Si la auditoría introduce una sesión que sería redundante, la sesión no se excluirá del análisis.

Campo	Tipo de análisis	Descripción
Política de análisis	Las directivas difieren según el tipo de análisis	Seleccione la política (colección de comprobaciones de vulnerabilidad y metodologías de ataque que el sensor implementa contra una aplicación web): Estándar: un análisis estándar incluye un rastreo automatizado del servidor y realiza comprobaciones de vulnerabilidades conocidas y desconocidas, como inyecciones de SQL y secuencias de comandos entre sitios, así como de un manejo deficiente de errores y de una configuración SSL débil en las capas del servidor web, el servidor de aplicaciones web y la aplicación web. Críticas y altas: utilice la política Críticas y altas para analizar rápidamente sus aplicaciones web en busca de las vulnerabilidades más urgentes y apremiantes, sin poner

Campo	Tipo de análisis	Descripción
		en peligro los servidores de producción. Esta política busca inyecciones de SQL, secuencias de comandos entre sitios y otras vulnerabilidades críticas y de alta gravedad. No contiene comprobaciones que puedan escribir datos en bases de datos o crear condiciones de denegación de servicio y es seguro ejecutarla en servidores de producción. Escaneo pasivo: la política de análisis pasivo analiza una aplicación en busca de vulnerabilidades detectables sin explotación activa, lo que hace que sea seguro ejecutarla en servidores de producción. Las vulnerabilidades detectadas por esta política incluyen problemas de divulgación de rutas, mensajes de error y otras de naturaleza similar.

Campo	Tipo de análisis	Descripción
		Api: La política de API contiene comprobaciones que abordan diversos temas relevantes en una evaluación de seguridad de API. Esto incluye diversos ataques de inyección, la seguridad de la capa de transporte y la violación de la privacidad, pero no incluye comprobaciones para detectar problemas del lado del cliente ni el descubrimiento de superficies de ataque, como la enumeración de directorios o comprobaciones de la búsqueda de archivos de copias de seguridad. Todas las vulnerabilidades detectadas por esta política podrían ser el objetivo directo de un atacante. Esta política no está destinada a analizar aplicaciones que consumen API web.

Campo	Tipo de análisis	Descripción
Duración del análisis de Timebox (horas)	◦ Sitio web ◦ API	Especifique la duración máxima del análisis. Si el análisis no se completa al final del período de duración especificado, el análisis finalizará y los resultados parciales estarán disponibles. Si el análisis se completa durante la el período de duración especificado, los resultados completos estarán disponibles. No es compatible con el análisis incremental.

Autenticación (dinámica sitio web, dinámica+ sitio web, dinámica manual, dinámica+ API, dinámica+, DAST manual)

Para editar la configuración de autenticación, haga clic en **Autenticación** y complete los campos según sea necesario.



Note

Los valores guardados en los campos de contraseñas se ocultan una vez realizada la configuración.

▼ Autenticación

☐ Se requiere autenticación mediante formulario

Nombre de usuario principal

Contraseña principal

Rol

Nombre de usuario secundario

Contraseña secundaria

Rol

Nombre de usuario 3

Contraseña 3

Rol

Campo	Descripción
Formulario Autenticación necesaria	(Opcional) Active la casilla si se requiere la autenticación de formularios. Proporcione nombres de usuario y contraseñas de al menos dos usuarios.  Note Para la autenticación durante evaluaciones dinámicas + y evaluaciones dinámicas manuales, puede proporcionar tres nombres de usuario, contraseñas y roles adicionales. Para indicar nombres de usuario, contraseñas y roles adicionales, haga clic en el signo más en la parte inferior del formulario. El rol es un campo opcional que admite hasta 32 caracteres.

Campo	Descripción
	 Important Haga preparativos para que las credenciales de usuario sigan siendo válidas durante todo el análisis, como aumentar la duración de la fecha de caducidad de la contraseña. El análisis se cancelará si falla la autenticación del sitio. Especificar las mismas credenciales para varios análisis activos simultáneamente puede generar demoras o resultados inexactos (debido al bloqueo de la cuenta, cambios de contraseña u otros eventos). Para evitar este problema, asegúrese de que los análisis que estén activos al mismo tiempo tengan credenciales distintas. Si está disponible, active la casilla Generar autenticación única si se requiere autoregistro.

Campo	Descripción
Red necesaria	(Opcional) Active la casilla de verificación si se requiere la autenticación de redes. Indique un nombre de usuario y una contraseña.
Instrucciones de autenticación adicional	(Opcional) Active la casilla si se requiere una autenticación adicional (p. ej., un número de cuenta o un código de inquilino) y escriba las instrucciones.  Important OpenText Core Application Security no admite la autenticación multifactor. Entre los ejemplos se incluyen los controles de autenticación que involucran mensajes SMS, verificaciones por email, CAPTCHA, tokens de OATH y tokens físicos.

Autenticación (DAST automatizado)

Para editar la configuración de autenticación, haga clic en **Autenticación** y complete los campos según sea necesario.



Note

Los valores guardados en los campos de contraseñas se ocultan. Puede borrar los campos de contraseña y proporcionar nuevos valores si es necesario.

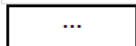
Autenticación

☒ Usar autenticación de sitio

☐ Solicitar creación de macro de inicio de sesión [?](#)

Las macros de inicio de sesión proporcionan acceso a ubicaciones protegidas de su aplicación. Por lo tanto, se recomienda utilizar una macro de inicio de sesión para aumentar la cobertura de su análisis. [?](#)

Please Upload your Login Macro File



 CARGAR

☒ Usar autenticación de red

Tipo de autenticación

Basic 

Nombre de usuario de red

Contraseña de red



Campo	Tipo de análisis	Descripción
Usar autenticación de sitio	Sitio web	(Opcional) Active la casilla de verificación si se requiere la autenticación de sitios. Cargue la macro de inicio de sesión (consulte Preparación del sitio web para la prueba dinámica).

Campo	Tipo de análisis	Descripción
		 Important Haga preparativos para que las credenciales de usuario sigan siendo válidas durante todo el análisis, como aumentar la duración de la fecha de caducidad de la contraseña. El análisis se cancelará si falla la autenticación del sitio. Especificar las mismas credenciales para varios análisis activos simultáneamente puede

Campo	Tipo de análisis	Descripción
		generar demoras o resultados inexactos (debido al bloqueo de la cuenta, cambios de contraseña u otros eventos). Para evitar este problema, asegúrese de que los análisis que estén activos al mismo tiempo tengan credenciales distintas.

Campo	Tipo de análisis	Descripción
Solicitar creación de macro de inicio de sesión	Sitio web	Seleccione la casilla de verificación para solicitar que el equipo de pruebas genere una macro de inicio de sesión una vez por cada aplicación. Una vez finalizado el análisis, la macro de inicio de sesión estará disponible para descargar en la página de Análisis. Esta opción está seleccionada de forma predeterminada si los complementos de DAST automatizada están permitidos en la directiva de seguridad; si no es así, la opción está deshabilitada.

Campo	Tipo de análisis	Descripción
		 Important La generación de macros de inicio de sesión y la eliminación de falsos positivos se ofrecen como un servicio opcional que está disponible una vez por cada aplicación y consume 1 unidad de evaluación adicional.

Campo	Tipo de análisis	Descripción
		 Important Si desea solicitar tanto la generación de macros de inicio de sesión como la eliminación de falsos positivos, debe seleccionar ambas opciones juntas; una vez que se haya completado un análisis que incluya cualquiera de las opciones, ambas se desactivarán para análisis posteriores.

Campo	Tipo de análisis	Descripción
Usar autenticación de red		(Opcional) Active la casilla de verificación si se requiere la autenticación de redes. Indique el tipo de autenticación, el nombre de usuario y la contraseña.  Note El análisis se cancelará si falla la autenticación de red.

API (DAST automatizada: API)

Si desea agregar instrucciones para el análisis de API web que utiliza el sitio, haga clic en **API**. Para obtener información sobre cómo preparar archivos de proyecto de API web adecuados para pruebas automáticas, consulte [Preparación de archivos de API web](#).

▼ API

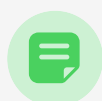
Para garantizar resultados de calidad y evitar pausas en los análisis, revise las instrucciones detalladas de las evaluaciones de las API. [?](#)

☒ API

Tipo de API

(Elija uno)

Seleccione el tipo de definición de API en el campo **Tipo de API: Postman Collection, OpenAPI**.



Note

Se admiten las versiones 2.0 y 3.0 de la especificación de OpenAPI.

Realice la tarea relevante en función del tipo de definición de API:

Tipo de definición de API	Procedimiento
Postman	Haga clic en ..., busque el archivo de colección Postman y selecciónelo. Se acepta el formato de archivo de JSON. Si ya existe un archivo, puede usarlo o cargar uno nuevo.

Tipo de definición de API	Procedimiento
colección Postman (URL)	✓ API Para garantizar resultados de calidad y evitar pausas en los análisis, revise las instrucciones detalladas de las evaluaciones de las API. ? Tipo de API Colección Postman Proporcione una URL para la colección Postman Se debe usar una SSL con el nombre del host Nombre de encabezado Valor de encabezado (dejar en blanco si no se modifica) Instrucciones adicionales Describir los encabezados, tokens, mecanismos de autenticación, etc. requeridos. 1. Proporcione la URL de la colección Postman (URL). 2. Si se necesita autenticación para acceder a la URL, proporcione el nombre del encabezado en Nombre de encabezado y las credenciales en los campos Valor de encabezado. Por ejemplo, proporcione Autorización en Nombre de encabezado y Bearer <token> en Valor de encabezado. Tenga en cuenta que esto es aparte de las credenciales usadas para autenticar solicitudes. Ejemplos: X-API-Key: <apikey> Authorization: <apikey> Authorization: Bearer <token> Note Si se pasan las credenciales como parámetro de consulta, inclúyalo en la URL.

Tipo de definición de API	Procedimiento
OpenAPI	Seleccione Archivo o URL de OpenAPI Specification y realice la tarea relevante según su selección.
	Archivo ◦ Haga clic en ..., busque el archivo de documento de OpenAPI y selecciónelo. Se acepta el formato de archivo de JSON. Si ya existe un archivo, puede usarlo o cargar uno nuevo. ◦ Si la API requiere de autenticación, proporcione el valor de clave de API en el campo Clave de API. Note El esquema de seguridad admitido es la clave de API. No se admiten varias claves de API en las solicitudes.

Tipo de definición de API	Procedimiento
	URL de OpenAPI Specification ◦ Proporcione la URL del documento de OpenAPI. ◦ Si la API requiere de autenticación, proporcione el valor de clave de API en el campo Clave de API. Note  El esquema de seguridad admitido es la clave de API. No se admiten varias claves de API en las solicitudes.

En el campo **Instrucciones adicionales**, proporcione las instrucciones adicionales.

API (API dinámica, API dinámica+, DAST manual)

Para obtener información sobre cómo preparar archivos de proyecto de API web adecuados para pruebas automáticas, consulte [Preparación de archivos de API web](#).

Si desea agregar instrucciones para el análisis de API web que utiliza el sitio, haga clic en **API**.

▼ API

Para garantizar resultados de calidad y evitar pausas en los análisis, revise las instrucciones detalladas de las evaluaciones de las API. [①](#)

☒ API

Tipo de API

Postman

Cargue sus archivos de Postman

El archivo de colección (flujo de trabajo) de Postman es obligatorio para continuar.

Seleccionar tipo de archivo

Flujo de trabajo ▼

...

 Cargar

Instrucciones adicionales

Describa los encabezados, tokens, mecanismos de autenticación y demás elementos necesarios.

Seleccione el tipo de definición de API en el campo **Tipo de API: SOAP, REST, Postman.**

Realice la tarea relevante en función del tipo de definición de API:

Tipo de definición de API	Procedimiento
SOAP	◦ Cargue un archivo WSDL que contenga datos de muestra de trabajo. Se aceptan los formatos de archivo JSON, WSDL, TXT y XML. ◦ (Opcional) En el campo Instrucciones adicionales escriba instrucciones adicionales, como los encabezados, los tokens o los mecanismos de autenticación necesarios. ◦ (Opcional) Proporcione el nombre de usuario y la contraseña, o la contraseña y la clave de la API.
REST	◦ Cargue un archivo de definición de API que contenga datos de muestra de trabajo. Se aceptan los formatos de archivo JSON, WSDL, TXT y XML. ◦ (Opcional) En el campo Instrucciones adicionales escriba instrucciones adicionales, como los encabezados, los tokens o los mecanismos de autenticación necesarios. ◦ (Opcional) Proporcione el nombre de usuario y la contraseña, o la contraseña y la clave de la API.

Tipo de definición de API	Procedimiento
Postman	◦ Cargue un archivo de definición de API que contenga datos de muestra de trabajo. Se aceptan los formatos de archivo JSON, WSDL, TXT y XML. ◦ En el campo Seleccionar tipo de archivo, seleccione el tipo de archivo como Workflow, Auth, Environment o Globals. El archivo de flujo de trabajo es obligatorio, mientras que los demás tipos de archivo son opcionales. ◦ (Opcional) En el campo Instrucciones adicionales escriba instrucciones adicionales, como los encabezados, los tokens o los mecanismos de autenticación necesarios. ◦ (Opcional) Proporcione el nombre de usuario y la contraseña, o la contraseña y la clave de la API.

Programación y disponibilidad (sitio web dinámico, sitio web dinámico+, API dinámica+)

Para editar la frecuencia de análisis y la configuración de disponibilidad del sitio, haga clic en **Programación y disponibilidad** y complete los campos según sea necesario.

Programación y disponibilidad

Frecuencia de repetición ⓘ

(No repetir)

Disponibilidad del sitio

DÍA	TODO EL DÍA	DE LAS 0:00 A LAS 4:00	DE LAS 4:00 A LAS 8:00	DE LAS 8:00 A LAS 12:00	DE LAS 12:00 A LAS 16:00	DE LAS 16:00 A LAS 20:00	DE LAS 20:00 A LAS 24:00
Domingo	☒	☐	☐	☐	☐	☐	☐
Lunes	☒	☐	☐	☐	☐	☐	☐
Martes	☒	☐	☐	☐	☐	☐	☐
Miércoles	☒	☐	☐	☐	☐	☐	☐
Jueves	☒	☐	☐	☐	☐	☐	☐
Viernes	☒	☐	☐	☐	☐	☐	☐
Sábado	☒	☐	☐	☐	☐	☐	☐

Fortify on Demand puede operar según las restricciones de disponibilidad de sus sitios. Sin embargo, reducir el periodo de análisis hará que el análisis tarde más tiempo que el SLA típico.

Campo	Descripción
Frecuencia de repetición	Seleccione la frecuencia de repetición del análisis: No repetir (predeterminado), 2 semanas, 1 mes, 2 meses, 3 meses, 4 meses, 6 meses, 12 meses. Si solicita un análisis único, utilice el valor predeterminado. Los análisis programados periódicos son automatizados y están sujetos a las siguientes condiciones: ◦ La programación de un análisis se produce siete días antes de la fecha de análisis calculada, la cual se determina a partir de la fecha de inicio del análisis anterior y la frecuencia de repetición. Por ejemplo, si un análisis programado mensualmente se inicia en el quinto día del mes, el próximo análisis se programará para el quinto día del mes siguiente. ◦ El derecho se deduce en el momento de la programación. ◦ Solo se programará un análisis si existe un derecho válido para el tipo de evaluación seleccionado en el momento de la programación. ◦ Si se cancela un análisis, no se programarán análisis adicionales. ◦ Si un análisis aún esta en curso cuando se debe programar el próximo análisis, OpenText Core Application Security intentará reprogramar el próximo análisis

Campo	Descripción
	una vez al día hasta que pase la fecha de análisis. Por ejemplo, si un análisis de programación mensual que empieza el 5 de cada mes está en curso el 5 del mes siguiente, el próximo intento de reprogramación se producirá siete días antes del 5 del mes posterior a dicha fecha.

Campo	Descripción
Disponibilidad del sitio	Active las casillas de verificación para indicar el momento en que el entorno está disponible para las pruebas. Utilice la hora local de la zona horaria especificada anteriormente. Debe proporcionar como mínimo un intervalo de cuatro horas de disponibilidad durante la semana.  Note Las restricciones a la disponibilidad del sitio pueden tener un efecto significativo en el tiempo de respuesta. Por ejemplo, si el tiempo de prueba se restringe a medio día, cabe esperar que las pruebas necesiten potencialmente el doble de tiempo. Póngase en contacto con el soporte técnico para obtener más información si hay restricciones de disponibilidad del sitio.

Detalles adicionales (dinámica de sitios web, dinámica+ de sitios web, dinámica+ de API)

Para agregar detalles adicionales sobre el análisis, haga clic en **Detalles adicionales**.

▼ Detalles adicionales

Subprocesos de solicitudes simultáneas [?]

☒ Estándar ☐ Limitado

Notas adicionales

Agregar notas o archivos adicionales requiere una revisión manual y aumenta el tiempo de respuesta.

Documentación adicional

...

Cargar

Cargar documentación o información adicional (límite de 30 MB)

Archivos cargados

No hay elementos para mostrar.

☐ Solicitar teleconferencia de evaluación previa

Esta función dejará de estar disponible a partir de la versión 26.1

Campo	Descripción
Subprocesos de solicitudes simultáneas	Seleccione el número de solicitudes simultáneas que se utilizarán para el análisis: ◦ Estándar (predeterminado): 5 subprocesos de solicitante de rastreo, 10 subprocesos de solicitante de auditoría, 20 segundos para el tiempo de espera de solicitud ◦ Limitado: 2 subprocesos de solicitante de rastreo, 3 subprocesos de solicitante de auditoría, 5 segundos para el tiempo de espera de solicitud Si se selecciona la opción Limitado, se reducirá la carga del análisis, pero el análisis tardará más en finalizar que el SLO estándar.
Notas adicionales	(Opcional) Escriba la información adicional que necesite el equipo de pruebas antes de comenzar con la evaluación.  Note Las notas de lista blanca y exclusión de formato libre se han migrado a este campo.

Campo	Descripción
Documentación adicional	(Opcional) Cargue la documentación (hasta 30 MB) que facilite la prueba de la aplicación. Los archivos cargados se muestran en la sección Archivos cargados que aparece a continuación. También puede descargar archivos que se enviaron previamente para evaluaciones dinámicas. Tipos de archivo compatibles: DOC, DOCX, PPT, TXT, PDF, PPTX, ZIP, XLS, XLSX y CSV.
Generar revisión virtual de WAF	 Note Póngase en contacto con el soporte para habilitar la opción WAF. (Opcional) Marque la casilla para generar una exportación de vulnerabilidades a un firewall de aplicación web (WAF). La exportación es un archivo XML que es compatible con los siguientes WAF: Imperva y F5. Cuando finalice la evaluación, podrá descargar el archivo de la página Análisis.

Campo	Descripción
Solicitar teleconferencia de evaluación previa	(Opcional, para evaluaciones dinámica premium y dinámica+) Active la casilla para solicitar una teleconferencia de evaluación previa. La casilla de verificación se desactiva cuando finaliza la evaluación.  Note No es posible solicitar una teleconferencia de evaluación previa para un análisis cuyo inicio se haya programado en las siguientes 72 horas. Esta función está obsoleta para la versión 25.4 y no estará disponible a partir de la versión 26.1.

6. Una vez que establezca los parámetros de evaluación, haga clic en **Guardar**.

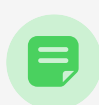
- Si el formulario está completo, **Estado de configuración** se marcará como **Válido**.
- Si el formulario no está completo, **Estado de configuración** se marcará como **Incompleto**. Se mostrará una lista de los problemas en la parte superior de la página. Puede situar el puntero sobre el icono **x** junto a **Estado de configuración** para mostrar la lista.

1.5.3.5. Programación de análisis dinámicos

Una vez que haya preparado su aplicación web y configurado los ajustes de análisis dinámico, puede programar el análisis dinámico. Puede haber un análisis dinámico en curso en todas las versiones de una aplicación.

Realice lo siguiente para programar un análisis dinámico:

1. Haga clic en Iniciar análisis.



Note

Si la aplicación ya tiene un análisis dinámico activo, no podrá iniciar otro análisis.

Se abrirá la ventana Iniciar análisis dinámico, la cual muestra la hora y la zona horaria actuales.

Iniciar análisis dinámico - <http://zero.webappsecurity.com/>



Fecha de inicio

Accesibilidad del sitio

Resumen

Esta URL se usa en otra aplicación.

Fecha de inicio

2017/11/17 03:16 pm

< **Noviembre 2017** >

Do	Lu	Ma	Mi	Ju	Vi	Sá
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Hora

Hora

Minuto

AHORA **LISTO**

ATRÁS

SIGUIENTE

INICIAR ANÁLISIS

2. Haga clic en el campo **Fecha de inicio**.

Haga clic en **Ahora** para programar un análisis inmediatamente o use el calendario para seleccionar una fecha y hora de inicio; luego, haga clic en **Listo**.

3. Haga clic en **Siguiente**.

Aparecen los resultados de la verificación de accesibilidad del sitio. La comprobación de accesibilidad del sitio busca los siguientes criterios:

- La URL resuelve.
- El DNS del nombre de host resuelve.
- OpenText Core Application Security recibe una respuesta HTTP válida.
- El servidor devuelve una respuesta válida (se indica el código de estado).
- La URL final, si hay algún redireccionamiento, está dentro del dominio de destino (aparece la URL final).
- Si la aplicación tiene funcionalidad de aplicación compleja o limitada (como vínculos, formularios o secuencias de comandos).
- Si se proporcionaron las credenciales actualizadas en caso de que se requiera autenticación.

Iniciar análisis dinámico - <http://zero.webappsecurity.com/>



Fecha de inicio

Accesibilidad del sitio

Resumen

La prueba de accesibilidad de la aplicación ha finalizado. ⓘ

- Formato URL válido
- Host válido
- Respuesta HTTP válida
- Se ha recibido una respuesta 200 OK
Código de estado: 200 - Correcto
- URL final válida en dominio de destino
URL final: <http://zero.webappsecurity.com:80/>
- Funcionalidad de aplicación detectada

ATRÁS

SIGUIENTE

INICIAR ANÁLISIS

Resuelva los problemas antes de comenzar el análisis para evitar que este se detenga.



Note

La verificación de accesibilidad del sitio está disponible para análisis de sitios web (con excepción de los sitios a los que se accede a través de VPN).

4. Haga clic en Siguiente.

Aparecerá un resumen de los valores de la configuración de análisis dinámicos.

Iniciar análisis dinámico - http://zero.webappsecurity.com/

✕

- ✓ Fecha de inicio
- ✓ Accesibilidad del sitio
- Resumen**

http://zero.webappsecurity.com/

Tipo de evaluación
Dynamic Premium - Suscripción (25 unidades)
El objetivo de nivel de servicio (SLO) de esta evaluación es de 7 días laborables Pacific Standard Time ?

Análisis de corrección
No

Zona horaria
(UTC+08:00) Taipei

Expuesto al entorno
Interno

Ámbito	Autenticación
Restringir al directorio y los subdirectorios No	Autenticación necesaria Sin autenticación
Permitir HTTP (:80) y HTTPS (:443) Sí	VPN necesaria No
Permitir el envío de formularios Sí	Autenticación adicional No
Exclusiones No	Detalles de autenticación adicional (Ninguno)

Si inicia esta evaluación, da su consentimiento para la realización de una evaluación de seguridad de la aplicación. ⓘ

ATRÁS SIGUIENTE INICIAR ANÁLISIS

5. Revise el resumen. Si es necesario, haga clic en **Atrás** y realice las correcciones. Si los valores son correctos, haga clic en **Iniciar análisis**.

Se le redirigirá a la página Análisis de versión; su nuevo escaneo tiene un estado **Programado**. El análisis comenzará a la hora programada. Si programa análisis periódicos, la versión se analizará en los intervalos que definió hasta que actualice su configuración de análisis dinámico.

Temas relacionados

Además de utilizando el portal, puede enviar una evaluación estática utilizando los siguientes métodos:

- Herramientas de integración del servidor de compilación: Fortify extensión de Azure DevOps, complemento OpenText Core Application Security de Jenkins. Para obtener más información, consulte [Herramienta de CI/CD](#).
- API de OpenText Core Application Security. Para obtener más información, consulte [OpenText Core Application Security API](#).

1.5.3.6. Edición de la configuración de análisis dinámico para análisis en curso y completados

Puede editar la configuración de análisis dinámico para análisis programados que no se han iniciado y análisis en pausa. Si necesita editar la configuración de análisis para un análisis en curso, cree un vale del Centro de ayuda para pausar el análisis. El equipo de pruebas responderá al vale.

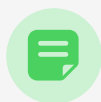
Los siguientes campos no se pueden editar después de programar un análisis dinámico:

- **Tipo de evaluación.** Cancele el análisis para editar el campo.
- **URL de sitio dinámica.** Si la versión no tiene un análisis completado, cancele el análisis para editar el campo. De lo contrario, el campo está bloqueado.

Además, al completar con éxito un análisis dinámico, los siguientes campos se establecen en los valores del análisis completado y se bloquean para su edición:

- **URL de sitio dinámica.**
- **Tipo de análisis**
- Todos los campos en la sección **Ámbito** (excepto para análisis automatizados de DAST)
- Campos de análisis controlado por flujo de trabajo
- Todos los campos de la sección **Autenticación**, a excepción de los campos nombre de usuario y contraseña.
- Todos los campos de la sección **API**, a excepción de los campos nombre de usuario y contraseña y los archivos cargados del proyecto.

Para editar estos campos, cree otra versión con la función de copia de estado y vuelva a configurar los ajustes de escaneo.



Note

Si está cambiando de un tipo de evaluación dinámica a un tipo de evaluación de DAST automatizada, puede editar la configuración del análisis dinámico. La configuración del análisis de DAST automatizada debe coincidir con la configuración del análisis de evaluación dinámica. Por ejemplo, si el tipo de evaluación original de la versión era Sitio web dinámico, el nuevo tipo de evaluación debe ser Sitio web de DAST automatizada.

Si el tipo de definición de API es una URL GraphQL, el cambio de API dinámica a DAST automatizada solo se admite a través del portal.

1.5.4. Evaluaciones móviles

Una evaluación móvil realiza pruebas en una aplicación móvil. Ofrece prueba de seguridad en el cliente, la red y el servidor back-end. OpenText Core Application Security es compatible con las siguientes plataformas: Android, iOS.

Esta sección contiene los siguientes temas:

- [Plataformas compatibles y sistemas operativos](#)
- [Preparación de archivos en evaluaciones móviles](#)
- [Preparación del back-end para la prueba móvil](#)
- [Configuración de análisis móviles](#)
- [Programación de análisis móviles](#)
- [Edición de la configuración de análisis móvil para un análisis en curso](#)

1.5.4.1. Plataformas compatibles y sistemas operativos

Plataformas de hardware

OpenText Core Application Security admite las siguientes plataformas de hardware:

	Móvil	Móvil+
Teléfono (formato pequeño)	N/D	Sí
Tableta (formato grande)	N/D	Sí
SIM/servicio móvil	N/D	Sí
Tipo de hardware (Apple Watch, Samsung Galaxy)	N/D	No

Sistemas operativos y arquitecturas

OpenText Core Application Security es compatible con los siguientes sistemas operativos y arquitecturas nativas:

	Móvil	Móvil+
Versión mínima de iOS (<code>MinimumOSVersion</code>)	N/D	Hasta 17.6
Arquitectura nativa de iOS	ARMv7, ARM64	ARMv7, ARM64
Versión mínima de Android (<code>android:minSdkVersion</code>)	N/D	Hasta 32 (Android 12)
Arquitectura nativa de Android	ARMv7, ARM64	ARMv7, ARM64

1.5.4.2. Preparación de archivos en evaluaciones móviles

El primer paso en una evaluación móvil es preparar el archivo binario de la aplicación móvil para su carga en OpenText Core Application Security. Con el fin de garantizar un análisis eficaz de la aplicación móvil, prepare sus archivos de acuerdo con las instrucciones que se proporcionaron para el marco de la aplicación móvil.

Esta sección contiene los siguientes temas:

- [Preparación de archivos de aplicaciones Android \(binarios\)](#)
- [Preparación de archivos de aplicaciones iOS \(binarios\)](#)

1.5.4.2.1. Preparación de archivos de aplicaciones Android (binarios)

Para las aplicaciones de Android, prepare el archivo binario (.aab o .apk) de su aplicación de acuerdo con las siguientes instrucciones.

- Asegúrese de que la aplicación no requiera características de MDM.
- Proporcione el archivo binario en su totalidad. Dado que solo se prueba el archivo enviado, no se admiten las características que requieren actualizaciones de aplicaciones.
- Para las evaluaciones que incluyen pruebas en el dispositivo (Mobile+), asegúrese de que la aplicación enviada se puede instalar y ejecutar en un dispositivo físico.
- Para facilitar la prueba de las evaluaciones de Mobile+, deshabilite cualquier mecanismo de anclaje de certificados, de detección de raíces o de manipulación de aplicaciones. Dejar estas características puede derivar en limitaciones de prueba que tienen un impacto en la cobertura del análisis.
- La evaluación de Mobile+ de archivos AAB admite los módulos de características dinámicas que tienen `<dist:fusing dist:include="true" />` especificado en el manifiesto.



Important

- Si envía un análisis posterior de una aplicación, ya sea como un análisis de corrección o como un nuevo análisis, OpenTextel Portal de MSP recomienda que el identificador de aplicación (el nombre del paquete) se mantenga coherente para preservar la integridad del seguimiento de problemas entre análisis. El identificador de aplicación se usa para calcular los identificadores de problemas que hacen el seguimiento a problemas únicos. Si se cambia el identificador de aplicación entre análisis, muchos problemas preexistentes se mostrarán como "Nuevos" en lugar de "Existentes" en los resultados del análisis.

Temas relacionados:

Para obtener información sobre cómo cargar archivos binarios de Android para evaluaciones estáticas, consulte [Preparación de archivos de aplicaciones Android \(código fuente\)](#).

1.5.4.2.2. Preparación de archivos de aplicaciones iOS (binarios)

Para las aplicaciones de iOS, prepare el archivo binario (.ipa) de su aplicación de acuerdo con las siguientes instrucciones.

- Para la evaluación que incluye pruebas en el dispositivo (Mobile+), asegúrese de que la aplicación enviada se puede instalar y ejecutar en un dispositivo físico.
- Para facilitar la prueba de las evaluaciones de Mobile+, deshabilite cualquier mecanismo de anclaje de certificados o de manipulación de aplicaciones. Dejar estas características puede derivar en limitaciones de prueba que tienen un impacto en la cobertura del análisis.
- Asegúrese de que la aplicación no requiera características de MDM.
- Exporte la aplicación para el envío mediante los tipos de distribución compatibles siguientes:
 - Envío de App Store (el IPA debe contener código ejecutable, por lo que debe asegurarse de que la casilla de verificación **Incluir código bit** está desactivada al exportar la aplicación)
 - Ad Hoc



Note

Introduzca contenido de advertencia aquí...

- Enterprise
- Desarrollo



Important

Los siguientes tipos de distribución NO son compatibles:

- Descarga de IPA desde App Store. El archivo IPA está cifrado para el usuario que lo ha descargado.
- El envío de App Store con la configuración «Incluir código bit». El archivo IPA no contiene código ejecutable.

Dado que solo se prueba el archivo enviado, no se admiten las características que requieren actualizaciones de aplicaciones.



Note

- Si va a enviar un análisis posterior de una aplicación, ya sea como un análisis de corrección o como un análisis de una nueva versión, OpenTextel Portal de MSP recomienda que el identificador de aplicación (el identificador del paquete) se mantenga coherente para preservar la integridad del seguimiento de problemas entre análisis. El identificador de aplicación se usa para calcular los identificadores de problemas que hacen el seguimiento a problemas únicos. Si se cambia el identificador de aplicación entre análisis, muchos problemas preexistentes se mostrarán como "Nuevos" en lugar de "Existentes" en los resultados del análisis.
- Antes de instalar el IPA en un dispositivo, se renueva la firma para agregar los [derechos](#) necesarios para la evaluación de seguridad y para garantizar que pueda instalarse en nuestros dispositivos de prueba. Este proceso de renovación de firma puede quitar los [derechos](#) necesarios para ciertas funcionalidades de la aplicación o activar mecanismos de seguridad relacionados con la integridad de la aplicación. El equipo MAST mantiene y desarrolla varias técnicas para mitigar los problemas causados por la renovación de la firma. Si la funcionalidad crítica de la aplicación continúa viéndose afectada, el análisis puede ponerse en pausa mientras investigamos y recomendamos soluciones o alternativas.

Temas relacionados:

Para obtener información sobre cómo preparar la carga de archivos de código fuente de iOS para la carga, consulte [Preparación de archivos de aplicaciones iOS \(código fuente\)](#).

1.5.4.3. Preparación del back-end para la prueba móvil

Para las evaluaciones móviles que incluyen la prueba de aplicaciones web y back-end, realice los siguientes preparativos para facilitar el proceso de pruebas:

- Antes de iniciar la evaluación, confirme que la aplicación web o las credenciales de usuario funcionan.
- Complete todas las pruebas funcionales y de rendimiento antes de la evaluación, e inmovilice el código de la aplicación durante la realización de las pruebas de seguridad.
- Como medida de precaución estándar, OpenText recomienda que realice una copia de seguridad de todos sus datos antes de comenzar el proceso de pruebas. Una vez completadas las pruebas, restaure los datos a partir de una copia de seguridad que sepa que está en buen estado para evitar que se dañen los datos.
- La aplicación web debe ser de acceso público. OpenText Core Application Security no admite el análisis a través de VPN.
- Agregue las direcciones IP de OpenText Core Application Security a la lista de direcciones permitidas en los firewall, los IPS, los IDS y los WAF para garantizar que el equipo de pruebas móviles pueda analizar la aplicación. Puede obtener las direcciones IP en la página Configuración del análisis móvil del portal. Es posible que se usen direcciones ad hoc con su consentimiento solo cuando las condiciones lo exijan.
- Proporcione las direcciones IP de OpenText Core Application Security a los equipos de operaciones de seguridad y redes, de manera que sepan que no deben bloquearlas si ven que se producen ataques contra el sitio, ya que estos forman parte del análisis de seguridad periódico previsto.



Note

Siempre y cuando se pueda acceder al sitio web mediante los puertos HTTP/HTTPS predeterminados (80/443), no deberá abrir puertos adicionales para la evaluación.

1.5.4.4. Configuración de análisis móviles

Si es la primera vez que se envía una evaluación móvil de una versión, debe completar la página Configuración del análisis móvil. Solo necesita completar la página una vez por versión, ya que la configuración se guardará para el próximo análisis. Puede editar la configuración como considere necesario en evaluaciones posteriores.

Realice lo siguiente para configurar un análisis móvil:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación.

Aparecerá la página Información general de la aplicación.

Mobile 02-07-18

Cumplimiento de directivas: ★☆☆☆☆ FALLIDO VER

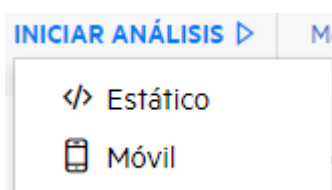
Problemas en producción: CRÍTICO 0, ALTO 22, MEDIO 0, BAJO 0

Estado de seguridad: APP DEFENDER DESHABILITADO

Versiones: 1 encontrados

INICIAR ANÁLISIS	VERSIÓN	ESTADO DE SDLC	CUMPLIMIENTO DE DIRECTIVAS	N.º PROBLEMAS				ESTÁTICO	MÓVIL	ÚLTIMO COMPLETADO
INICIAR ANÁLISIS >	1	Producción	FALLIDO ★☆☆☆☆	CRÍTICO 0	ALTO 22	MEDIO 0	BAJO 0	✓	📱	2018/02/14

3. Haga clic en Iniciar análisis para la versión que desea evaluar y seleccione Móvil en el menú.



Aparecerá la página Configuración del análisis móvil.

4. Rellene los campos según sea necesario. Los siguientes campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Tipo de evaluación	Seleccione un tipo de evaluación. Solo se muestran los tipos de evaluación que permite la directiva de seguridad de la organización. El SLO del tipo de evaluación seleccionado aparece debajo del campo.
Derecho	Seleccione el derecho que la evaluación utilizará. El campo muestra los derechos que son válidos para el tipo de evaluación seleccionado, incluidos los que pueden comprarse. Si la versión tiene una suscripción activa, solo se muestran las opciones que no usan derechos.
Tipo de marco	Seleccione el sistema operativo móvil: iOS, Android, Windows (solo para evaluaciones Premium).
Zona horaria	Seleccione la zona horaria de su ubicación, ya que se utilizará para programar la hora de inicio del análisis.

Campo	Descripción
Preferencia de auditoría	Seleccione la preferencia de auditoría. El valor se fija como Manual para las evaluaciones Móvil estándar, Móvil premium y Móvil+. Publicar automáticamente (sin auditoría): los resultados del análisis se publican de forma automática al completarse el análisis. Manual: los auditores revisan los resultados del análisis antes de publicarlos.
Plataforma de la aplicación	(Opcional) Seleccione la plataforma preferida de la aplicación: Teléfono o Tableta.

5. Si fuera necesario, puede establecer parámetros de análisis adicionales en las secciones que aparecen debajo de los campos obligatorios. Las secciones que están disponibles varían según el tipo de evaluación seleccionado.

Autenticación (móvil estándar, móvil premium y Mobile+)

Para editar la configuración de autenticación, complete los campos según corresponda en la sección **Autenticación**.

Autenticación

- ☐ Autenticación necesaria
- ☐ Autenticación multifactor

Campo	Descripción
Autenticación	(Opcional) Active la casilla si se requiere una autenticación e introduzca los nombres de usuario y las contraseñas de al menos dos usuarios. Para agregar más credenciales, use el campo Agregar notas [...] adicionales de la parte inferior del formulario.  Important Especificar las mismas credenciales para varios análisis activos simultáneamente puede generar demoras o resultados inexactos (debido al bloqueo de la cuenta, cambios de contraseña u otros eventos). Por ejemplo, puede programar análisis para las versiones Android y iOS de una aplicación al mismo tiempo. Para evitar este problema, asegúrese de que los análisis que estén activos al mismo tiempo tengan credenciales distintas.
Autenticación multifactor	(Opcional) Active la casilla si se necesita una autenticación multifactor e indique los detalles de esta.

API (móvil estándar, móvil premium y Mobile+)

Para agregar detalles sobre los servicios de API, complete los campos según corresponda en la sección **API**.

Servicios web

☒ Acceso a los servicios web

Exclusiones

URL de ejemplo: mail.google.com, Nota de ejemplo: La función de finalización de compra del carrito está conectada a los servidores de producción. No compruebe esta función.

El análisis de servicios web se limita a los sitios controlados por primeras partes. Los extremos de terceros (como Salesforce o Google Analytics) no se probarán sin la autorización escrita de los propietarios de los extremos.

Las evaluaciones de Fortify on Demand tendrán lugar en los intervalos IP y redes: 15.0.0.0/8, 16.0.0.0/8, 174.137.32.22/32, 62.73.140.103/32, 62.73.140.104/32

Disponibilidad del entorno

DÍA	TODO EL DÍA	DE LAS 0:00 A LAS 4:00	DE LAS 4:00 A LAS 8:00	DE LAS 8:00 A LAS 12:00	DE LAS 12:00 A LAS 16:00
Domingo	☒	☐	☐	☐	☐
Lunes	☒	☐	☐	☐	☐
Martes	☒	☐	☐	☐	☐
Miércoles	☒	☐	☐	☐	☐
Jueves	☒	☐	☐	☐	☐
Viernes	☒	☐	☐	☐	☐
Sábado	☒	☐	☐	☐	☐

< >

Fortify on Demand puede operar según las restricciones de disponibilidad de sus sitios. Sin embargo, reducir el periodo de análisis hará que el análisis tarde más tiempo que el SLA típico.

Campo	Descripción
Acceso a las API	(Opcional) Active la casilla para permitir que OpenText Core Application Security analice las API web que utiliza la aplicación.
Exclusiones	(Opcional) Enumere los sitios web, los servicios web back-end, las API web o los servicios internos con los que se comunica la aplicación a través de HTTP/HTTPS que se deben excluir durante el análisis. Esto proporcionará al equipo de pruebas el contexto y los límites adecuados para realizar el análisis; puede que se clasifiquen como vulnerabilidades los dominios no excluidos que se detecten.

Campo	Descripción
Disponibilidad del entorno	Active las casillas de verificación para indicar el momento en que el entorno está disponible para las pruebas. Utilice la hora local de la zona horaria anteriormente especificada. Las pausas y las reanudaciones de las pruebas provocan que el análisis tarde más que el SLA estándar que se suele asignar para un análisis. Póngase en contacto con el equipo de soporte para obtener más información si hay restricciones de disponibilidad del sitio.  Note Las modificaciones de aplicaciones durante periodos de apagón generan incertidumbre en los resultados.

Documentación adicional (móvil estándar, móvil premium y Mobile+)

Para agregar detalles adicionales sobre el análisis, rellene los campos según corresponda en la sección **Documentación adicional**.

Documentación adicional

Cargar documentación o información adicional (Límite de 30 MB)



Agregar notas de aplicación y evaluación adicionales

Enumere los requisitos especiales para probar esta aplicación, como: tarjeta SIM obligatoria, número de teléfono en funcionamiento obligatorio, restricciones de ubicación, detalles de anclaje de certificados, aplicación de root/jailbreak, etc.

☐ Solicitar teleconferencia de evaluación previa

Esta función dejará de estar disponible a partir de la versión 26.1

Archivos cargados

Nombre

Creado

No hay elementos para mostrar.

Guardar

☐ Iniciar análisis

Campo	Descripción
Cargar documentación o información adicional (límite de 30 MB)	(Opcional) Cargue la documentación (hasta 30 MB) que facilite la prueba de la aplicación. Los archivos cargados se muestran en la sección Archivos cargados que aparece a continuación. Tipos de archivo compatibles: DOC, DOCX, PPT, TXT, PDF, PPTX, ZIP, XLS, XLSX y CSV.
Agregar notas de aplicación y evaluación adicionales	(Opcional) Agregue la información que el equipo de pruebas necesite para compilar la aplicación correctamente.
Solicitar teleconferencia de evaluación previa	(Opcional, solo evaluaciones Premium y Móvil+) Active la casilla para solicitar una teleconferencia de evaluación previa. La casilla de verificación se desactiva cuando finaliza la evaluación.  Note No es posible solicitar una teleconferencia de evaluación previa para un análisis cuyo inicio se haya programado en las siguientes 72 horas. Esta función está obsoleta para la versión 25.4 y no estará disponible a partir de la versión 26.1.

- Una vez que complete la página Configuración del análisis móvil, haga clic en **Guardar**.

- Si el formulario está completo, **Estado de configuración** se marcará como **Válido**.
- Si el formulario no está completo, **Estado de configuración** se marcará como **Incompleto**. Se mostrará una lista de los problemas en la parte superior de la página. También puede situar el puntero sobre el icono **x** junto a **Estado de configuración** para mostrar la lista.

Próximo paso:

[Programación de análisis móviles](#)

1.5.4.5. Programación de análisis móviles

Una vez que haya preparado su aplicación móvil y configurado los ajustes de análisis móvil, puede realizar la carga y programar el análisis móvil. Puede haber un análisis móvil en curso en todas las versiones de una aplicación.

Realice lo siguiente para programar un análisis móvil:

1. Haga clic en Iniciar análisis.



Note

Si ya existe un análisis móvil activo en la aplicación, no podrá iniciar otro.

Se abrirá la ventana Iniciar análisis móvil.

Iniciar análisis móvil
✕

Fecha de inicio
 Seleccionar binario
 Validación de carga útil
 Resumen

Fecha de inicio
 24/01/2024 1:28
 (UTC -05:00) Hora del Este (EE. UU. y Canadá)

ATRÁS

SIGUIENTE

INICIAR ANÁLISIS

2. Haga clic en el campo **Fecha de inicio**.

Haga clic en **Ahora** para programar un análisis inmediatamente o use el calendario para seleccionar una fecha y hora de inicio; luego, haga clic en **Listo**.



Note

Este paso solo se aplica a los análisis móviles que incluyen pruebas de back-end.

3. Haga clic en **Siguiente**.

Aparece la página Seleccionar binario.

Iniciar análisis móvil

✓ StartDate

Seleccionar binario

Validación de carga útil

Resumen

Cargar binario de Android (.apk, .aab)

...

Asegúrese de que el archivo binario no incluya detección de root/jailbreak ni fijación de certificados. Los archivos binarios que no hayan quitado estas mitigaciones provocarán que se reduzca la cobertura del análisis.

ATRÁS

SIGUIENTE

INICIAR ANÁLISIS

4. Haga clic en ..., desplácese hasta el archivo binario y selecciónelo.



Note

La casilla de verificación **Anular validación de carga útil** aparece para cargas útiles superiores a 500 MB. Seleccione la casilla de verificación **Anular validación de carga útil** para omitir la validación de la carga útil móvil.

☐ Anular validación de carga útil

ATRÁS

SIGUIENTE

INICIAR ANÁLISIS

5. Haga clic en **Siguiente**.

Aparecen los resultados de la validación de carga útil. La validación de carga útil busca los siguientes criterios:

- La carga útil es un archivo zip válido. (Móvil, Móvil+)
- La carga útil es un formato de aplicación válido. (Móvil, Móvil+)
- La aplicación admite formatos de dispositivo estándar. (Móvil+)
- La aplicación admite las arquitecturas requeridas. (Móvil+)
- La aplicación tiene como objetivo una versión mínima compatible del sistema operativo. (Móvil+)
- El paquete ejecutable de la aplicación iOS contiene código ejecutable. (Móvil+)
- El paquete ejecutable de la aplicación IOS no está cifrado. (Móvil+)
- El paquete ejecutable de la aplicación iOS se ejecuta en un dispositivo físico. (Móvil+)

Iniciar análisis móvil

✓ StartDate

✓ SelectBinary

Validación de carga útil

Resumen

Resultado de la prueba de validación de carga útil ⓘ

✓ La carga útil es un archivo zip válido.

✓ La carga útil es un formato de aplicación válido: apk.

✓ La aplicación admite formatos estándar: teléfono, tableta.

✓ La aplicación admite las arquitecturas requeridas: arm64-v8a, armeabi-v7a.

✓ La aplicación tiene como objetivo una versión mínima compatible del sistema operativo: SDK 15.

ATRÁS

SIGUIENTE

INICIAR ANÁLISIS

OpenText El Portal de MSP recomienda resolver los problemas antes de comenzar el análisis para evitar que este se cancele. En algunos casos, el

equipo de pruebas puede continuar con el análisis a pesar de los fallos de validación. Seleccione **Sobrescribir errores de validación** para continuar con el siguiente paso. Para obtener más información sobre cómo sobrescribir errores de validación, póngase en contacto con el soporte.

6. Haga clic en **Siguiente**.

Aparece la página Resumen.

Iniciar análisis móvil

- ✓ StartDate
- ✓ SelectBinary
- ✓ Validación de carga útil
- Resumen**

Detalles del análisis

Fecha de inicio
24/01/2024 1:28:47

Zona horaria
(UTC -05:00) Hora del Este (EE. UU. y Canadá)

Tipo de evaluación
Evaluación móvil+

El objetivo de nivel de servicio (SLO) de la evaluación es de 3 días laborables, hora estándar del Pacífico. ?

Análisis de corrección
No

Detalles de la aplicación

Tipo de marco
Android

Plataforma de la aplicación
Aplicación para teléfonos y tablets

Autenticación necesaria
No

Al iniciar esta evaluación, usted reconoce que cuenta con la autorización para realizar una evaluación de seguridad de la aplicación. i

ATRÁS
SIGUIENTE
INICIAR ANÁLISIS

7. Revise el resumen. Si es necesario, haga clic en **Atrás** y realice las correcciones. Si los valores son correctos, haga clic en **Iniciar análisis**.

Se le redirigirá a la página Análisis de versión; su nuevo escaneo tiene un estado **Programado**. El análisis comenzará a la hora programada.



Note

Si usó un derecho móvil premium, habrá disponible un derecho estático asociado —llamado "<Nombre premium móvil> (origen)"— cuando inicie un análisis estático.

Temas relacionados

Además de utilizar el portal, puede enviar una evaluación móvil utilizando los siguientes métodos:

- API de OpenText Core Application Security. Para obtener más información, consulte [OpenText Core Application Security API](#).

1.5.4.6. Edición de la configuración de análisis móvil para un análisis en curso

Puede editar la configuración de análisis móvil para los análisis detenidos y los análisis programados que aún no se han iniciado. Tenga en cuenta que no puede editar los campos **Tipo de evaluación**, **Tipo de marco**, **Preferencia de auditoría** y **Plataforma de la aplicación**. Si necesita editar esos campos, cancele el análisis y vuelva a enviar la evaluación móvil.

Si necesita pausar un análisis en curso para editar la configuración del análisis, cree un vale en el Centro de ayuda. El equipo de pruebas responderá directamente al vale con datos actualizados. Para obtener más información sobre la creación de un vale del Centro de ayuda, consulte [Envío de un vale del Centro de ayuda](#).

1.5.5. Uso de derechos

El portal administra el uso de los derechos. La cantidad de derechos disponible se muestra en las páginas Configuración del análisis. Si se compraron análisis, se muestra el número de evaluaciones disponibles. Si compró unidades de evaluación, se muestran el coste unitario de cada evaluación y el número total de unidades disponibles en todos los derechos.

Cuando inicia o programa un análisis, el coste se deduce automáticamente de la cobertura de derechos. Los análisis únicos se deducen cada vez que realiza un análisis, mientras que una suscripción se deduce una sola vez y, luego, es válida para la aplicación hasta la fecha de finalización de la suscripción. Puede identificar una aplicación sujeta a una suscripción porque la fecha de finalización de la suscripción reemplaza el coste de los derechos.

Se ofrece información adicional sobre los derechos a través de los siguientes orígenes:

- Los mosaicos de panel de derechos activos y de uso de los derechos. Para obtener más información, consulte [Tipos de gráfico del panel](#).
- La exportación de datos de uso de los derechos. Para obtener más información, consulte [Creación de un Plantilla para la exportación de datos](#).
- La página Derechos en la vista Administración. Para obtener más información, consulte [Visualización de derechos](#).

1.5.6. Administración de análisis

Puede administrar las actividades de análisis tanto a nivel de inquilino, como de aplicación y como de versión. La página *Sus análisis* muestra los análisis del inquilino. Los usuarios pueden obtener más información sobre una aplicación. La página *Análisis de la aplicación* muestra los análisis ejecutados en la aplicación, mientras que la página *Análisis de versión* muestra los análisis ejecutados en la versión. En las páginas *Análisis*, que comparten un diseño y una funcionalidad similares, se proporciona una vista única en la que los usuarios pueden revisar los detalles del análisis y hacer un seguimiento del progreso de este.

Esta sección contiene los siguientes temas:

- [Visualización de todos los análisis](#)
- [Visualización de análisis de la aplicación](#)
- [Visualización de análisis de versión](#)
- [Desplazamiento por la página Análisis](#)
- [Filtrado de la página Sus análisis](#)
- [Comprobación del estado del análisis](#)
- [Cancelación de un análisis](#)
- [Reanudación de un análisis detenido](#)
- [Visualización de vales del Centro de ayuda vinculados a un análisis](#)

1.5.6.1. Visualización de todos los análisis

Puede ver los análisis de todas sus aplicaciones a nivel de inquilino.

Para ver análisis a nivel de inquilino:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus análisis**.

Aparecerá la página Sus análisis. La cantidad de derechos disponibles se muestra en la parte superior.

opentext | Core Application Security 26.1

Aplicaciones

Panel

Informes

Administración

🔍

📄

🔔

👤

🔄

AUTO-TAM

Sus análisis

360 unidades disponibles

380 problemas encontrados

12345→↩

Mostrar: 2550100

Seleccionar todo Hay 1 elementos seleccionados.

Editar atributos

Aplicación	Versión	Id. de análisis	Tipo de análisis	Tipo de evaluación	Estado	Aviator	Iniciado	Completado	# Problemas	
☒ Aviator 2025	Aviator 25.1.2	65116	Estático	Evaluación estática	✓	✗	2025/11/20	2025/11/20	44160161	📄 ⋮
☐ Prueba de corrección automática de Aviator	R1	64980	Estático	Evaluación estática	✓	✓	2025/10/10	2025/10/10	441600161	📄 ⋮
☐ Demostración del estado del auditor personalizado de Aviator	Guía de corrección	64971	Estático	Evaluación estática	✗	—	2025/10/10	2025/10/10		📄 ⋮
☐ Guía de corrección	R1	64961	Estático	Evaluación estática	✓	✗	2025/10/09	2025/10/09	441600161	📄 ⋮
☐ Guía de corrección	R1	64960	Estático	Evaluación estática	✓	✗	2025/10/09	2025/10/09	441600161	📄 ⋮
☐ Demostración del estado del auditor personalizado de Aviator	Guía de corrección	64959	Estático	Evaluación estática	✗	—	2025/10/09	2025/10/10		📄 ⋮
☐ Demostración del estado del auditor personalizado de Aviator	R1	64958	Estático	Evaluación estática	✓	✓	2025/10/09	2025/10/09	441600161	📄 ⋮
☐ Aplicación DAST 25.4	R1	64667	Dinámico	Evaluación dinámica de sitios web	🔒		2025/09/19			📄 ⋮
☐ Aviator 25.4	R3	64666	Estático	Evaluación estática	✓	✓	2025/09/19	2025/09/19	441600161	📄 ⋮
☐ Aviator 25.4	Atributos para Editar problemas en masa	64665	Estático	Evaluación estática	✓	✓	2025/09/19	2025/09/19	441600161	📄 ⋮
☐ Aviator 25.4	R1	64662	Estático	Evaluación estática	✓	✓	2025/09/19	2025/09/19	38700146	📄 ⋮

En la siguiente tabla, se describe cómo desplazarse por la página Sus análisis.

Tarea	Acción
Buscar en la lista de análisis	Escriba una palabra clave o una frase en el cuadro de texto de búsqueda y pulse Intro . Para quitar los resultados de búsqueda, elimine el texto del cuadro de búsqueda y haga clic en Intro . Para obtener más información, consulte Búsqueda de aplicaciones y versiones .
Mostrar u ocultar la lista de filtros	Haga clic en  .
Expandir o contraer filtros	Haga clic en expandir todo contraer todo  o en la flecha junto al nombre del filtro.
Ver los vales del Centro de ayuda asociados a un análisis	Haga clic en  .
Solicitar la cancelación de un análisis en curso	Haga clic en  y seleccione Cancelar análisis . Consulte Cancelación de un análisis en curso .
Ver el resumen de un análisis	Haga clic en  y seleccione Resumen del análisis . El resumen del análisis incluye el id. de análisis y una comparación con el análisis anterior.
Ver las notas de un análisis estático	Haga clic en  y seleccione Notas del análisis .

Tarea	Acción
Descargar resultados de análisis	Estático, dinámico y móvil: haga clic en ■ ■ ■ y seleccione Descargar resultados. Código abierto: haga clic en ■ ■ ■ y seleccione Descargar SBOM. Para descargar CycloneDX, seleccione CycloneDX. Para descargar SPDX, seleccione SPDX.
Descargar el manifiesto de la carga de análisis estático	Haga clic en ■ ■ ■ y seleccione Descargar el manifiesto. El manifiesto enumera archivos cargados y excluye imágenes, archivos multimedia y archivos CSS.
Descargar la carga de análisis estático	 Note Póngase en contacto con el soporte para habilitar la función de descarga de código fuente. Haga clic en ■ ■ ■ y seleccione Descargar código de origen para un análisis completo.

Tarea	Acción
Editar atributos	Seleccione uno o más análisis de la lista y haga clic Editar atributos o haga clic ■■■ y entonces seleccione Editar atributos.  Note Puede seleccionar uno o más análisis de la vista de lista de análisis y agregar valores de atributos personalizados. La ventana Editar atributos muestra los atributos del tipo de análisis, donde puede ingresar o actualizar valores según sea necesario.
Descargar árbol del sitio de análisis dinámico	Haga clic en ■■■ y seleccione Descargar árbol del sitio . Seleccionar CSV o JSON para el tipo de archivo.
Ver hosts detectados por el análisis dinámico	Haga clic en ■■■ y seleccione Hosts detectados . Los hosts detectados son hosts a los que la aplicación hace referencia, pero que no están especificados como hosts permitidos.
Enviar análisis de Debricked en SBOM	Haga clic en ■■■ y seleccione Enviar a Debricked . El SBOM debe estar disponible para su descarga.
Eliminar un análisis importado	Haga clic en ■■■ y Cancelar análisis importado . Consulte Eliminación de un análisis importado .

Tarea	Acción
Crear un archivo de exportación WAF	 Note Póngase en contacto con el soporte para habilitar la opción WAF. Haga clic en ■ ■ ■ y seleccione Enviar a WAF/IPS. La exportación es un archivo XML.

1.5.6.2. Visualización de análisis de la aplicación

Puede obtener más información de una aplicación y ver los análisis únicamente de esa aplicación.

Para ver análisis a nivel de aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación para la que desea ver los análisis que se han ejecutado.

3. Haga clic en **Análisis**.

Aparecerá la página Análisis de la aplicación, donde se muestran los análisis ejecutados en la aplicación.

Version	Id. de análisis	Tipo de análisis	Tipo de evaluación	Tipo de derecho	Estado	Iniciado	Completado	# Problemas
V2	49974	Código abierto	Debricked (importado)	N/A	✓	2022/09/01	2022/09/01	49 72 86 8 223
V1	49966	Código abierto	Sonatype (importado)	N/A	✓	2022/09/01	2022/09/01	49 72 86 8 223
V1	49726	Código abierto	Whitesource (importado)	N/A	✓	2022/08/25	2022/08/25	49 72 86 8 223
V2	49722	Código abierto	Módulo Node.js (importado)	N/A	✓	2022/08/25	2022/08/25	0 0 0 0 0
V2	49720	Código abierto	Módulo Node.js (importado)	N/A	✓	2022/08/25	2022/08/25	0 0 0 0 0
V1	49647	Código abierto	Debricked (importado)	N/A	✓	2022/08/24	2022/08/24	49 72 86 8 223

En la siguiente tabla se describe cómo desplazarse por la página Análisis de la aplicación.

Tarea	Acción
Ver los vales del Centro de ayuda asociados a un análisis	Haga clic en  .
Solicitar la cancelación de un análisis en curso	Haga clic en ■ ■ ■ y seleccione Cancelar análisis . Consulte Cancelación de un análisis en curso .
Ver el resumen de un análisis	Haga clic en ■ ■ ■ y seleccione Resumen del análisis . El resumen del análisis incluye el id. de análisis y una comparación con el análisis anterior.
Ver las notas de un análisis estático	Haga clic en ■ ■ ■ y seleccione Notas del análisis .
Descargar resultados de análisis	Estático, dinámico y móvil: haga clic en ■ ■ ■ y seleccione Descargar resultados. Código abierto: haga clic en ■ ■ ■ y seleccione Descargar SBOM. Para descargar CycloneDX, seleccione CycloneDX. Para descargar SPDX, seleccione SPDX.
Descargar el manifiesto de la carga de análisis estático	Haga clic en ■ ■ ■ y seleccione Descargar el manifiesto . El manifiesto enumera archivos cargados y excluye imágenes, archivos multimedia y archivos CSS.

Tarea	Acción
Editar atributos	Seleccione uno o más análisis de la lista y haga clic en Editar atributos o haga clic en [icon] y seleccione Editar atributos.  Note Puede seleccionar uno o más análisis de la vista de lista de análisis y agregar valores de atributos personalizados. La ventana Editar atributos muestra los atributos del tipo de análisis, donde puede ingresar o actualizar valores según sea necesario.
Descargar árbol del sitio de análisis dinámico	Haga clic en [icon] y seleccione Descargar árbol del sitio . Seleccionar CSV o JSON para el tipo de archivo.
Ver hosts detectados por el análisis dinámico	Haga clic en [icon] y seleccione Hosts detectados . Los hosts detectados son hosts a los que la aplicación hace referencia, pero que no están especificados como hosts permitidos.
Enviar análisis de Debricked en SBOM	Haga clic en [icon] y seleccione Enviar a Debricked . El SBOM debe estar disponible para su descarga.
Eliminar un análisis importado	Haga clic en [icon] y Cancelar análisis importado . Consulte Eliminación de un análisis importado .

Tarea	Acción
Crear un archivo de exportación WAF	 Note Póngase en contacto con el soporte para habilitar la opción WAF. Haga clic en ■ ■ ■ y seleccione Enviar a WAF/IPS. La exportación es un archivo XML.

1.5.6.3. Visualización de análisis de versión

Puede obtener más información de una versión y ver los análisis únicamente de esa versión.

Para ver análisis a nivel de versión:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

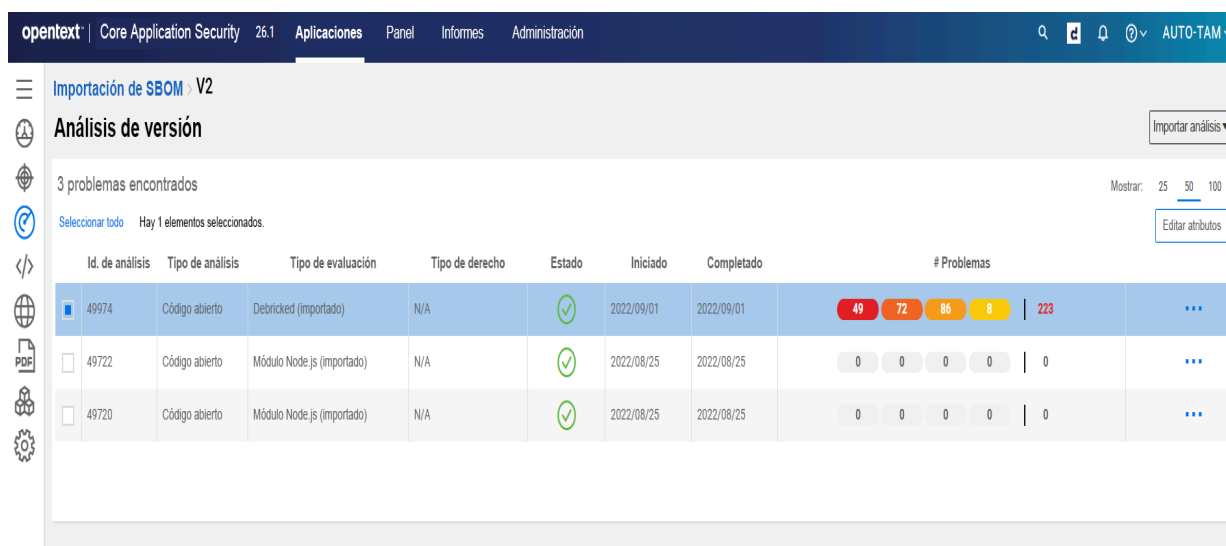
2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

3. Haga clic en el nombre de la versión para la que desea ver los análisis que se ejecutaron.

4. Haga clic en **Análisis**.

Aparecerá la página Análisis de versión, donde se muestran los análisis ejecutados en la versión.



	Id. de análisis	Tipo de análisis	Tipo de evaluación	Tipo de derecho	Estado	Iniciado	Completado	# Problemas	
☒	49974	Código abierto	Debricked (importado)	N/A	✓	2022/09/01	2022/09/01	49 72 86 8 223	...
☐	49722	Código abierto	Módulo Node.js (importado)	N/A	✓	2022/08/25	2022/08/25	0 0 0 0 0	...
☐	49720	Código abierto	Módulo Node.js (importado)	N/A	✓	2022/08/25	2022/08/25	0 0 0 0 0	...

En la siguiente tabla se describe cómo desplazarse por la página Análisis de versión.

Tarea	Acción
Importar un análisis	Haga clic en Importar análisis y seleccione el tipo de análisis. OpenText Core Application Security Admite resultados de análisis en las instalaciones (Importación de una lista de materiales de software) y resultados de análisis de código abierto (Importación de una lista de materiales de software).
Ver los vales del Centro de ayuda asociados al análisis	Haga clic en  .
Solicitar la cancelación de un análisis en curso	Haga clic en ■ ■ ■ y seleccione Cancelar análisis . Consulte Cancelación de un análisis en curso .
Ver el resumen de un análisis	Haga clic en ■ ■ ■ y seleccione Resumen del análisis . El resumen del análisis incluye el id. de análisis y una comparación con el análisis anterior.
Ver las notas de un análisis estático	Haga clic en ■ ■ ■ y seleccione Notas del análisis .
Descargar resultados de análisis	- Estático, dinámico y móvil: haga clic en ■ ■ ■ y seleccione Descargar resultados. - Código abierto: haga clic en ■ ■ ■ y seleccione Descargar SBOM. Para descargar CycloneDX, seleccione CycloneDX. Para descargar SPDX, seleccione SPDX.

Tarea	Acción
Descargar el manifiesto de la carga de análisis estático	Haga clic en ■ ■ ■ y seleccione Descargar el manifiesto. El manifiesto enumera archivos cargados y excluye imágenes, archivos multimedia y archivos CSS.
Descargar la carga de análisis estático	 Note Póngase en contacto con el soporte para habilitar la función de descarga de código fuente. Haga clic en ■ ■ ■ y seleccione Descargar código de origen para un análisis completo.
Editar atributos	Seleccione uno o más análisis de la lista y haga clic en Editar atributos o haga clic en ■ ■ ■ y seleccione Editar atributos.  Note Puede seleccionar uno o más análisis de la vista de lista de análisis y agregar valores de atributos personalizados. La ventana Editar atributos muestra los atributos del tipo de análisis, donde puede ingresar o actualizar valores según sea necesario.
Descargar árbol del sitio de análisis dinámico	Haga clic en ■ ■ ■ y seleccione Descargar árbol del sitio. Seleccionar CSV o JSON para el tipo de archivo.

Tarea	Acción
Ver hosts detectados por el análisis dinámico	Haga clic en ■ ■ ■ y seleccione Hosts detectados . Los hosts detectados son hosts a los que la aplicación hace referencia, pero que no están especificados como hosts permitidos.
Descargar macro de inicio de sesión	Haga clic en ■ ■ ■ y seleccione Descargar macro de inicio de sesión.
Error en la descarga del archivo de registros de los análisis de DAST automatizados	
Enviar análisis de Debricked en SBOM	Haga clic en ■ ■ ■ y seleccione Enviar a Debricked . El SBOM debe estar disponible para su descarga.
Eliminar un análisis importado	Haga clic en ■ ■ ■ y Cancelar análisis importado . Consulte Eliminación de un análisis importado .
Crear un archivo de exportación WAF	 Note Póngase en contacto con el soporte para habilitar la opción WAF. Haga clic en ■ ■ ■ y seleccione Enviar a WAF/IPS. La exportación es un archivo XML.

1.5.6.4. Desplazamiento por la página Análisis

En la siguiente tabla, se describe cómo desplazarse por la página Sus análisis, la página Análisis de la aplicación y la página Análisis de versión. Las páginas de Análisis comparten las mismas características excepto donde se indique lo contrario.

Tarea	Acción	Notas
Buscar en la lista de análisis	Escriba una palabra clave o una frase en el cuadro de texto de búsqueda y pulse Intro. Para quitar los resultados de búsqueda, elimine el texto del cuadro de búsqueda y haga clic en Intro. Para obtener más información, consulte Búsqueda de aplicaciones y versiones.	La búsqueda de texto solo está disponible en la página Sus análisis
Mostrar u ocultar la lista de filtros	Haga clic en  .	La opción de filtrar está disponible en la página Sus análisis. No está disponible en otras páginas de análisis. Para obtener más información, consulte Opciones de filtrado en la página Problemas .
Expandir o contraer filtros	Haga clic en  o en la flecha junto al nombre del filtro.	
Ver los vales del Centro de ayuda asociados a un análisis	Haga clic en  .	
Solicitar la cancelación de un análisis en curso	Haga clic en  y seleccione Cancelar análisis . Consulte Cancelación de un análisis en curso .	

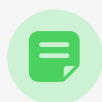
Tarea	Acción	Notas
Ver el resumen de un análisis	Haga clic en ... y seleccione Resumen del análisis . El resumen del análisis incluye el id. de análisis y una comparación con el análisis anterior.	
Ver las notas de un análisis estático	Haga clic en ... y seleccione Notas del análisis .	
Descargar resultados de análisis	Estático, dinámico y móvil: haga clic en ... y seleccione Descargar resultados. Código abierto: haga clic en ... y seleccione Descargar SBOM. Para descargar CycloneDX, seleccione CycloneDX. Para descargar SPDX, seleccione SPDX.	
Descargar el manifiesto de la carga de análisis estático	Haga clic en ... y seleccione Descargar el manifiesto . El manifiesto enumera archivos cargados y excluye imágenes, archivos multimedia y archivos CSS.	

Tarea	Acción	Notas
Descargar la carga de análisis estático	 Note Póngase en contacto con el soporte para habilitar la función de descarga de código fuente. Haga clic en ... y seleccione Descargar código de origen para un análisis completo.	La descarga de la carga del análisis estático solo está disponible en la página Sus análisis y en la página Versiones.

Tarea	Acción	Notas
Editar atributos	Seleccione uno o más análisis de la lista y haga clic en Editar atributos o haga clic en  y seleccione Editar atributos.  Note Puede seleccionar uno o más análisis de la vista de lista de análisis y agregar valores de atributos personalizados. La ventana Editar atributos muestra los atributos del tipo de análisis, donde puede ingresar o actualizar valores según sea necesario.	
Descargar árbol del sitio de análisis dinámico	Haga clic en  y seleccione Descargar árbol del sitio. Seleccionar CSV o JSON para el tipo de archivo.	

Tarea	Acción	Notas
Ver hosts detectados por el análisis dinámico	Haga clic en ... y seleccione Hosts detectados . Los hosts detectados son hosts a los que la aplicación hace referencia, pero que no están especificados como hosts permitidos.	
Descargar la macro de inicio de sesión utilizada en el análisis dinámico	Haga clic en ... y seleccione Descargar macro de inicio de sesión .	La macro de inicio de sesión está disponible para los siguientes tipos de análisis: sitio web de DAST automatizada, dinámica, dinámica+
Descargar el registro de análisis para un análisis dinámico fallido	Haga clic en ... y seleccione Descargar registro de análisis .	El registro de análisis está disponible para el análisis de DAST automatizada.
Enviar análisis de OpenText Core SCA en SBOM	Haga clic en ... y seleccione Enviar a Debricked . El SBOM debe estar disponible para su descarga.	
Eliminar un análisis importado	Haga clic en ... y seleccione Cancelar análisis importado . Consulte Eliminación de un análisis importado .	

Tarea	Acción	Notas
Crear un archivo de exportación WAF	 Note Póngase en contacto con el soporte para habilitar la opción WAF. Haga clic en ... y seleccione Enviar a WAF/IPS. La exportación es un archivo XML.	



Note

La duración de la disponibilidad la establece la [Directiva de retención de datos](#).

1.5.6.5. Filtrado de la página Sus análisis

Puede limitar los análisis que se muestran en la página Sus análisis aplicando filtros. Las siguientes opciones de filtro y agrupación están disponibles en la página Sus análisis:



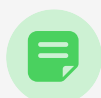
Note

Para que un filtro aparezca en la lista de filtros, los resultados deben contener varios valores para ese filtro.

Filtro	Descripción	Valores
Iniciado el	Intervalo de fechas en que comenzaron los análisis	
Completado el	Intervalo de fechas en que se completaron los análisis	
Tipo de evaluación	Tipo de evaluación del análisis	
Tipo de derecho	Tipo de derecho del análisis	Análisis único, N/A, Suscripción, Corrección
Es corrección	Si el análisis es un análisis de corrección.	Falso, Verdadero
Versión	Versión asociada con el análisis	
Estado de análisis	Estado de los análisis estático, dinámico, móvil y de red.	En curso, Completado, Cancelado, En espera
Tipo de análisis	Tipo de análisis	Estático, Dinámico, Móvil, Red, Código abierto

1.5.6.6. Comprobación del estado del análisis

Puede comprobar el estado del análisis en el portal. Los propietarios de versiones, los emisores de análisis y los usuarios en la lista de notificaciones de una aplicación también reciben notificaciones de correo electrónico sobre las siguientes actualizaciones del estado del análisis: inicio del análisis, finalización del análisis, cancelación del análisis y pausa del análisis, así como envío y finalización de desafíos de falso positivo.



Note

Los estados de análisis disponibles dependen del tipo de evaluación. Hay un límite de 25 análisis en curso por inquilino.

- Estático: una aplicación puede tener un análisis estático en curso para una versión (máximo de dos en curso por aplicación). Los análisis adicionales se ponen en cola y, luego, se ejecutan en el orden en que aparecen allí. Cada aplicación puede tener hasta 30 análisis en la cola.
- Código abierto: una aplicación puede tener un análisis OpenText Core SCA en curso para una versión (máximo de dos en progreso por aplicación). Los análisis adicionales se ponen en cola y, luego, se ejecutan en el orden en que aparecen allí
- Dinámico: una aplicación puede tener un solo análisis dinámico en curso a la vez. Los análisis no se pueden poner en cola.
- Móvil: una aplicación puede tener un solo análisis móvil en curso a la vez. Los análisis no se pueden poner en cola.

Para comprobar el estado del análisis de una aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación para la que desea comprobar el estado del análisis.

Aparecerá la página Información general de la aplicación.



3. Coloque el cursor sobre el icono de estado de análisis para obtener más información sobre el análisis más reciente de ese tipo de versiones.
4. Haga clic en un icono de estado para acceder a los detalles del estado del análisis directamente:
 - No iniciado: se le redirigirá a la página Configuración del análisis relevante.
 - Programado: se le redirigirá a la página Configuración del análisis relevante.
 - En curso: se le redirigirá a la página Análisis de versión o Análisis de la aplicación si una aplicación de microservicios tiene análisis estáticos en la cola.
 - En cola: se le redirigirá a la página Configuración del análisis relevante.
 - En pausa: se le redirigirá a la ventana de vales del Centro de ayuda en la página Análisis de versión.
 - Cancelado: se le redirigirá a la página Configuración del análisis relevante.
 - Completado: se le redirigirá a la página Problemas de versión (análisis estáticos, dinámicos y móviles) o a la página Problemas de la aplicación, las cuales estarán filtradas por el tipo de análisis relevante.



Note

Los análisis de DAST automatizada y de OpenText Core SCA pueden tener resultados parciales; el icono de estado del análisis para análisis completados que tienen resultados parciales está resaltado en naranja;

1.5.6.7. Cancelación de un análisis

Puede que deba cancelar un análisis que no se haya iniciado, o bien uno que se haya iniciado, pero que no se haya completado. El portal automatiza el procesamiento de la solicitud de cancelación. El coste de los derechos se reembolsará si se estima adecuado.

Para cancelar un análisis:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación para la cual desea cancelar un análisis.

Aparecerá la página Versiones.

3. Haga clic en **Análisis**.

Aparecerá la página Análisis de la aplicación.

</

4. Haga clic en **...** en la fila del análisis y seleccione **Cancelar análisis**.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí** para confirmar la cancelación del análisis.

- Los análisis con un estado **En cola** o **Programado** se cancelan automáticamente.
- Para los análisis con el estado **En curso**:
 - Si el análisis es estático y no se ha auditado, se cancela automáticamente.
 - Si el análisis es un análisis dinámico, móvil o estático auditado, se generará un vale del Centro de ayuda con la solicitud de cancelación y los detalles del análisis. Se envía un correo electrónico al equipo de pruebas, que luego cancela manualmente el análisis.

- Los análisis con el estado **En espera** se cancelan automáticamente. Se envía un correo electrónico al equipo de pruebas.

Cuando se cancela un análisis, los vales del Centro de ayuda asociados a este se marcan como resueltos.

1.5.6.8. Reanudación de un análisis detenido

El equipo de pruebas pausará un análisis si se necesita información adicional. Responda al vale del Centro de ayuda asociado para que se pueda reanudar el análisis. Tenga en cuenta que las pausas y las reanudaciones de las pruebas provocan que el análisis tarde más que el SLO estándar.



Note

Los análisis en pausa durante más de 21 días consecutivos se cancelan automáticamente. Los vales del Centro de ayuda asociados al análisis se marcan como resueltos.

Para reanudar un análisis detenido:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el icono de estado En pausa en la columna **Estado de seguridad y análisis** de la aplicación.

Se abrirá la ventana de vales del Centro de ayuda.

3. Haga clic en la sección **Vales pendientes**.

Se mostrarán los vales pendientes del análisis.

4. Haga clic en un vale para ver los comentarios.

5. Haga clic en **Agregar comentario público**.

Debajo aparecerá un cuadro de texto.

6. Escriba el comentario que se agregará al vale.

7. Haga clic en **+ Agregar comentario público**.

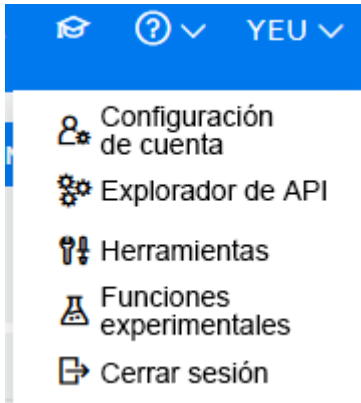
El comentario se agregará a los detalles del vale en el portal y en el Centro de ayuda. El estado de la evaluación cambiará a En curso.



Note

Si necesita agregar un archivo al vale, deberá hacerlo mediante el Centro de ayuda.

1. Haga clic en su nombre de cuenta.
2. Seleccione Centro de ayuda.



El Centro de ayuda se abrirá en una ventana independiente.

3. Haga clic en Ver vales.



Se muestra una nueva pantalla con una lista de vales enviados. Cada vale tiene un estado, que se muestra en la columna izquierda. Los estados posibles son **Nuevo**, **Abierto**, **Pendiente** y **Solucionado**.

4. Haga clic en Mostrar pendiente.

La lista muestra ahora solo los vales que requieren una acción de su organización.



Note

El número total de vales con estado Pendiente aparece como un número en rojo encima del vínculo Centro de ayuda en la parte superior de la página.

5. Haga clic en Respuesta y escriba su respuesta a la pregunta.

Tan pronto envía su respuesta, el estado de la evaluación vuelve a En curso.

1.5.6.9. Visualización de vales del Centro de ayuda vinculados a un análisis

Puede ver los vales del Centro de ayuda vinculados con un análisis activo en las páginas Sus análisis, Análisis de la aplicación y Análisis de versión.



Note

Si se ha detenido un análisis, podrá acceder a los vales del Centro de ayuda asociados a este desde cualquier página a nivel de versión haciendo clic en el botón **Vales del Centro de ayuda** de la barra de estado.

Para ver los vales del Centro de ayuda vinculados a un análisis activo:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación.

3. Haga clic en **Análisis**.

Aparecerá la lista de todos los análisis ejecutados en la aplicación o la versión.

</

4. Haga clic en el icono

Se abre la ventana modal Centro de ayuda, que muestra todos los vales pendientes, abiertos y solucionados asociados al análisis.

Help Center Tickets

✕

▼ Pending Tickets

1

Ticket: 70

Status: pending

Assessment Waiting for Customer Action

Assessment for Drupal - 7.25 is waiting for customer meaning we are having issues accessing the site...

> Add Public Comment

From: Dylan Thomas

2016/07/19 08:49:02 AM

Quick feedback!

From: Dylan Thomas

2016/07/19 06:23:04 AM

I swear they work! But I'm such a great customer, I'll update them anyway.
Sincerely,
Happy FoD customer

From: Dylan Thomas

2015/08/25 06:42:33 PM

Assessment for Drupal - 7.25 is waiting for customer meaning we are having issues accessing the site properly.

Assessment Type: Dynamic
Tenant: Dylan Tenant

Notes: The scan of your application has been paused because the credentials provided are not working. Please verify the credentials and notify the Help Center with the updated information so we may complete your scan. To chat with an FoD representative or log a support ticket, visit the FoD Help Center link on the FoD portal. For immediate assistance, use the Help Center Voice Channel (800)893-8141. Without your response, your scan may be cancelled.

We would appreciate it if you could log in and help us resolve the issues.
You can access the Assessment by going to [HTTPS://FODQA9-IIS2/Releases/Issues/1621](https://FODQA9-IIS2/Releases/Issues/1621)

Thanks.
HP Security Services

5. En la sección Vales pendientes, haga clic en un vale para ver sus comentarios.
6. Haga clic en **Agregar comentario público**.

Debajo aparecerá un cuadro de texto.
7. Escriba el comentario que se agregará al vale.
8. Haga clic en **+ Agregar comentario público**.

El comentario se agregará a los detalles del vale en el portal y en el Centro de ayuda.

1.6. Corrección de vulnerabilidades

Cuando el equipo de prueba complete el análisis, publicará los resultados del análisis en el portal. Inicie sesión en OpenText Core Application Security para ver los resultados del análisis y corregir las vulnerabilidades detectadas en la aplicación.

Esta sección contiene los siguientes temas:

- [Revisión de problemas](#)
- [Detalles del problema](#)
- [Actualizar problemas](#)
- [Auditoría de la corrección de problemas](#)
- [Auditoría y corrección con SAST Aviator](#)
- [Plantillas de auditoría](#)
- [Reglas de limpieza de flujo de datos](#)
- [Solicitud de un análisis de corrección](#)

1.6.1. Revisión de problemas

Puede ver información detallada sobre los problemas que se encontraron en un análisis tanto en el nivel de aplicación como de versión. En la página Problemas de la aplicación se muestran los problemas encontrados en todas las versiones de una aplicación (a excepción de las versiones retiradas). En la página Problemas de versión, se muestran los problemas encontrados en todos los análisis de una versión.

En las páginas de problemas de la aplicación y de versión, que comparten diseño y funcionalidad similares, se proporciona una sola vista integrada de los datos de problemas. Una página se divide en tres paneles:

- El panel de navegación muestra una lista de los problemas. Los problemas se organizan por su gravedad en pestañas individuales para cada nivel de gravedad y en una pestaña para todos los problemas.
- El panel de detalles de los problemas muestra información sobre el problema seleccionado en el panel de navegación. Los detalles se organizan en varias pestañas. Las pestañas disponibles dependen del tipo de análisis en el cual se encontró el problema.
- El panel de auditoría se puede contraer. Muestra campos de corrección del usuario del problema seleccionado en el panel de navegación, así como el estado del problema, la fecha en la que se introdujo y la fecha en la se encontró por última vez.

Los problemas tienen uno de los siguientes estados:

Estado	Descripción
Novedad	Una vulnerabilidad aparece por primera vez en el último análisis.
Existente	Una vulnerabilidad del último análisis aparece en uno o varios análisis anteriores, incluido el análisis inmediatamente anterior al último.
Reabierto	Apareció una vulnerabilidad en el último análisis y había aparecido antes, pero no en el análisis inmediatamente anterior al último. Dicho de otra forma, un problema no volvió a detectarse en uno o más análisis, por lo que parecía haberse solucionado; no obstante, volvió a aparecer posteriormente.
Solucionado/Solución validada	Una vulnerabilidad apareció al menos una vez, pero no se detectó en el último análisis. Las vulnerabilidades solucionadas están ocultas de forma predeterminada. Para ver las vulnerabilidades con el estado Solucionado , seleccione Mostrar... Solucionados en las páginas Información general de versión y Problemas.

Esta sección contiene los siguientes temas:

- [Visualización de los problemas de la aplicación](#)
- [Visualización de los problemas de versión](#)
- [Desplazamiento por la página Problemas](#)
- [Opciones de filtrado y agrupación en la página Problemas](#)
- [Personalización de filtros y agrupaciones de problemas](#)
- [Asignación de atributos para un problema](#)

1.6.1.1. Visualización de los problemas de la aplicación

Puede ver los problemas de todas las versiones de una aplicación (excluidas las versiones retiradas).

Para ver problemas a nivel de aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación que desea ver.

Aparecerá la página Información general de la aplicación.

3. Haga clic en **Problemas**.

Aparecerá la página Problemas de la aplicación. Dentro de una agrupación, los problemas se ordenan por nombre de archivo y, luego, por número de línea. Los problemas con el mismo Id. de instancia en las diversas versiones se agrupan en una sola vista. Puede deseleccionar problemas individuales cuando el grupo esté seleccionado.

Page 365 of 784

1.6.1.2. Visualización de los problemas de versión

Puede ver los problemas de una versión de una aplicación, incluidos los problemas de análisis de código abierto y en las instalaciones.

Para ver problemas a nivel de versión:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

3. Seleccione una versión de la lista.

4. Haga clic en **Problemas**.

Aparecerá la página Problemas de versión. Dentro de una agrupación, los problemas se ordenan por nombre de archivo y, luego, por número de línea. Puede deseleccionar problemas individuales cuando el grupo esté seleccionado.

opentext | Core Application Security 26.1
Aplicaciones
Panel
Informes
Administración

Demostraciones de API 24.4
CS3

Problemas de versión

782
1K
512
463
3K

4061291
Samples/SCA/dev/azure-quickstart-templates/demos/e-shop-website-with-il...

CS3
Crítico
Configuración incorrecta de Azure Resource Manager: HTTPS no necesario
Solución inteligente

Vulnerabilidad
Recomendaciones
Código
Diagrama
Más pruebas
Historial

Id. de instancia
Id. de regla principal

Agrupar por
CWE

(Sin configurar)
7

azuredeploy.json : 133

azuredeploy.json : 313

azuredeploy.json : 397

azuredeploy.json : 457

azuredeploy.json : 627

azuredeploy.json : 662

storage-account-v2.json : 23

CWE:259
19

1
→
→

app.js : 11

azuredeploy.json : 116

azuredeploy.json : 137

bosh.yml : 53

bosh.yml : 144

bosh.yml : 144

cross.yml : 64

install_openldap.sh : 70

install_openldap.sh : 73

install_openldap.sh : 76

CWE:287
492

CWE:297
4

CWE:311
49

CWE:319
90

Auditar

Estado
Nuevo

Fecha de introducción
2023/01/30

Fecha de la última vez que se encontró
2023/01/30

Periodo de gracia de corrección
1043 días de retraso

Usuario asignado
(Sin configurar)

Estado del desarrollador
Abierto

Estado del auditor
Pendiente de revisión

Gravedad
Crítico

Comentario

Agregar

Enviar error

Agregar filtro de auditoría

Asignar atributos

This PDF was generated on February 12, 2026

Page 367 of 784

1.6.1.3. Desplazamiento por la página Problemas

En las siguientes tablas, se describe cómo desplazarse por las páginas Problemas de la aplicación y Problemas de versión.

Navegación general

Tarea	Acción
Enviar desafíos de falso positivo	Haga clic en Enviar desafío . Se requiere el permiso Enviar desafío de falso positivo .
Exportar datos de problemas	Haga clic en ↓. Se envía un vínculo para descargar un archivo CSV a la dirección de correo electrónico especificada en la configuración de la cuenta. El vínculo es válido durante 7 días desde el momento en que se envía el correo electrónico y solo el usuario puede acceder a él.  Note Las funcionalidades de exportación en las páginas Panel de inquilino, Sus versiones, Problemas de la aplicación y Problemas de versión muestran los mismos campos para las columnas. Los filtros aplicados actualmente también se aplican a la exportación.
Buscar problemas	Escriba una palabra clave o una frase en el campo de texto de búsqueda y pulse Intro .
Mostrar u ocultar los problemas solucionados	Haga clic en Mostrar... Solucionados para mostrar u ocultar los problemas con el estado Solución validados.

Tarea	Acción
Mostrar u ocultar los problemas suprimidos	Haga clic en Mostrar... Suprimidos para mostrar u ocultar los problemas con el estado Falso positivo confirmado y Suprimido.
Mostrar u ocultar la lista de filtros	Haga clic en  .
Personalice las opciones de filtros y agrupaciones	Haga clic en  . Sus selecciones determinan las opciones que se muestran en la página Problemas. Para obtener más información, consulte Personalización de filtros y agrupaciones de problemas .
Expandir o contraer filtros	Haga clic en expandir todo o contraer todo en la flecha junto al nombre del filtro.
Aplicar un filtro	Seleccione los valores de filtro deseados debajo del nombre del filtro. La página se actualizará automáticamente con los resultados filtrados. Para algunos filtros, haga clic en aplicar para actualizar la página. Para obtener más información, consulte Opciones de filtrado y agrupación en la página Problemas .
Guardar los filtros aplicados como una consulta	Haga clic en Guardar consulta . Aparecerá la ventana Ponga nombre a su consulta personalizada. Escriba un nombre para la consulta y haga clic en Guardar . La consulta que se guardó aparece en el filtro Consultas preestablecidas .

Tarea	Acción
Quitar los filtros aplicados	Haga clic en X o en Borrar filtros .

Panel de navegación

Tarea	Acción
Expandir o contraer el panel de navegación	Haga clic en > o en < .
Ver problemas por nivel de gravedad	Seleccione una de las siguientes pestañas: Crítica , Alta , Media , Baja o Todo .
Agrupar los problemas mostrados según un atributo	Seleccione un valor de la lista Agrupar por . Dentro de un grupo, los problemas se ordenan por nombre de archivo y, luego, por número de línea. Para obtener más información, consulte Opciones de filtrado y agrupación en la página Problemas .
Ver más detalles de un problema	Haga clic en la descripción del problema.
Seleccionar varios problemas	Marque las casillas junto a los problemas.
Desplazarse por los problemas de un grupo	Haga clic en las flechas a la derecha y a la izquierda ←→ .

Panel de detalles del problema

Tarea	Acción
Ver una instancia específica de un problema encontrado en varias versiones	Seleccione el id. del problema (específico de una versión) de la lista desplegable. El panel de detalles del problema en la página Problemas de versión muestra por defecto el problema específico de esa versión. 1549640 JavaSource/org/owasp/webgoat/util/Exec.java : 103 Jenkins test Crítico Command Injection SMART FIX
Ver el diagrama de seguimiento de análisis de un problema junto con otros de la misma categoría	Haga clic en el vínculo Smart Fix. Aparecerá una vista en pantalla completa de Smart Fix que muestra todos los problemas de la categoría de problema seleccionada y en la que se resalta el flujo de datos del problema seleccionado.
Ver detalles concretos de un problema	Seleccione una pestaña. Para obtener más información, consulte Visualización de detalles del problema.

Panel de auditoría

Tarea	Acción
Expandir o contraer el panel de navegación	Haga clic en > o en <.
Editar un problema	Edite los campos disponibles. Para obtener más información, consulte Actualizar problemas .
Enviar un problema al seguimiento de errores:	Haga clic en Enviar error . Para obtener más información, consulte Envío de problemas al seguimiento de errores .
Agregar un filtro de auditoría para un problema	Haga clic en Agregar filtro de auditoría . Para obtener más información, consulte Creación de un filtro de plantilla de auditoría de aplicaciones para un problema .
Asignar atributos a un problema	Haga clic en Asignar atributos . Para obtener más información, consulte Asignar un atributo a un problema .

1.6.1.4. Opciones de filtrado y agrupación en la página Problemas

Las siguientes opciones de filtros y agrupación están disponibles en la página Problemas:



Note

Para que un filtro aparezca en la lista de filtros, el filtro debe estar habilitado (consulte [Personalización de filtros y agrupaciones de problemas](#)) y los resultados deben contener múltiples valores para ese filtro.

Filtrar y agrupar	Descripción	Valores
Estado de App Defender	Compatibilidad de la categoría de problema con Application Defender	Apto, No apto
Usuario asignado	Definido por el usuario	Sin configurar, Definido por el usuario
Marca de tiempo auditada	Fecha de la última actualización del Estado del auditor (solo filtro)	

Filtrar y agrupar	Descripción	Valores
Estado del auditor	Estado de corrección de problema de auditor.	- Valores del sistema no suprimidos: Pendiente de revisión, Corrección necesaria, Corrección pospuesta, Riesgo mitigado, Sospechoso, Propuesto como no es un problema  Note Sospechoso y Propuesto como no es un problema son establecidos por SAST Aviator. - Valores del sistema suprimidos: Riesgo aceptado, No es un problema, estado del auditor de Aviator suprimido - Definido por el usuario

Filtrar y agrupar	Descripción	Valores
Error enviado	Se envió un problema como un error a un sistema de seguimiento de errores	Falso, Verdadero
Categoría	Categoría del problema	
Solicitudes preestablecidas	Consultas predeterminadas (opción de solo filtro)	Mis problemas abiertos
Consultas personalizadas	Consultas personalizadas guardadas (opción de solo filtro)	Definido por el usuario
CWE	Clasificación Common Weakness Enumeration	
CWE Top 25 2023	Clasificación Common Weakness Enumeration Top 25	
CWE Top 25 2024	Clasificación Common Weakness Enumeration Top 25	

Filtrar y agrupar	Descripción	Valores
Estado del desarrollador	Estado de corrección de problema del desarrollador	- Valores del sistema: Desafiado, Abierto, En corrección, Corregido, No se solucionará o Componente de terceros - Definido por el usuario
DISA STIG 6.1	Desarrollo y seguridad de las aplicaciones DISA STIG 6.1	
DISA STIG 6.2	Desarrollo y seguridad de las aplicaciones DISA STIG 6.2	
DISA STIG 6.3	Desarrollo y seguridad de las aplicaciones DISA STIG 6.3	
Desafío de falso positivo		Sin configurar, Desafiado, Problema confirmado
FISMA	Clasificación de FISMA (obsoleta)	
SAST Aviator	Auditado por SAST Aviator	Falso, Verdadero
Con datos adjuntos		Falso, Verdadero
Con comentarios		Falso, Verdadero

Filtrar y agrupar	Descripción	Valores
Tiene notas		Falso, Verdadero
Fecha de introducción	Fecha original de creación del problema (solo filtro)	
Periodo de gracia de corrección	Los días restantes o vencidos. Este campo se aplica únicamente a problemas con categoría de estado del desarrollador 'Abierto'.	
Se ha suprimido	El problema se ha suprimido (solo filtro)	Falso, Verdadero
Antigüedad del problema	Número de días que los problemas han estado presentes en la aplicación (solo filtro). Las categorías son acumulativas. Por ejemplo, un problema que se considera más antiguo de 30 días también se tiene en cuenta para el recuento de los que tienen más de 10 días de antigüedad.	>/< 5 días, >/< 10 días, >/< 30 días, >/< 60 días, >/< 45 días o >/< 90 días
Microservicio		
NIST SP 800-53 Rev. 5	Publicación especial 800-53 del Instituto Nacional de Estándares y Tecnología	

Filtrar y agrupar	Descripción	Valores
OWASP 2014 Mobile	Clasificación según el Top 10 móvil de OWASP 2014	
OWASP 2017	Clasificación según el Top 10 de OWASP 2017	
OWASP 2021	Clasificación según el Top 10 de OWASP 2021	
OWASP API Top 10 2023	Clasificación OWASP API top 10 2023	
OWASP ASVS 4.0	Clasificación OWASP ASVS 4.0	
OWASP ASVS 5.0	Clasificación OWASP ASVS 5.0	
OWASP Mobile Top 10 2024	Clasificación según el Top 10 móvil de OWASP 2024	
Paquete	Paquete o espacio de nombre	
PCI 4.0	Clasificación de PCI 4.0	
PCI DSS 4.0.1	Clasificación de PCI 4.0.1	
PCI SSF1.2	Clasificación de PCI SSF 1.2	

Filtrar y agrupar	Descripción	Valores
Versión	Versión en la que se identificó el problema (solo filtro)  Note El filtro Versión solo aparece en la página Problemas de la aplicación.	
Herramienta de análisis	Herramienta de análisis utilizada para encontrar el problema	DAST, SAST, MAST, Debricked, Sonatype
Tipo de análisis	Tipo de análisis al que pertenece el problema	Dinámico, Estático, Móvil, Código abierto
Ámbito	Dependencia de producción o no producción (análisis de OpenText Core SCA)	
Gravedad	Gravedad del problema (solo filtro)	Crítico, Alto, Medio, Bajo, Mejor procedimiento, Información
Receptor	Función de receptor de flujo de datos, aplicable para problemas de análisis estático	

Filtrar y agrupar	Descripción	Valores
Código fuente	Función de origen de flujo de datos, aplicable para problemas de análisis estático	
Estado	Estado del problema	Nuevo, Existente, Reabierto o Solucionado/Solución validados
<Atributo personalizado>	Atributos personalizados	Definido por el usuario

1.6.1.5. Personalización de filtros y agrupaciones de problemas

Puede personalizar los filtros y las agrupaciones de problemas que se muestran en la página Problemas de la aplicación o Problemas de versión.

Para personalizar filtros y agrupaciones de problemas:

1. En el panel de auditoría, haga clic en .

Aparecerá la ventana Configuración.

Configuración

×

Filtros

Grupos

☒ Gravedad

☐ Versión

☐ Microservicio

☐ Estado de SDLC

☒ Categoría

☒ Estado

☒ Usuario asignado

☐ Paquete

☒ OWASP 2013

☒ Tipo de análisis

GUARDAR

CERRAR

2. Realice la tarea que corresponda:

Tarea	Procedimiento
Personalizar filtros de problemas	1. Seleccione la pestaña Filtros. 2. Marque las casillas de verificación situadas junto a los filtros que desee agregar. 3. Quite la marca de las casillas de verificación situadas junto a los filtros que desee quitar. 4. Haga clic en Guardar. La página de problemas se actualizará con los filtros nuevos en la lista de filtros.  Note Un filtro aparece en la lista de filtros solamente cuando los resultados contienen varios valores para ese filtro.

Tarea	Procedimiento
Personalice las agrupaciones de problemas (opciones Agrupar por en el panel de navegación)	1. Seleccione Grupos. 2. Marque las casillas de verificación situadas junto a los valores que desea agregar a la lista Agrupar por. 3. Anule la selección de las casillas de verificación situadas junto a los valores que desea eliminar de la lista Agrupar por. 4. Haga clic en Guardar. La página Problemas se actualizará con los nuevos valores de los grupos.

1.6.1.6. Asignación de atributos para un problema

Los atributos son solo informativos y no influyen en el proceso de evaluación. Los usuarios con los permisos necesarios pueden asignar atributos a un problema desde la página Problemas.

Para asignar atributos a un problema:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación cuyos atributos desee asignar.

Aparecerá la página Información general de la aplicación.

3. Desplácese hasta la página Problemas de la aplicación o Problemas de versión.

The screenshot shows the OpenText Core Application Security interface. The top navigation bar includes 'opentext | Core Application Security 26.1', 'Applications', 'Dashboard', 'Reports', and 'Administration'. The main content area is titled '24.4 API Demos' and 'Application Issues'. On the left, there's a sidebar with a search bar and a list of issues grouped by category. The main panel displays details for a selected issue: 'Samples/SCA/dev/azure-quickstart-templates/application-workloads/apache/...'. The issue is categorized as 'CS4 - Critical' and 'Azure ARM Misconfiguration: Improper Compute VM Access Control'. The 'Summary' section states: 'On line 206 of azuredeploy.json, the template defines a VM that allows SSH basic authentication. The template defines a VM that allows SSH basic authentication.' The 'Explanation' section states: 'Systems protected by basic authentication offer attackers a potential weak link. Attackers can compromise passwords (especially weak ones) by brute force, guessing, or social engineering.' Below the explanation is a JSON snippet for 'resources' showing a VM configuration. The right panel shows the 'Audit' section with fields for 'Status' (New), 'Introduced Date' (2023/01/30), 'Last Found Date' (2023/01/30), 'Assigned User' (Not Set), 'Developer Status' (Open), 'Auditor Status' (Pending Review), 'Severity' (Critical), and a 'Comment' field. There are buttons for 'Add', 'Submit Bug', 'Add Audit Filter', and 'Assign Attributes'.

4. En el panel de auditoría, haga clic en **Asignar atributos**.

Aparecerá la ventana Asignar atributos.

5. Realice la tarea que corresponda:

×

ASIGNAR ATRIBUTOS

Grupo

(Elija uno) ▾

Atr. del problema

issueattribute

Guardar

Cancelar

1. Seleccione **grupo**.
2. Introduzca los atributos del problema.
3. Haga clic en **Guardar**. Los atributos se guardan.

1.6.2. Detalles del problema

El panel de detalles de problema en la página Problemas de la aplicación o Problemas de versión proporciona detalles integrales del problema que permiten analizar las vulnerabilidades encontradas en la aplicación. Los detalles se organizan en varias pestañas. Las pestañas disponibles dependen del tipo de análisis en el cual se encontró el problema.

Esta sección aborda los siguientes temas:

- [Detalles de los problemas de un análisis estático](#)
- [Detalles de problemas del análisis de código abierto](#)
- [Detalles de los problemas de un análisis dinámico](#)
- [Detalles de los problemas de un análisis móvil](#)

1.6.2.1. Detalles de los problemas de un análisis estático

El panel de detalles de problema de un problema de análisis estático muestra el id. del problema, su ubicación, su gravedad y su categoría en la parte superior. Las siguientes pestañas proporcionan información adicional sobre el problema, incluidos los detalles técnicos, la línea de código (si se envió el código fuente) y un diagrama de seguimiento de análisis.

Vulnerabilidad

La pestaña **Vulnerabilidad** muestra los siguientes detalles técnicos sobre el problema: resumen del problema, explicación de la ejecución e implicaciones del problema, id. de instancia e id. de regla; e información sobre los estándares y las prácticas recomendadas de Fortify Software Security Research.

930712 <https://zero.webappsecurity.com:443/>



Crítico

Insecure Transport: Weak SSL Cipher

Vulnerabilidad

Recomendaciones

HTTP ▼

Más pruebas ▼

Historial

Resumen

WebInspect ha detectado compatibilidad con cifrados TLS/SSL débiles en el servidor .

Los protocolos Seguridad de la capa de transporte (TLS) y Capa de sockets seguros (SSL) proporcionan un mecanismo de protección que garantiza la autenticidad, confidencialidad e integridad de los datos transmitidos entre un cliente y un servidor web. La fortaleza de tal mecanismo de protección viene determinada por los algoritmos de autenticación, cifrado y hash (conocidos colectivamente como conjunto de cifrado) elegidos para la transmisión de información confidencial a través del canal TLS/SSL. La mayoría de los servidores web es compatible con diferentes conjuntos de cifrado de distintas fortalezas. Usar un cifrado débil o una clave de cifrado de longitud insuficiente, por ejemplo, podría permitir a un atacante inhabilitar el mecanismo de protección y robar o modificar información confidencial.

Mal configurado, un servidor web se podría manipular para que eligiese conjuntos de cifrado débiles. Se recomienda, entre otras medidas, actualizar la configuración del servidor web para que elija siempre los conjuntos de cifrado de mayor fortaleza.

Explicación

Un esquema de cifrado débil puede ser objeto de ataques por fuerza bruta con posibilidades de éxito razonables empleando los métodos y recursos actuales. Un atacante podría ser capaz de ejecutar un ataque de tipo "man-in-the-middle" para interceptar, supervisar y manipular datos confidenciales.

Id. de instancia: a95f108e-ae6e-37ff-d32c-abd2f01232d6

Id. de regla principal: 11285

Estándares y procedimientos recomendados

PCI 3.2

- 4.1 - Insecure Cardholder Data Transmission
- 6.5.4 - Insecure Communications

Recomendaciones

La pestaña Recomendaciones muestra recomendaciones para corregir el problema, además de consejos y referencias para investigarlo en profundidad. Si está disponible, la sección **Formación interactiva** contiene vínculos a una formación interactiva para la categoría del problema, vídeos sobre la categoría del problema y otros recursos educativos. La sección **Formación interactiva** está desarrollada por Secure Code Warrior. Para obtener más información sobre Secure Code Warrior, consulte [Integración con Secure Code Warrior](#).

930712 <https://zero.webappsecurity.com:443/>

Crítico

Insecure Transport: Weak SSL Cipher

Vulnerabilidad

Recomendaciones

Código

Diagrama

Más pruebas ▼

Historial

Recomendación

Deshabilite la compatibilidad con cifrados débiles en el servidor. En general, se definen como cifrados débiles:

- Todos los cifrados con clave de longitud inferior a 128 bits
- Los conjuntos de cifrado de clase de exportación
- Los cifrados NULL
- Los cifrados compatibles con modos no autenticados
- Los cifrados evaluados a niveles de seguridad inferiores a 112 bits
- Todos los cifrados RC4
- Todos los cifrados de bloques de 64 bits

Los siguientes cifrados admitidos por el servidor son débiles y deben deshabilitarse:

- En Apache, modifique las líneas siguientes en httpd.conf o ssl.conf:
 - SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!NULL:!RC4:!RC2:!DES:!3DES+HIGH:+MEDIUM
- En IIS, consulte los artículos de Microsoft Knowledge Base:
 - Id. de artículo: 187498
 - Id. de artículo: 245030 y
 - Security Guidance for IIS
 - Id. de artículo: 2868725
- En otros servidores, consulte la documentación específica del proveedor.

Los siguientes cifrados admitidos por el servidor deben proporcionar la protección adecuada y pueden mantenerse habilitados:

Consejos

Todos los cifrados débiles se han obtenido estableciendo una conexión SSL con el host de destino y especificando el cifrado que se deseaba probar en el mensaje Client Hello de la etapa de sincronización SSL.

Código

La pestaña Código muestra el código específico donde se encontró el problema. Los usuarios pueden realizar las siguientes acciones para revisar código con más facilidad:

- Habilitar o deshabilitar el ajuste de línea
- Navegar por varios seguimientos de análisis (si corresponde)

- Cambiar entre una vista apilada del código y una vista de árbol del seguimiento de análisis junto al código
- Saltar a la línea de código al seleccionar un nodo de seguimiento de análisis en la vista de árbol
- Habilitar y deshabilitar la visualización del seguimiento de análisis alineado



Note

Para ver todos los problemas de la categoría de problema seleccionada, haga clic en el vínculo **Smart Fix**.

1073136 ▾

pebble-web/themes/default/jsp/blogEntry.jsp : 68

1

Crítico

Cross-Site Scripting: Reflected

SMART FIX

Vulnerabilidad

Recomendaciones

Código

Diagrama

Más pruebas ▾

Historial

< Ruta 1 de 5 >

☐ Ajuste de línea

☒ Vista apilada

☒ Seguimiento de análisis en línea

⚡() SaveBlogEntryAction.java:320 - getParameter(return)

307

// we're creating a new blog entry

308

return blog.getBlogForToday().createBlogEntry();

309

}

310

}

311

312

private void populateBlogEntry(BlogEntry blogEntry, HttpServletRequest request) {

313

SimpleBlog blog = (SimpleBlog)request.getAttribute(Constants.BLOG_KEY);

314

String title = request.getParameter("title");

315

String subtitle = request.getParameter("subtitle");

316

String body = StringUtils.filterNewlines(request.getParameter("body"));

317

String excerpt = StringUtils.filterNewlines(request.getParameter("excerpt"));

318

String originalPermalink = request.getParameter("originalPermalink");

319

String tags = request.getParameter("tags");

320

String staticName = request.getParameter("staticName");

321

String commentsEnabled = request.getParameter("commentsEnabled");

322

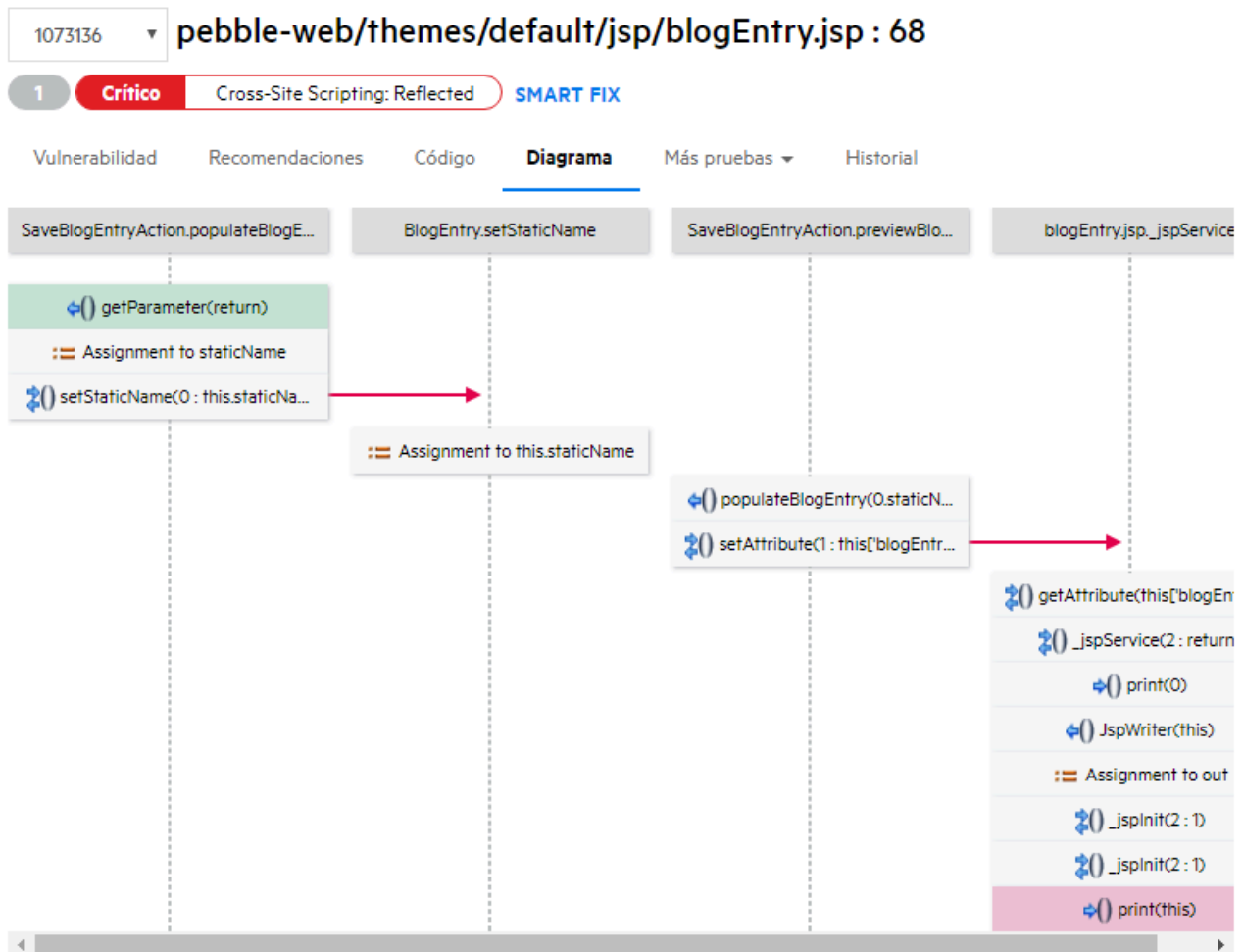
String trackBacksEnabled = request.getParameter("trackBacksEnabled");

⚡() SaveBlogEntryAction.java:320 - getParameter(return)

⚡ SaveBlogEntryAction.java:320 - Assignment to staticName

Diagrama

La pestaña Diagrama muestra un diagrama de seguimiento de análisis sobre el problema.



Más pruebas

La pestaña **Más pruebas** contiene notas y capturas de pantallas, a las que se accede por separado a través del menú desplegable.

- La sección **Notas** muestra anotaciones sobre el problema del equipo de evaluación.
- La sección **Capturas de pantalla** le permite cargar capturas de pantalla que ofrezcan información contextual sobre el problema. Para obtener más información, consulte [Carga de capturas de pantalla](#).

1073136 ▾ pebble-web/themes/default/jsp/blogEntry.jsp : 68

1 **Crítico** Cross-Site Scripting: Reflected **SMART FIX**

Vulnerabilidad Recomendaciones Código Diagrama **Más pruebas ▾** Historial

+ AGREGAR CAPTURA DE PANTALLA

No hay elementos para mostrar.

Historial

La pestaña **Historial** muestra un registro de los siguientes eventos del problema: cambios de auditoría, comentarios y eventos del sistema (cambios de estado, acciones de estado de copia y resultados de desafío de falso positivo). Puede filtrar el registro por tipo de evento (auditoría, seguimiento de errores, comentario o evento del sistema).

3889610 EternalStorage/EternalStorage.sol : 4

Solidity

Crítico

Configuración incorrecta de Solidity: Compilador con vulnerabilidades conocidas



[Solución inteligente](#)

Vulnerabilidad

Recomendaciones

Código

Diagrama

Más pruebas ▾

Historial



Auditorías



Comentarios



Eventos del sistema

OpenText™ Core Application Security 2024/04/02 11:32:52 AM

Se ha encontrado un problema en el análisis 58934 de la versión Solidity.

Agregar comentario

Agregar

1.6.2.2. Detalles de problemas del análisis de código abierto

El panel de detalles de problemas de un problema de análisis código abierto muestra el id. del problema, su ubicación, su gravedad y su id. de regla en la parte superior. Las siguientes pestañas ofrecen información adicional sobre el problema.



Note

Si el análisis de Sonatype más reciente detecta que un problema de código abierto es una vulnerabilidad no activa, el panel de detalles de problemas muestra el mensaje "Esta vulnerabilidad ya no se indica como una vulnerabilidad activa". El estado del problema también se marca como **Solución validada**. Esto no se aplica a los problemas asociados con componentes de código abierto que se hayan eliminado.

Vulnerabilidad

La pestaña **Vulnerabilidad** muestra los siguientes detalles técnicos sobre el problema: datos sobre la vulnerabilidad de la herramienta de análisis utilizada, el id. de instancia y el id. de regla, las ubicaciones de archivos, e información sobre los estándares y procedimientos recomendados de Fortify Software Security Research.

Para obtener más información sobre los datos de vulnerabilidad de las herramientas de análisis, consulte los siguientes enlaces:

- Sonatype: <https://guides.sonatype.com/iqserver/technical-guides/sonatype-vuln-data/>
- OpenText Core SCA: <https://debricked.com/docs/security/security-about#data-refinement>

1723241 org.apache.commons:commons-compress@1.9 :

R1

Crítico

CVE-2021-35516



Vulnerabilidad

Recomendaciones

Dependencias

Más pruebas

Historial

Resumen

When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.

Nombre del componente: org.apache.commons:commons-compress

Versión del componente: 1.9

Repositorio: maven

Id. de instancia: 593F2439BDC83487B1F45A42BAD6BF6B

Id. de regla principal: CVE-2021-35516

Fecha de publicación: 2021/07/13

Fecha de actualización: 2021/07/13

Fecha de creación: 2021/07/13

Puntuación total de CVSS: 7,5

Vector de CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Estándares y procedimientos recomendados

OWASP 2021

- A06:2021 – Vulnerable and Outdated Components

PCI 4.0

- 6.3.3 – All system components are protected from known vulnerabilities by installing applicable security patches/updates

CWE

- CWE-770

Recomendaciones

La pestaña Recomendaciones muestra información y referencias de correcciones para investigar en profundidad. Haga clic en **Ver todos los problemas** para ver todos los problemas filtrados por la URL del paquete en la versión.

Además, las métricas de salud de Open Source Select se muestran gráficamente para los problemas de OpenText Core SCA. Open Source Select es una base de datos de todos los proyectos de código abierto en GitHub.

3862670 certifi@2022.5.18.1 :

v1

Crítico

CVE-2023-37920



Vulnerabilidad

Recomendaciones

Dependencias

Más pruebas ▾ Historial

Recomendación

Component:pkg:pypi/certifi@2022.5.18.1

Versión segura:2023.7.22.

VER TODOS LOS PROBLEMAS

Salud comunitaria de código abierto

El estado de la comunidad es una consideración importante a la hora de evaluar el riesgo actual y futuro de utilizar proyectos de código abierto en su aplicación. Open Source Select sirve de ayuda a los desarrolladores para empezar por la izquierda y elegir un código abierto más inteligente. Los equipos de aplicaciones deben revisar de manera continua el estado de sus dependencias de código abierto y considerar alternativas a proyectos con bajas puntuaciones de Contribuidores, Popularidad y/o Seguridad.

Haga clic aquí para obtener más detalles.

52

Colaboradores

Ligeramente mantenido

72

Popularidad

Muy popular

67

Líder en

Prácticas de seguridad decentes

Referencias

- <https://github.com/pypa/advisory-db/blob/main/vulns/certifi/PYSEC-2023-135.yaml>

Dependencias (OpenText Core SCA, CycloneDX)

La pestaña **dependencias** muestra un árbol de dependencia visualizado para el componente vulnerable. Aparece un árbol de dependencias para cada nodo raíz (dependencia directa) que contiene el componente vulnerable.



Note

Los árboles de dependencia no están disponibles para SBOM sin detalles de dependencia y el archivo `debricked.fingerprints.txt`.

OpenTextEl Portal de MSP recomienda revisar el árbol de dependencias y usar la solución de reparación raíz para resolver el problema. Una corrección raíz contiene la siguiente versión de la dependencia directa que no contiene una versión vulnerable de la dependencia afectada. En términos más simples, la corrección raíz es una solución a una vulnerabilidad de dependencia que comienza en la raíz del árbol de

dependencia. Para obtener más información sobre el uso de la corrección raíz, consulte [¿Cómo soluciono manualmente una vulnerabilidad con la solución Corrección raíz?](#)

- Para un problema encontrado en diferentes archivos de bloqueo, al seleccionar un archivo de bloqueo de la lista desplegable se muestra la ruta completa del archivo de bloqueo seleccionado.
- Un árbol de dependencia se puede expandir y contraer.
- Los nodos vulnerables están marcados en rojo.
- La cantidad de árboles de dependencia que se muestran es la cantidad de nodos raíz que tienen una versión segura conocida o son arreglos solo para archivos de bloqueo. Una corrección solo de archivo de bloqueo significa que puede regenerar el archivo de bloqueo en su repositorio y la vulnerabilidad se resolverá. No necesita actualizar la dependencia directa; en su lugar, reinstale la misma versión (por ejemplo: ejecute la actualización de hilo y genere un nuevo archivo `yarn.lock`).

1825937

com.h2database:h2@1.4.197 :

test1015

Alto

CVE-2018-10054

Vulnerabilidad

Recomendaciones

Dependencias

Más pruebas

Historial

Introducido a través de

.debricked-maven-dependencies.tgf

1 archivo

1 dependencia directa para actualizar

com.h2database/h2

✖ 1.4.197

>

✔ 1.4.198

Más pruebas

La pestaña **Más pruebas** muestra notas y capturas de pantallas, a las que se accede por separado a través del menú desplegable.

- La sección **Notas** muestra anotaciones sobre el problema del equipo de evaluación.
- La sección **Capturas de pantalla** le permite cargar capturas de pantalla que ofrezcan información contextual sobre el problema. Para obtener más información, consulte [Carga de capturas de pantalla](#).

1723241 org.apache.commons:commons-compress@1.9 :

R1

Crítico

CVE-2021-35516



Vulnerabilidad

Recomendaciones

Dependencias

Más pruebas ▾

Historial

No hay notas adicionales para esta instancia de vulnerabilidad.

Notas

Capturas de pantalla

Historial

La pestaña **Historial** muestra un registro de los siguientes eventos relacionados con el problema: cambios de auditoría, comentarios y eventos del sistema (cambios de estado, acciones de estado de copia y resultados de desafío de falso positivo). Puede filtrar el registro por tipo de evento (auditoría, seguimiento de errores, comentario o evento del sistema).

4004379 com.fasterxml.jackson.core:jackson-databind@2.9.6 :

Julio de 2024

Crítico

CVE-2019-20330



Vulnerabilidad

Recomendaciones

Dependencias

Más pruebas ▾

Historial



Auditorías



Comentarios



Eventos del sistema

OpenText™ Core Application Security 2024/07/11 11:51:48 AM

Problema encontrado por Debricked en el análisis 60173 de la versión de julio de 2024.

Agregar comentario

Agregar

1.6.2.3. Detalles de los problemas de un análisis dinámico

El panel de detalles de problema de un problema de análisis dinámico muestra el id. del problema, su ubicación, su gravedad y su categoría en la parte superior. Las siguientes pestañas ofrecen información adicional sobre la vulnerabilidad, incluidos los detalles técnicos, la solicitud y la respuesta.

Vulnerabilidad

La pestaña **Vulnerabilidad** muestra los siguientes detalles técnicos sobre el problema: el resumen del problema, que incluye el id. de instancia y el id. de regla del problema, la explicación de la ejecución y las implicaciones del problema, e información sobre los estándares y las prácticas recomendadas del equipo de Fortify Software Security Research.

102979 <http://zero.webappsecurity.com/>

.01

Crítico

Web Server Misconfiguration: Unprotected File



SMART FIX

Vulnerabilidad

Recomendaciones

HTTP ▾

Más pruebas ▾

Historial

Resumen

Se ha encontrado el archivo service.pwd en el directorio _vti_pvt de la raíz de documentos del servidor HTTP. Este archivo contiene las contraseñas cifradas de las Extensiones de servidor de Microsoft FrontPage. El archivo puede recuperarlo remotamente un atacante, que podría obtener las contraseñas de texto simple y utilizarlas para acceder a los recursos del servidor. Se recomienda, entre otras medidas, asegurarse de que las contraseñas de las cuentas de FrontPage sean lo suficientemente seguras como para evitar que un atacante pueda averiguarlas. Además, modifique los permisos para el directorio _vti_pvt y los archivos *.pwd del directorio para denegar el acceso a los atacantes remotos.

Explicación

Si las contraseñas del archivo service.pwd son débiles o si el atacante pasa tiempo suficiente tratando de averiguarlas, este podría obtener las contraseñas sin cifrar y usarlas para acceder a los recursos del servidor.

Versiones vulnerables:

Microsoft FrontPage, cualquier versión

Id. de instancia: 7d6ac147-7d4a-4d61-8883-941b2cd72663

Id. de regla principal: 22

Estándares y procedimientos recomendados

PCI 3.2

- 6.5.8 - Improper Access Control

FISMA

- SI
- AC

CWE

Recomendaciones

La pestaña Recomendaciones muestra recomendaciones para corregir el problema, además de consejos y referencias para investigarlo en profundidad. Si se encuentra disponible, la sección **Formación interactiva** contiene un vínculo para iniciar la formación interactiva para la categoría de problema que proporciona Secure Code Warrior. Para obtener más información sobre Secure Code Warrior, consulte [Integración con Secure Code Warrior](#).

102979 <http://zero.webappsecurity.com/>

.01

Crítico

Web Server Misconfiguration: Unprotected File



SMART FIX

Vulnerabilidad

Recomendaciones

HTTP ▾

Más pruebas ▾

Historial

Recomendación

Para el equipo de Operaciones de seguridad:

Asegúrese de que las contraseñas de las cuentas de FrontPage sean lo suficientemente seguras como para evitar que un atacante pueda averiguarlas. Asegúrese también de que los nombres de usuario y contraseñas almacenados en los archivos de contraseñas de FrontPage no coincidan con aquellos que permiten iniciar sesión en el host.

Siga estas instrucciones para las contraseñas:

- Cree contraseñas de ocho caracteres, como mínimo.
- Permita que los usuarios creen contraseñas que acepten los 94 caracteres ASCII que se muestran, incluidas las letras mayúsculas y minúsculas.
- Anime a los usuarios a buscar otras palabras que no formen parte del diccionario, como combinaciones de letras mayúsculas y minúsculas, números, signos de puntuación, y símbolos.

Modifique los permisos para el directorio `_vti_pvt` y los archivos `*.pwd` del directorio para denegar el acceso a los atacantes.

Nota: La modificación de permisos puede afectar negativamente al funcionamiento normal del servidor de FrontPage.

Para los desarrolladores:

Al crear la aplicación web, asegúrese de que no se han publicado archivos `*.pwd` a través del servidor de producción.

Para el equipo de Control de calidad:

Durante el proceso de pruebas, esta evaluación enumera todos los archivos y todas las carpetas de la aplicación web y comenta su significado. Asegúrese de que los desarrolladores no publiquen archivos valiosos a los que un posible atacante podría tener

HTTP

En la pestaña **HTTP** se muestran el contenido, los encabezados y los parámetros de la solicitud y la respuesta, a los que se accede por separado a través del menú desplegable.

En la sección **Pruebas** se encuentra una lista del tráfico completo de la sesión que encontró el problema.

484981

http://zero.webappsecurity.com:80/zero/bank/account-sum...

show23

Crítico

Privacy Violation: Credit Card Number

Vulnerabilidad

Recomendaciones

HTTP

Más pruebas

Historial

Solicitud

AJUSTE DE LÍNEA

```

1 GET /zero/bank/account-summary.html HTTP/1.1
2 Host: zero.webappsecurity.com
3 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.2.29pre) Gecko/20110614 Firefox/3.6.3
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-us,en;q=0.5
6 Accept-Encoding: gzip,deflate
7 Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
8 Keep-Alive: 115
9 Referer: http://zero.webappsecurity.com/zero/login.html
10 Pragma: no-cache
11 Cookie: JSESSIONID=BAC758EC
12 X-WIPP: AscVersion=1.0.0.483.0
13 X-Scan-Memo: Category="Crawl.EventMacro.Startup"; SID="F5151B0DF075DAB63D14E1F00153A156"; Sessid
14 X-RequestManager-Memo: Category="EventMacro.Login"; MacroName="LoginMacro";
15 X-Request-Memo: ID="0242b0bf-10ca-45f3-8b09-1e764865028a"; ThreadId="63";
16
17

```

Respuesta

AJUSTE DE LÍNEA

```

1 HTTP/1.1 200 OK
2 Date: Mon, 25 Mar 2013 22:49:53 GMT
3 Server: Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/0.9.8t mod_lk/1.2.37

```

Más pruebas

La pestaña **Más pruebas** muestra notas y capturas de pantallas, a las que se accede por separado a través del menú desplegable.

- La sección **Notas** muestra anotaciones sobre el problema del equipo de evaluación.
- La sección **Capturas de pantalla** le permite cargar capturas de pantalla que ofrezcan información contextual sobre el problema. Para obtener más información, consulte [Carga de capturas de pantalla](#).

67813 thebuggenie/js/thebuggenie.js : 550

Static 1.0

Crítico

Open Redirect



SMART FIX

Vulnerabilidad

Recomendaciones

HTTP ▾

Más pruebas ▾

Historial

No hay notas adicionales para esta instancia de vulnerabilidad

Notas

Capturas de pantalla

Historial

La pestaña **Historial** muestra un registro de los siguientes eventos del problema: cambios de auditoría, comentarios y eventos del sistema (cambios de estado, acciones de estado de copia y resultados de desafío de falso positivo). Puede filtrar el registro por tipo de evento (auditoría, seguimiento de errores, comentario o evento del sistema).

4307907 ▾

<http://zero.webappsecurity.com:80/bank/pay-bills-new-payee.html>



R1

Crítico

Secuencias de comandos entre sitios: reflejado



Vulnerabilidad

Recomendaciones

HTTP ▾

Más pruebas ▾

Historial



Auditorías



Comentarios



Eventos del sistema

OpenText™ Core Application Security 2025/04/07 11:40:48 AM

Se ha encontrado un problema en el análisis 63191 de la versión R1.

Agregar comentario

Agregar

1.6.2.4. Detalles de los problemas de un análisis móvil

El panel de detalles de problema de un problema de análisis móvil muestra el id. del problema, su ubicación, su gravedad y su categoría en la parte superior. Las siguientes pestañas ofrecen información adicional sobre el problema.

Vulnerabilidad

La pestaña **Vulnerabilidad** muestra los siguientes detalles técnicos sobre el problema: el resumen del problema, el id. de instancia y el id. de regla, y la explicación de la ejecución y las implicaciones del problema.

1825947

org.apache.commons:commons-compress@1.9 :

test1015

Crítico

CVE-2021-35516

Vulnerabilidad

Recomendaciones

Dependencias

Más pruebas

Historial

Resumen

When reading a specially crafted 7Z archive, Compress can be made to allocate large amounts of memory that finally leads to an out of memory error even for very small inputs. This could be used to mount a denial of service attack against services that use Compress' sevenz package.

Nombre del componente: org.apache.commons:commons-compress

Versión del componente: 1.9

Repositorio: maven

Id. de instancia: 593F2439BDC83487B1F45A42BAD6BF6B

Id. de regla principal: CVE-2021-35516

Fecha de publicación: 2021/07/13

Fecha de actualización: 2021/07/13

Fecha de creación: 2021/07/13

Puntuación total de CVSS: 7.5

Vector de CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Estándares y procedimientos recomendados

OWASP 2021

- A06:2021 – Vulnerable and Outdated Components

PCI 4.0

- 6.3.3 – All system components are protected from known vulnerabilities by installing applicable security patches/updates

CWE

- CWE-770

Recomendaciones

La pestaña Recomendaciones muestra recomendaciones para corregir el problema, además de consejos y referencias para investigarlo en profundidad. Si se encuentra disponible, la sección **Formación interactiva** contiene un vínculo para iniciar la formación interactiva para la categoría de problema que proporciona Secure Code Warrior. Para obtener más información sobre Secure Code Warrior, consulte [Integración con Secure Code Warrior](#).

235774 @_kCFStreamSSLAllowsAnyRoot

Medio

Often Misused: Weak SSL Certificate

Vulnerabilidad

Recomendaciones

Más pruebas ▾

Historial

Recomendación

Utilice los métodos seguros que se encuentran en NSURL. En una situación en la que deba usarse CFNetwork, utilice certificados sólidos y seguros. En la mayoría de los casos se recomienda incluir un certificado con el paquete de su aplicación y usar el anclaje de certificados.

Consejos

Para explotar esta vulnerabilidad, un atacante tendría que realizar un ataque de tipo MITM (Man in the middle) contra la conexión de la aplicación al servidor de back-end. Para ello tal vez el atacante tenga que estar en la misma red que el destino.

Referencias

Tareas de servicio de confianza, certificados y claves para iOS: https://developer.apple.com/library/ios/DOCUMENTATION/Security/Conceptual/CertKeyTrustProgGuide/iPhone_Tasks/iPhone_Tasks.html

Más pruebas

La pestaña **Más pruebas** contiene notas y capturas de pantallas, a las que se accede por separado a través del menú desplegable.

- La sección **Notas** muestra anotaciones sobre el problema del equipo de evaluación.
- La sección **Capturas de pantalla** le permite cargar capturas de pantalla que ofrezcan información contextual sobre el problema. Para obtener más información, consulte [Carga de capturas de pantalla](#).

235774 @_kCFStreamSSLAllowsAnyRoot

Medio

Often Misused: Weak SSL Certificate

Vulnerabilidad

Recomendaciones

Más pruebas ▾

Historial

No hay notas adicionales para esta instancia

Notas

Capturas de pantalla

Historial

La pestaña **Historial** muestra un registro de los siguientes eventos del problema: cambios de auditoría, comentarios y eventos del sistema (cambios de estado,

acciones de estado de copia y resultados de desafío de falso positivo). Puede filtrar el registro por tipo de evento (auditoría, seguimiento de errores, comentario o evento del sistema).

235774 @_kCFStreamSSLAllowsAnyRoot

Medio

Often Misused: Weak SSL Certificate



Vulnerabilidad

Recomendaciones

Más pruebas ▼

Historial

No hay elementos para mostrar.

Mostrar



Auditorías



Comentarios



Eventos del sistema

[Ver historial](#)

Agregar comentario

AGREGAR

1.6.3. Actualizar problemas

Mediante la información proporcionada en los resultados del análisis, corrija las vulnerabilidades detectadas. Puede actualizar los problemas tanto en el nivel de aplicación como en el nivel de versión para el seguimiento de los esfuerzos de corrección.

Esta sección contiene los siguientes temas:

- [Edición de un problema](#)
- [Edición de varios problemas](#)
- [Carga de capturas de pantalla](#)

1.6.3.1. Edición de un problema

Puede editar problemas en las páginas Problemas de la aplicación y Problemas de versión. Los usuarios con el permiso Editar problemas pueden editar el estado del desarrollador de un problema y el usuario al que se le ha asignado. Los usuarios con permisos de auditoría también pueden editar el estado del auditor y la gravedad del problema.

Para editar un problema:



Note

En las siguientes instrucciones, se describe cómo editar un problema en la página Problemas de la aplicación. La selección y actualización de problemas funciona de la misma manera en la página Problemas de versión.

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación con problemas que desee editar.

Aparecerá la página Información general de la aplicación.

3. Haga clic en **Problemas**.

The screenshot displays the 'Problemas de la aplicación' (Application Problems) page. On the left, a sidebar lists various security categories with counts: Cross-Site Sc... (280), Dangerous FL... (14), Insecure Tran... (2), Open Redirect (2), Password Ma... (2), and Path Manipul... (50). The main panel shows a search bar with '1073124' and a dropdown for 'pebble-web/jsp/blogEntry.jsp : 53'. Below this, a 'Vulnerabilidad' (Vulnerability) section highlights a 'Crítico' (Critical) issue: 'Cross-Site Scripting: Reflected'. A 'SMART FIX' button is visible. The 'Resumen' (Summary) states that the method `_jspService()` in `blogEntry.jsp` sends unvalidated data to a web browser on line 53. The 'Explicación' (Explanation) details how XSS vulnerabilities occur when data from an untrusted source is reflected in the browser. It notes that in this case, data enters through `getParameter()` in `SaveBlogEntryAction.java` on line 319 and is included in dynamic content sent to the user without validation. The final paragraph explains that malicious content can take the form of JavaScript, HTML, or Flash, which the browser executes, potentially leading to data theft or redirection. On the right, an 'Auditar' (Audit) panel allows filtering by state (Nuevo), introduction date (2017/10/20), last found date (2017/10/20), assigned user (Sin configurar), developer state (Abierto), auditor state (Pendiente de rev), severity (Crítico), and a comment field. Buttons for 'AGREGAR' (Add), 'ENVIAR ERROR' (Send Error), and 'AGREGAR FILTRO ...' (Add Filter) are at the bottom right.

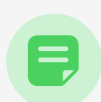
Aparecerá la página Problemas de la aplicación.

4. Seleccione el problema que desea editar en el panel de navegación. Si el problema se encuentra en varias versiones, seleccione una instancia específica seleccionando el id. del problema, que es específico de la versión, de la lista desplegable en el panel de detalles del problema.
5. En el panel de auditoría, edite los campos según sea necesario.

Campo	Descripción
Usuario asignado	Seleccione el usuario al que se le asignará el problema
Estado del desarrollador	Seleccione el estado de desarrollo del problema. El valor predeterminado es Abierto. Las categorías correspondientes de estados son abierto o cerrado. ◦ Si está revisando el problema, seleccione En corrección. ◦ Si cree que el problema no es válido, seleccione Desafío de falso positivo. Consulte Envío de un desafío de falso positivo para obtener más información sobre el proceso de desafío de falso positivo. ◦ Si corrigió el problema, seleccione Corregido. ◦ Si decidió no corregir el problema, seleccione No se solucionará. ◦ Si el problema está en el código de terceros, seleccione Componente de terceros.

Campo	Descripción
Estado del auditor	Seleccione el estado de la auditoría del problema. El estado predeterminado es Pendiente de revisión. Las categorías correspondientes de estados son no suprimido o suprimido. - No suprimido: Corrección necesaria, Corrección pospuesta, Riesgo mitigado - Suprimido: Riesgo aceptado, No es un problema
Gravedad	Seleccione una gravedad diferente para cambiar la gravedad del problema predeterminada.
Comentario	Escriba comentarios explicativos en el campo Comentario y haga clic en Agregar.

6. Actualice la página Problemas para ver los cambios en los problemas.



Note

Si un problema se ha eliminado, se ocultará en la página Problemas y solo aparecerá cuando se seleccione **Mostrar... Suprimidos**.

Temas relacionados

[Envío de problemas al seguimiento de errores](#)

1.6.3.2. Edición de varios problemas

Puede editar varios problemas en las páginas Problemas de la aplicación y Problemas de versión.

Para editar varios problemas:



Note

Las siguientes instrucciones describen cómo editar varios problemas en la página Problemas de la aplicación. La selección y actualización de problemas funciona de la misma manera en la página Problemas de versión.

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación con problemas que desee editar.

Aparecerá la página Información general de la aplicación.

3. Haga clic en **Problemas**.

Aparecerá la página Problemas de la aplicación.

4. Puede realizar las siguientes acciones para seleccionar varios problemas:

- En el panel de navegación, marque las casillas junto a los problemas.



Note

En la página Problemas de versión, puede seleccionar la casilla de verificación **Incluir problemas de otras versiones** para seleccionar todas las instancias del problema que se encuentran en las versiones. Los problemas se pueden eliminar individualmente.

Auditoría de múltiples problemas

☐ Incluir problemas de otras versiones

The screenshot shows the 'Problemas de la aplicación' interface. On the left, there's a sidebar with a list of problems grouped by version. The main area is titled 'Auditoría de varios problemas' and displays a table of 'Problemas seleccionados'. The table has columns for ID, version, location, audit status, and attachments. On the right, there are filters for user assigned, developer status, auditor status, severity, and a comment field. At the bottom right, there are buttons for 'ENVIAR CAMBIOS', 'RESTABLECER VALORES', and 'ENVIAR ERROR'.

ID DEL PROBLEMA	VERSIÓN	UBICACIÓN PRINCIPAL	AUDITADO	DATOS ADJUNTOS
349074	3.2	calendar.php: 39	VIEW AUDIT DETAILS	false
236460	3.1	calendar.php: 39	VIEW AUDIT DETAILS	false

- En el panel de navegación, puede marcar la casilla junto a un nombre de grupo para seleccionar todos los problemas del grupo.



Note

En la página Problemas de versión, puede seleccionar la casilla de verificación **Incluir problemas de otras versiones** para seleccionar problemas encontrados en la misma versión como un grupo separado. Los grupos de versiones se pueden eliminar individualmente.

Auditoría de múltiples problemas

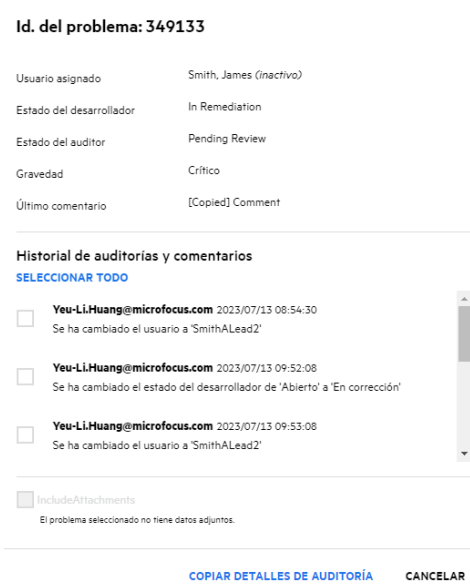
☐ Incluir problemas de otras versiones

The screenshot shows the 'Problemas de la aplicación' interface for 'Jeopardy (PHP)'. The main area is titled 'Auditoría de varios problemas' and displays a table of 'Grupos seleccionados'. The table has columns for count, version, and group name. On the right, there are filters for user assigned, developer status, auditor status, severity, and a comment field. At the bottom right, there are buttons for 'ENVIAR CAMBIOS', 'BORRAR SELECCIONES', and 'ENVIAR ERROR'.

RECuento DE ELEMENTOS	VERSIÓN	NOMBRE DEL GRUPO
19	3.1	Cross-Site Scripting: Reflected
19	3.2	Cross-Site Scripting: Reflected
61	3.1	Dangerous File Inclusion
61	3.2	Dangerous File Inclusion

5. Realice las siguientes tareas para editar campos de auditoría:

Tarea	Descripción
Editar campos de auditoría manualmente	En el panel de auditoría, edite los campos según sea necesario. Estos son los campos disponibles para su edición: Usuario asignado, Estado del desarrollador, Estado del auditor, Gravedad y Comentarios.

Tarea	Descripción
Copiar detalles de auditoría de un problema a otros problemas	- En el panel de problemas, haga clic en Ver detalles de auditoría en la fila del problema que desea copiar. Aparece la ventana Id. del problema.  - Seleccione las entradas de auditoría y comentario que desea copiar. - Seleccione la casilla de verificación Incluir datos adjuntos para copiar todos los datos adjuntos. - Hacer clic en Copiar detalles de auditoría. Se le redirigirá a la página Problemas Los valores de auditoría, junto con las entradas de auditoría seleccionadas, los comentarios y los datos adjuntos, se aplican

Tarea	Descripción
	a los demás problemas seleccionados.  Important Los problemas seleccionados deben tener identificadores de instancia coincidentes; de lo contrario, no podrá continuar con la copia de los detalles de la auditoría.

6. Haga clic en **Enviar cambios**.

La página Problemas se actualiza con los cambios de los problemas.

Temas relacionados

[Envío de problemas al seguimiento de errores](#)

1.6.3.3. Carga de capturas de pantalla

Puede cargar las capturas de pantalla de un problema a través de la página Problemas de la aplicación o Problemas de versión.

- Los tipos de archivos admitidos son .jpg, .gif y .png.
- Los archivos no deben superar los 3 MB.

Existen dos métodos para cargar una captura de pantalla: cargar un archivo guardado o copiar y pegar la imagen en la ventana modal.

Para cargar una captura de pantalla de un problema haga lo siguiente:

1. En el panel de detalles de problema, seleccione la pestaña **Más pruebas > Capturas de pantalla.**

The screenshot displays the OpenText Core Application Security interface. On the left, a sidebar contains navigation icons. The main area is titled '17.4 Static Application' and 'Problemas de la aplicación'. It shows a list of vulnerabilities, with 'Cross-Site Scripting: Reflected' selected. The details for this vulnerability are shown, including a 'Resumen' (Summary) and 'Explicación' (Explanation). The 'Más pruebas' (More tests) tab is active, and a 'Capturas de pantalla' (Screenshots) button is visible. On the right, a sidebar contains metadata for the vulnerability, including 'Estado' (Status), 'Fecha de introducción' (Introduction date), 'Fecha de la última vez que se encontró' (Last found date), 'Usuario asignado' (Assigned user), 'Estado del desarrollador' (Developer status), 'Estado del auditor' (Auditor status), and 'Gravedad' (Severity).

2. Haga clic en +Agregar captura de pantalla.

Aparecerá la ventana modal Captura de pantalla.

Captura de pantalla



Cargar captura de pantalla

Copiar y pegar captura de pantalla

Descripción

Captura de pantalla

CARGAR

3. Elija una de las siguientes maneras de cargar la captura de pantalla:

- Para cargar un archivo:
 1. Seleccione la pestaña **Cargar captura de pantalla**.
 2. (Opcional) Escriba una descripción del archivo.
 3. Haga clic en ..., busque la captura de pantalla y selecciónela.
 4. Haga clic en **Cargar**.
- Para copiar y pegar la captura de pantalla:
 1. Seleccione la pestaña **Copiar y pegar captura de pantalla**.
 2. (Opcional) Escriba una descripción del archivo.
 3. Copie una imagen en el portapapeles.
 4. Seleccione el cuadro y pulse **Ctrl+V** para pegar la imagen desde el portapapeles.
 5. Haga clic en **Cargar**.

En la pestaña aparecen los detalles de la captura de pantalla cargada y los iconos para visualizarla, guardarla y eliminarla.

Icono	Descripción
	Vea la captura de pantalla en el navegador.
	Abra la captura de pantalla o guárdela en el sistema local.
	Elimine la captura de pantalla.

1.6.4. Auditoría de la corrección de problemas

OpenText Core Application Security permite a los equipos de desarrollo y seguridad de una organización auditar la corrección de problemas, donde varios roles de usuario participan en el flujo de trabajo de corrección de problemas. Los usuarios con el permiso **Editar problemas** (generalmente el equipo de desarrollo) reciben los problemas, y deciden si deben corregirlos o no. Los usuarios con el permiso **Auditar problemas** (generalmente el equipo de seguridad) validan los problemas una vez que el equipo de desarrollo termina su labor, y deciden si deben suprimirlos o no. Los usuarios con el permiso **Ver problemas** pueden ver los problemas, pero no pueden realizar ningún cambio.

Esta sección contiene los siguientes temas:

- [Flujo de trabajo de auditoría para auditores](#)
- [Flujo de trabajo de auditoría para desarrolladores](#)

1.6.4.1. Flujo de trabajo de auditoría para auditores

En los siguientes procedimientos, se describe el flujo de trabajo típico que sigue un equipo de seguridad para asignar nuevos problemas y revisar los problemas cerrados.

Los auditores del equipo de seguridad necesitan el permiso de auditoría de problemas, que les permite editar los campos **Estado del auditor** y **Gravedad**.

Asignación de un problema nuevo

Un problema nuevo llega a la cola con los siguientes valores predeterminados:

- **Estado del desarrollador:** **Abierto**
- **Usuarios:** (Sin configurar)
- **Estado del auditor:** **Pendiente de revisión**
- **Gravedad:** predeterminada por OpenText Core Application Security

El equipo de seguridad analiza el problema y se lo asigna a un desarrollador para su corrección.

Para asignar un nuevo problema a un desarrollador para que lo corrija:

1. Revise un problema en el que **Estado del desarrollador** esté configurado como **Abierto**.
2. Si es necesario, seleccione una gravedad de problema diferente en la lista **Gravedad**. Para obtener más información sobre la gravedad de los problemas, consulte [Orden de prioridad](#).
3. Seleccione el desarrollador al que se le asignará el problema en la lista **Usuario**.

Revisión de problemas cerrados

Después de trabajar en el problema, el desarrollador cambia el **Estado del desarrollador** a un estado cerrado (**Corregido**, **No se solucionará** o **Componente de terceros**). A continuación, el problema regresa a la cola de problemas del equipo de seguridad para su auditoría.

Para revisar un problema cerrado:

1. Audite el cambio realizado en el problema cerrado.

2. En función de la evaluación del cambio, decida si se debe suprimir el problema y, a continuación, seleccione el motivo correspondiente de la lista **Estado del auditor**.
 - No suprimido: **Corrección necesaria, Corrección pospuesta, Riesgo mitigado**
 - Suprimido: **Riesgo aceptado, No es un problema**
3. Si seleccionó **Corrección necesaria**, vuelva a asignarle el problema a un desarrollador.
4. Agregue comentarios explicativos.

1.6.4.2. Flujo de trabajo de auditoría para desarrolladores

En los siguientes procedimientos se describe el flujo de trabajo típico que sigue un equipo de desarrollo para corregir y cerrar un problema.

Los desarrolladores del equipo de desarrollo necesitan el permiso de edición de problemas, que les permite editar los campos **Estado del desarrollador** y **Usuario**.

Corrección de un problema

El equipo de seguridad le asigna un problema abierto a un desarrollador para su corrección.

Para corregir un problema:

1. Establezca el **Estado del desarrollador** en la opción **En corrección**.
2. Analice el problema y realice una de las siguientes acciones:
 - Si no considera que el problema sea válido, establézcalo como falso positivo. Consulte Envío de un desafío de falso positivo para obtener más información sobre el proceso de desafío de falso positivo.
 - Corrija el problema.
 - No corrija el problema.

Cierre de un problema

Para cerrar un problema:

1. Cuando haya terminado de trabajar en el problema, establezca el **Estado del desarrollador** como **Corregido**, **No se solucionará** o **Componente de terceros**.

En este momento se cerrará el problema.

2. Agregue comentarios explicativos.
3. Seleccione el auditor que revisará el problema en la lista **Usuario**.

1.6.5. Auditoría y corrección con SAST Aviator

El servicio SAST Aviator aprovecha la inteligencia artificial generativa (IAG) con el modelo de lenguaje grande (LLM) Claude 3,5 Sonnet para auditar los resultados y brindar una guía de corrección mejorada. La guía de corrección consta de comentarios agregados a los resultados del análisis e incluye fragmentos de código.

SAST Aviator se aplica para analizar los resultados después de la auditoría inicial de Fortify Audit Assistant. El contenido de SAST Aviator se añade a los resultados del análisis y se importa a OpenText Core Application Security. El contenido está disponible en el portal y la API.

Disponibilidad y cobertura

- SAST Aviator está disponible para evaluaciones estáticas con auditoría automatizada.
- Para obtener detalles sobre las pilas de tecnología, las categorías y los tipos de archivos compatibles, consulte [Inicio - Core SAST Aviator](#).
- En el caso de resultados de análisis excepcionalmente grandes o resultados de análisis con una cantidad excepcionalmente grande de problemas en una categoría, SAST Aviator podría restringirse a un subconjunto de problemas en cada categoría.

Guía de auditoría y corrección

SAST Aviator revisa los problemas con el **Estado del auditor** de **Pendiente de revisión**. SAST Aviator actualiza el **Estado del auditor** y añade notas. Estas acciones se registran en la pestaña **Historial** del panel de detalles del problema en las páginas de Problemas. Las acciones de auditoría se registran como **Auditorías**; las orientaciones de corrección se registran como **Comentarios**.

- Los falsos positivos se marcan como **No es un problema** y automáticamente se suprimen.

Vulnerabilidad
Recomendaciones
Código
Diagrama
Más pruebas
Historial

☐ Auditorías
☐ Comentarios
☒ Eventos del sistema

OpenText™ Core Application Security 2025/09/24 02:26:40 AM
Problema encontrado en el análisis 64719 de la versión R_PHP_default.

Core SAST Aviator 2025/09/24 02:26:35 AM
 Se cambió el estado del auditor de 'Pendiente de revisión' a 'No es un problema'

- Los falsos positivos provisionales se marcan como **Propuesto como no es un problema** y no se suprimen.

Vulnerabilidad Recomendaciones Código Diagrama Más pruebas ▾

Historial

☒ Auditorías ☒ Comentarios ☒ Eventos del sistema

OpenText™ Core Application Security 2025/09/24 02:26:40 AM
Problema encontrado en el análisis 64719 de la versión R_PHP_default.

Core SAST Aviator 2025/09/24 02:26:35 AM
Se cambió el estado del auditor de 'Pendiente de revisión' a 'Propuesto como que no es un problema'

Core SAST Aviator 2025/09/24 02:26:35 AM

Este resultado no representa un riesgo de seguridad. La línea en cuestión es 'MAIL_PASSWORD=null' en el archivo .env, que se ha marcado como una contraseña codificada. Sin embargo, en realidad no se trata de una credencial codificada por las siguientes razones:

1. El valor se establece en "null", que actúa como un marcador de posición e indica que actualmente no hay ninguna contraseña definida. Esta es una práctica común en los archivos de configuración para indicar que no se ha proporcionado ningún valor.
2. Esto se encuentra en un archivo de configuración de entorno (.env), diseñado específicamente para definir valores de configuración. En este caso, el valor "null" no se utiliza como una credencial real, sino que indica que no hay ninguna contraseña de correo definida.
3. El nombre de usuario correspondiente también está establecido como "null" ('MAIL_USERNAME=null'), lo que refuerza que se trata simplemente de una configuración de plantilla con valores de marcador de posición.

El valor "null" no es una contraseña real que pueda utilizarse para obtener acceso no autorizado; únicamente indica que la contraseña de correo está sin configurar.

Agregar comentario

Enviar

regresar

- Los positivos reales se marcan como **Corrección necesaria**. La asistencia para la corrección consiste en comentarios adicionales, incluidos fragmentos de código.

Vulnerabilidad Recomendaciones Código Diagrama Más pruebas **Historial**

☐ Auditorías ☐ Comentarios ☐ Eventos del sistema

OpenText™ Core Application Security 2025/09/24 02:26:40 AM
Problema encontrado en el análisis 64719 de la versión R_PHP_default.

Core SAST Aviator 2025/09/24 02:26:35 AM
Se ha cambiado el estado del auditor de 'Pendiente de revisión' a 'Corrección necesaria'

Core SAST Aviator 2025/09/24 02:26:35 AM

Esta es una vulnerabilidad de seguridad legítima. El archivo contiene un ID de clave de acceso de AWS codificado (AKIAIHZXYMTIZQ5A3WRA) directamente en el archivo de configuración shippable.yml. Esto es peligroso porque:

1. Cualquier persona con acceso al repositorio de código fuente puede ver esta credencial
2. Si el repositorio es público, la credencial queda expuesta a todo Internet.
3. Las credenciales de AWS nunca deben codificarse en archivos de configuración, especialmente los que se puedan enviar al control de versiones.

Al observar el resto del archivo, puedo ver que esta ID de clave de acceso de AWS se utiliza en la línea 30 para configurar la CLI de AWS. La clave secreta correspondiente parece estar almacenada en una variable de entorno llamada SAWSSecretKey, a la que se hace referencia en la línea 31. Es probable que la clave secreta esté almacenada en la variable "segura" cifrada en la línea 20.

Para corregir este problema:

En el archivo shippable.yml, reemplace la línea 19 por las siguientes líneas:
- secure: # AWSAccessKeyld debe estar cifrado

La ID de clave de acceso de AWS debe almacenarse como una variable de entorno cifrada mediante la función de variable segura de Shippable, de forma similar a como parece que se maneja la clave secreta en la línea 20. De esta manera, la credencial no quedará expuesta en texto sin formato en el archivo de configuración.

Después de realizar este cambio, deberá actualizar su canalización CI/CD para configurar correctamente la variable de entorno AWSAccessKeyld durante el tiempo de compilación.

Agregar comentario

Agregar

- Los verdaderos positivos provisionales se marcan como **Sospechoso** y no se suprimen.

Vulnerabilidad Recomendaciones Código Diagrama Más pruebas ▾ **Historial**

☐ Auditorías ☒ Comentarios ☐ Eventos del sistema

OpenText™ Core Application Security 2025/09/22 01:54:54 AM
Se ha encontrado un problema en el análisis 64677 de la versión R_2500Payload.

Core SAST Aviator 2025/09/22 01:45:41 AM
Se ha cambiado el estado del auditor de 'Pendiente de revisión' a 'Sospechoso'

Core SAST Aviator 2025/09/22 01:45:41 AM
Este código contiene credenciales de API codificadas en el Dockerfile. El archivo de configuración en '/etc/chromium.d/googleapikeys' incluye:

- Una clave de API de Google: "AlzaSyCkfPOPZXDKNn8hhgu3JrA62wlgC93d44k"
- Un id. de cliente de Google: "811574891467.apps.googleusercontent.com"
- Un secreto de cliente de Google: "kdloedMFGdGla2P1zacGjAQh"

Esto representa un riesgo de seguridad porque:

1. Estas credenciales están expuestas a cualquier persona con acceso al Dockerfile
2. Si se publica la imagen de Docker, estas credenciales se integran en las capas de la imagen
3. Las credenciales no se pueden rotar fácilmente sin reconstruir la imagen
4. Si se ve comprometido, un atacante podría usar estas credenciales para acceder a las API de Google con los permisos otorgados a estas claves

Para solucionar este problema, las credenciales de la API deben proporcionarse en tiempo de ejecución a través de variables de entorno o archivos de configuración montados, en lugar de estar codificado en el Dockerfile.

En el archivo chromium-Copy-Copy/Dockerfile, reemplace las líneas 42-43 con:

```
&& mkdir -p /etc/chromium.d/ \
&& echo '#!/bin/bash\nexport GOOGLE_API_KEY="${GOOGLE_API_KEY}"\nexport\nGOOGLE_DEFAULT_CLIENT_ID="${GOOGLE_DEFAULT_CLIENT_ID}"\nexport\nGOOGLE_DEFAULT_CLIENT_SECRET="${GOOGLE_DEFAULT_CLIENT_SECRET}"' > /etc/chromium.d/googleapikeys
```

Al ejecutar el contenedor, proporcione las credenciales reales como variables de entorno:

```
...
docker run -e GOOGLE_API_KEY=your_api_key -e GOOGLE_DEFAULT_CLIENT_ID=your_client_id -e\nGOOGLE_DEFAULT_CLIENT_SECRET=your_client_secret ...
...
```

Este enfoque permite administrar por separado las credenciales del código y rotarlas sin reconstruir la imagen.

Agregar comentario

Agregar

- Los problemas en marcos, idiomas o categorías no compatibles permanecen como **Pendiente de revisión**.

Vulnerabilidad Recomendaciones Código Diagrama Más pruebas ▾ **Historial**

☐ Auditorías ☐ Comentarios ☐ Eventos del sistema

OpenText™ Core Application Security 2025/01/21 07:30:09 AM
Se ha encontrado un problema en el análisis 62652 de la versión PHP.

OpenText™ Core Application Security 2025/01/13 12:44:49 PM
Se ha encontrado un problema en el análisis 62276 de la versión PHP.

 **Core SAST Aviator** 2025/01/13 12:44:46 PM
Actualmente no admitido por **Core SAST Aviator**

Agregar comentario

Para obtener más información acerca del filtrado y la agrupación de problemas, consulte [Desplazamiento por la página Problemas](#).

1.6.6. Plantillas de auditoría

Las plantillas de auditoría permiten que las decisiones de auditoría se apliquen sistemáticamente a análisis estáticos, dinámicos, móviles y de código abierto. Una plantilla de auditoría consta de filtros personalizados que suprimen los problemas o cambian la gravedad de estos en todos los análisis del tipo especificado.

Puede crearse una plantilla de auditoría para cada tipo de análisis a nivel global y a nivel de aplicación. Los líderes en seguridad pueden administrar plantillas de auditoría globales, mientras que los usuarios con permiso para **Editar problemas** pueden administrar plantillas de auditoría para las aplicaciones a las que tengan acceso.



Important

La plantilla de auditoría es una función avanzada y puede provocar cambios significativos en las métricas y los informes de vulnerabilidad. Debe revisar la documentación antes de utilizar plantillas de auditoría. Si tiene más preguntas, póngase en contacto con el equipo de soporte.

Esta sección contiene los siguientes temas:

- [Creación de una plantilla de auditoría global](#)
- [Creación de una plantilla de auditoría de aplicaciones](#)
- [Creación de un filtro de plantilla de auditoría de aplicaciones para un problema](#)
- [Uso de plantillas de auditoría y ejemplos](#)

1.6.6.1. Creación de una plantilla de auditoría global

Los líderes en seguridad pueden administrar plantillas de auditoría global. Las plantillas de auditoría global se aplican a todos los análisis del tipo especificado en el inquilino.

Las plantillas de auditoría están sujetas a las siguientes condiciones:

- Los filtros de plantillas de auditoría no distinguen mayúsculas de minúsculas.
- Los filtros de plantillas de auditoría modificadas o de nueva creación se aplican a análisis publicados para avanzar.

Para crear una plantilla de auditoría global:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Herramientas de auditoría**.

Aparecerá la página Herramientas de auditoría avanzadas.

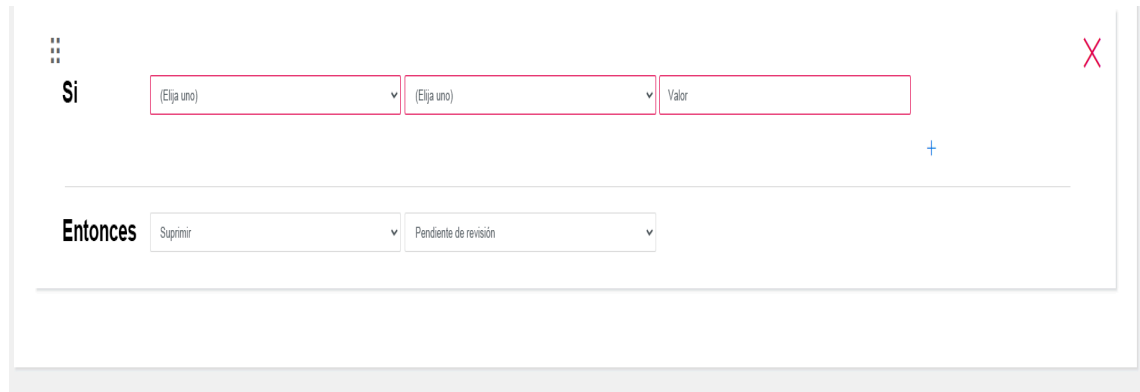


3. En la pestaña **Plantilla de auditoría global**, en la lista **Tipo de análisis**, seleccione el tipo de análisis al que se aplicará la plantilla de auditoría global.

4. Siga los pasos descritos a continuación para agregar un filtro. Puede agregar varios filtros.

1. Haga clic en **Agregar filtro**.

Aparecerá un filtro en blanco.



2. Especifique las condiciones del filtro.

1. En la fila **SI**, seleccione un atributo de problema o un atributo personalizado para filtrar:



Note

Fortify Software Security Content establece los atributos de problema estáticos, dinámicos y móviles. Sonatype establece los atributos de problema de código abierto.

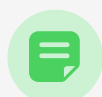
Campo	Tipo de análisis	Descripción
Gravedad	Estático, dinámico, móvil, código abierto	Gravedad del problema
Id. de regla	Estático, dinámico, móvil, código abierto	Un identificador único para la regla que identificó un problema. Puede encontrar el identificador de regla en la pestaña Vulnerabilidad del panel de detalles del problema.
Kingdom	Estático, dinámico, móvil	Clasificación Siete reinos perniciosos
Categoría	Estático, dinámico, móvil	Categoría de vulnerabilidad, que contiene uno o varios identificadores de regla. Un filtro basado en una categoría se aplicará a todos los identificadores de regla que pertenezcan a dicha categoría.

Campo	Tipo de análisis	Descripción
<Atributo de la aplicación personalizado>	Estático, dinámico, móvil	Atributos personalizados del inquilino (lista de selección, texto y booleanos).
URL	Dinámico, móvil	URL del problema
Cuerpo	Dinámico, móvil	Cuerpo del mensaje de HTTP
Encabezados	Dinámico, móvil	Encabezado de solicitud de HTTP
Parámetros	Dinámico, móvil	Parámetros de consulta de HTTP
Nombre del componente	Código abierto	Nombre del componente
Versión del componente	Código abierto	Versión del componente
Ubicación de archivo	Código abierto	Ubicación de archivo

2. Seleccione uno de los operadores siguientes:

Operador	Descripción
Contiene	Busca los resultados que contienen el valor especificado
No contiene	Busca los resultados que no contienen el valor especificado
Es igual a	Busca una coincidencia exacta con el valor especificado
No es igual a	Busca resultados que no coincidan con el valor especificado

3. Escriba el valor del atributo de problema. No se admiten caracteres comodín.



Note

Si ha seleccionado anteriormente un atributo personalizado de lista de selección o booleano y el operador **Es igual a**, los valores se rellenan automáticamente.

4. En caso necesario, haga clic en **+** para crear más condiciones de filtro.
5. Seleccione **Y** u **O** para combinar varias condiciones de filtro.
3. En la fila **ENTONCES**, seleccione una de las siguientes acciones de auditoría para aplicarla a los resultados que coincidan con la búsqueda:

Operador	Descripción
Suprimir	Suprime los resultados que coincidan con el filtro. Puede seleccionar el siguiente estado del auditor que se aplicará cuando la supresión se produzca automáticamente. ▪ Pendiente de revisión ▪ Riesgo aceptado ▪ No es un problema ▪ Estado del auditor de Aviator suprimido
Definir gravedad	Establece la gravedad del problema de los resultados coincidentes en el valor especificado.

- Para reordenar la ubicación de un filtro, haga clic en  y arrastre el filtro a la ubicación que desee.
 - Cuando haya acabado de agregar y organizar los filtros, haga clic en **Guardar**.
- La plantilla de auditoría global se guardará.

Temas relacionados:

Para obtener información sobre la creación de una plantilla de auditoría global, consulte [Creación de una plantilla de auditoría de aplicaciones](#).

1.6.6.2. Creación de una plantilla de auditoría de aplicaciones

Los usuarios que tienen el permiso de **Auditoría de problemas** pueden administrar las plantillas de auditoría para las aplicaciones a las que tienen acceso. Una plantilla de auditoría de aplicaciones se aplica a todos los análisis del tipo especificado para la aplicación.

Las plantillas de auditoría están sujetas a las siguientes condiciones:

- Los filtros de plantillas de auditoría no distinguen mayúsculas de minúsculas.
- Los filtros de plantillas de auditoría modificadas o de nueva creación se aplican a análisis publicados para avanzar.

Para crear una plantilla de auditoría de aplicaciones:

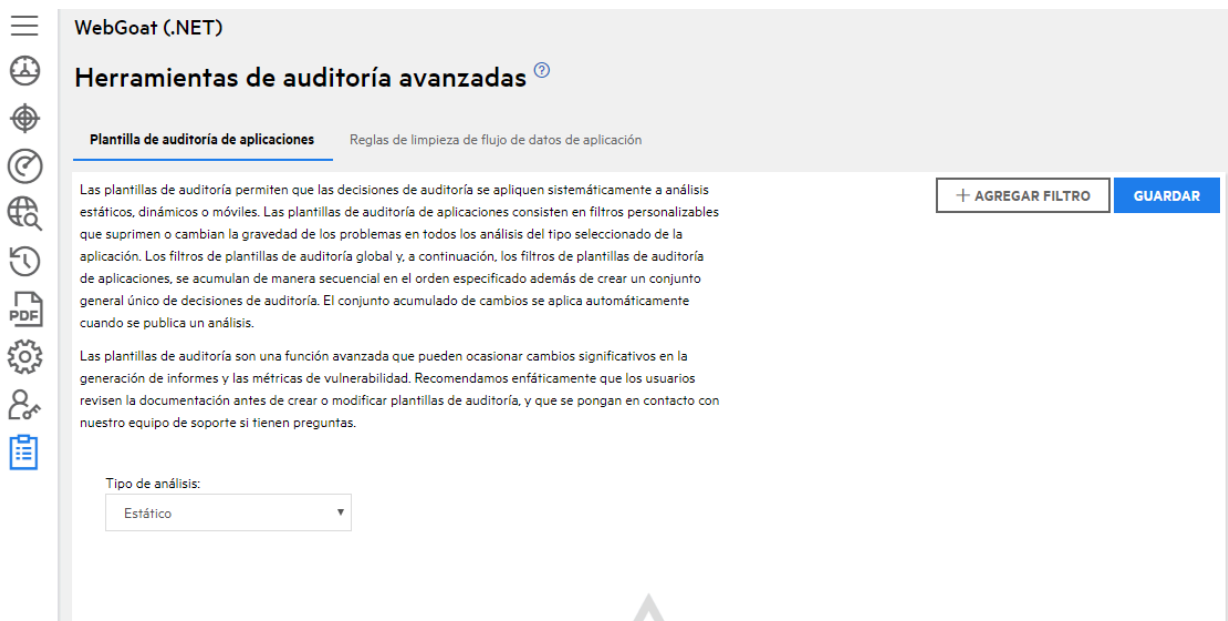
1. Seleccione la vista **Aplicación**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación para la que desea crear una plantilla de auditoría de aplicaciones.

3. Haga clic en **Herramientas de auditoría**.

Aparecerá la página Herramientas de auditoría avanzadas.

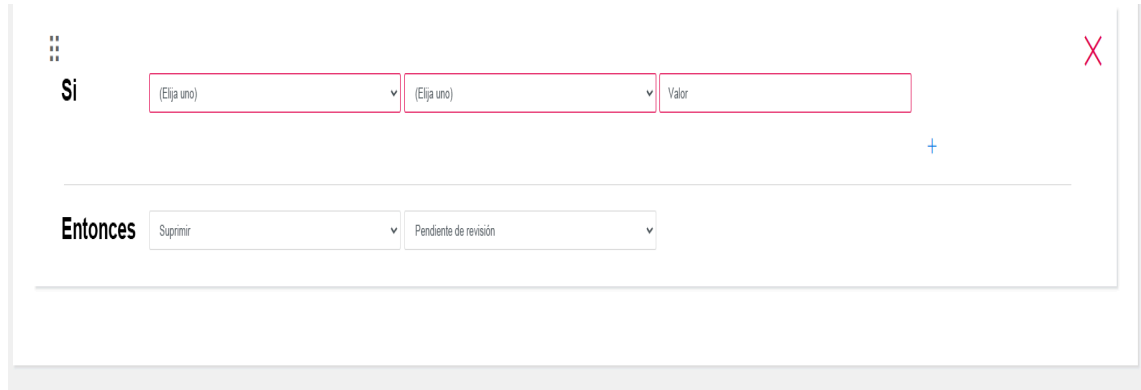


4. En la pestaña **Plantilla de auditoría de aplicaciones**, en la lista **Tipo de análisis**, seleccione el tipo de análisis al que se aplicará la plantilla de auditoría de aplicaciones.

5. Siga los pasos descritos a continuación para agregar un filtro. Puede agregar varios filtros.

1. Haga clic en **Agregar filtro**.

Aparecerá un filtro en blanco.



2. Especifique las condiciones del filtro.

1. En la fila **SI**, seleccione uno de los siguientes atributos de problema para usar de filtro:



Note

Fortify Software Security Content establece los atributos de problema estáticos, dinámicos y móviles. Sonatype establece los atributos de problema de código abierto.

Campo	Tipo de análisis	Descripción
Gravedad	Estático, dinámico, móvil, código abierto	Gravedad del problema.
Id. de regla	Estático, dinámico, móvil, código abierto	Un identificador único para la regla que identificó un problema. Puede encontrar el id. de regla en la pestaña Vulnerabilidad cuando consulte los detalles del problema.
Kingdom	Estático, dinámico, móvil	Clasificación Siete reinos perniciosos.
Categoría	Estático, dinámico, móvil	Categoría de vulnerabilidad, que contiene uno o varios identificadores de regla. Un filtro basado en una categoría se aplicará a todos los identificadores de regla que pertenezcan a dicha categoría.

Campo	Tipo de análisis	Descripción
Archivo	Estático	Ruta de archivo completa
Paquete	Estático	Paquete o espacio de nombre
Código fuente	Estático	Función de origen de flujo de datos
Receptor	Estático	Función de receptor de flujo de datos
URL	Dinámico, móvil	URL del problema
Cuerpo	Dinámico, móvil	Cuerpo del mensaje de HTTP
Encabezados	Dinámico, móvil	Encabezado de solicitud de HTTP
Parámetros	Dinámico, móvil	Parámetros de consulta de HTTP
Nombre del componente	Código abierto	Nombre del componente
Versión del componente	Código abierto	Versión del componente
Ubicación de archivo	Código abierto	Ubicación de archivo

2. Seleccione uno de los operadores siguientes:

Operador	Descripción
Contiene	Busca los resultados que contienen el valor especificado
No contiene	Busca los resultados que no contienen el valor especificado
Es igual a	Busca una coincidencia exacta con el valor especificado
No es igual a	Busca resultados que no coincidan con el valor especificado

3. Escriba el valor del atributo de problema. No se admiten caracteres comodín.
4. En caso necesario, haga clic en + para crear más condiciones de filtro.
5. Seleccione **Y** u **O** para combinar varias condiciones de filtro.

3. En la fila **ENTONCES**, seleccione una de las siguientes acciones de auditoría para aplicarla a los resultados que coincidan con la búsqueda:

Operador	Descripción
Suprimir	Suprime los resultados que coincidan con el filtro. Puede seleccionar el siguiente estado del auditor que se aplicará cuando la supresión se produzca automáticamente. ▪ Pendiente de revisión ▪ Riesgo aceptado ▪ No es un problema ▪ Estado del auditor de Aviator suprimido
Definir gravedad	Establece la gravedad del problema del resultado coincidente en el valor especificado

6. Para reordenar la ubicación de un filtro, haga clic en  y arrastre el filtro a la ubicación que desee.

7. Cuando haya acabado de agregar y organizar los filtros, haga clic en **Guardar**.

Se guardó la plantilla de auditoría de aplicaciones.

Temas relacionados:

Para obtener información sobre la creación de una plantilla de auditoría global, consulte [Creación de una plantilla de auditoría global](#).

1.6.6.3. Creación de un filtro de plantilla de auditoría de aplicaciones para un problema

Además de crear una plantilla de auditoría de aplicaciones desde cero, los usuarios con el permiso **Auditar problemas** pueden crear filtros de plantilla de auditoría de aplicaciones para un problema en la página Problemas. Esto permite a los auditores aplicar fácilmente las decisiones de auditoría a los problemas mientras los revisan.

Siga los siguientes pasos para crear un filtro de plantilla de auditoría de aplicaciones para un problema:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación que desea auditar.

Aparecerá la página Información general de la aplicación.

3. Desplácese hasta la página Problemas de la aplicación o Problemas de versión.

The screenshot displays the OpenText Core Application Security 26.1 interface. The top navigation bar includes 'opentext | Core Application Security 26.1', 'Applications', 'Dashboard', 'Reports', and 'Administration'. A search bar and 'AUTO-TAM' dropdown are on the right. The left sidebar shows a '24.4 API Demos' section and 'Application Issues' with a search bar and filters (6K, 18K, 5K, 4K, 35K). A list of issues is shown, with 'azuredeploy.json : 206' selected. The main panel shows details for 'Samples/SCA/dev/azure-quickstart-templates/application-workloads/apache/...' with a 'Critical' severity and 'Azure ARM Misconfiguration: Improper Compute VM Access Control' rule. It includes a 'Summary', 'Explanation', and a code snippet for 'Example 1'. The right sidebar shows 'Audit' details: Status (New), Introduced Date (2023/01/30), Last Found Date (2023/01/30), Assigned User (Not Set), Developer Status (Open), Auditor Status (Pending Review), Severity (Critical), and a Comment field with an 'Add' button. At the bottom, there are buttons for 'Submit Bug', 'Add Audit Filter', and 'Assign Attributes'.

4. En el panel de auditoría, haga clic en **Agregar filtro de auditoría**.

Aparecerá la ventana Plantilla de auditoría.

5. Realice la tarea que corresponda:

- Si el problema seleccionado tiene filtros existentes que se aplican, se muestran dichos filtros. Puede editar los filtros.



Note

Si pueden aplicarse varios filtros y uno de ellos es una supresión, solo se muestra ese filtro.

Plantilla de auditoría

×

Los siguientes filtros ya existen en la plantilla de auditoría de la aplicación.

Si **Categoría** Es igual a **Cross-Site Scripting: Reflected**
Y **Id. de regla** Es igual a **D027DAA9-A38E-49E4-BDBF-3DFF657F84CA**
Y **Gravedad** Es igual a **critical**
Y **Reino** Es igual a **Input Validation and Representation**
Y **Archivo** Es igual a **PWC_US_Mashup_Plugins/mashup-libs-2016xR2/cloudview-core.jar/com/exalead/cloudview/indexing/replication/service/ReplicationClientServiceFLISServletDelegate.jav**
Y **Paquete** Es igual a **Java J2EE ServletAPI**
Entonces **Suprimir**

EDITAR FILTRO(S)

CERRAR

1. Haga clic en **Editar filtros**.

Se le redirigirá a la página Plantilla de auditoría de aplicaciones.

2. Edite los filtros existentes según corresponda.

- Si el problema seleccionado no tiene ningún filtro aplicable, puede crear un filtro nuevo a partir de una lista de condiciones predefinidas que se aplican a ese problema.

X

Plantilla de auditoría

Las plantillas de auditoría consisten en filtros personalizables que suprimen o cambian la gravedad de los problemas automáticamente cuando se publica un análisis.

Aplique un filtro cuando se cumplan todas las condiciones seleccionadas.

☒

Categoría Es igual a **Fuga de información del sistema: externa**

☒

Id. de regla Es igual a **243F5467-EFA4-4F69-8C9D-DB1932A9C0C0**

☒

Gravedad Es igual a **Crítico**

☒

Reino Es igual a **Encapsulación**

☒

Origen Es igual a **java.lang.Throwable.getMessage()**

☒

Archivo Es igual a **iwa_java-master/iwa_java-master/Src/IWA-Java-main/src/main/java/com/microfocus/example/config/handlers/BasicAuthenticationEntryPointCus**

☒

Receptor Es igual a **java.io.PrintWriter.println()**

☒

Paquete Es igual a **E/S del núcleo de Java**

Realice la siguiente acción:

☒ Suprimir

Pendiente de revisión ▼

☐ Definir gravedad

(Elija uno) ▼

Crear filtro

Cerrar

1. Seleccione las condiciones de filtro. Varias condiciones se unen con el operador AND.
2. Seleccione la acción de auditoría. Para **Suprimir**, las opciones disponibles son 'Pendiente de revisión', 'Riesgo aceptado', 'No es un problema' y 'Estado del auditor de Aviator suprimido'. Para **Definir gravedad**, las opciones disponibles son 'Crítico', 'Alto', 'Medio' y 'Bajo'.
3. Haga clic en **Crear filtro**. Se guardó el filtro de plantilla de auditoría de aplicaciones.

1.6.6.4. Uso de plantillas de auditoría y ejemplos

Los filtros de plantilla de auditoría se agregan de forma secuencial en el orden en que aparecen. Primero, se agregan los filtros de plantilla de auditoría global y luego los filtros de plantilla de auditoría de aplicaciones, para crear un solo conjunto general de decisiones de auditoría que se aplicarán automáticamente cuando se publique un análisis. Los cambios en problemas a causa de las plantillas de auditoría aparecen en la pestaña **Historial** del panel de detalles del problema como eventos de tipo **Auditoría**. Los cambios de auditoría global y de auditoría de aplicaciones se registran por separado.

En general, use filtros basados en categorías en lugar de filtros basados en reglas, excepto en algunos escenarios en que el uso de filtros basados en reglas puede ser más apropiado. Por ejemplo, podría querer usar filtros basados en identificadores de regla para operar con varias directivas de corrección sobre comprobaciones SSL/TLS en análisis dinámicos.

Es importante que revise sus filtros y los actualice en caso necesario tras cada actualización de contenido de seguridad, ya que estas actualizaciones suponen cambios en categorías y reglas:

- Se podrían agregar nuevas categorías.
- Los nombres de categoría podrían cambiar. Tendría que actualizar cualquier filtro basado en categorías para que refleje los nombres cambiados.
- Se podrían agregar nuevas reglas a las categorías. Algunos filtros de categorías ya existentes podrían aplicarse a las nuevas reglas. Tenga en cuenta que las reglas nuevas cubren vulnerabilidades nuevas y críticas que difieren en gran medida de las reglas ya existentes en una categoría.
- Algunas reglas ya existentes se podrían actualizar para reflejar nuevos estándares o recomendaciones del sector. Por ejemplo, la gravedad dada a una vulnerabilidad podría aumentar a causa de nueva información relativa a dicha vulnerabilidad.

Para obtener más información sobre cambios de reglas y categorías, consulte las actualizaciones trimestrales de contenido de seguridad de software de Fortify de Fortify Software Security Research (SSR). Podrá encontrar esta información en el Centro de ayuda.

Los siguientes ejemplos muestran varias combinaciones de filtros y cómo se aplican.

Ejemplo 1:

Filtros de plantilla de auditoría:

1. Si **Gravedad Es igual a Crítico**, entonces **Definir gravedad** se ajusta en **Alto**
2. Si **Gravedad Es igual a Crítico**, entonces **Definir gravedad** se ajusta en **Medio**

Resultado: los problemas con valor Crítico se configuran en Medio en el tipo de análisis seleccionado.

Ejemplo 2:

Filtros de plantilla de auditoría:

1. Si **Gravedad Es igual a Crítico**, entonces **Definir gravedad** se ajusta en **Alto**
2. Si **Gravedad Es igual a Alto**, entonces **Definir gravedad** se ajusta en **Medio**

Resultado: los problemas con valor Crítico se configuran en Alto y los problemas con valor Alto se configuran en Medio en el tipo de análisis seleccionado.

Ejemplo 3:

Filtro de plantilla de auditoría: Si **Id. de regla Es igual a 11516**, entonces **Suprimir**.

Resultado: los problemas con el Id. de regla 1156 se suprimen en el tipo de análisis seleccionado.

Ejemplo 4:

Filtro de plantilla de auditoría global: Si **Gravedad Es igual a Crítico**, entonces **Definir gravedad** se ajusta en **Alto**

Filtro de plantilla de auditoría de aplicaciones: Si **Gravedad Es igual a Crítico**, entonces **Definir gravedad** se ajusta en **Medio**

Resultado: los problemas con valor Crítico se establecen en Alto en todos los análisis del tipo seleccionado, pero los problemas con valor Crítico se establecen en Medio en los análisis del tipo seleccionado para la aplicación anterior.

1.6.7. Reglas de limpieza de flujo de datos

Las reglas de limpieza de flujo de datos describen la lógica de validación y otras acciones que limpian los datos dañados (entrada controlada por el usuario). Las reglas de limpieza de flujo de datos se incorporan en un análisis estático para ayudar a OpenText SAST a reconocer las funciones de limpieza. De este modo, las reglas de limpieza de flujo de datos ayudan a evitar los falsos positivos relacionados con los problemas de flujo de datos.

Las reglas de limpieza de flujo de datos se pueden crear a nivel global y de aplicación. Los líderes en seguridad pueden administrar reglas de limpieza de flujo de datos globales; por su parte, los usuarios con el permiso de **Auditar problemas** pueden administrar reglas de limpieza de flujo de datos para las aplicaciones a las que tengan acceso.



Important

La regla de limpieza de flujo de datos es una característica avanzada y puede generar cambios significativos en las vulnerabilidades encontradas en un análisis. OpenTextEl Portal de MSP recomienda encarecidamente que revise la documentación antes de usar las reglas de limpieza de flujo de datos. Si tiene más preguntas, póngase en contacto con soporte.

Esta sección contiene los siguientes temas:

- [Creación de una regla de limpieza de flujo de datos global](#)
- [Creación de una regla de limpieza de flujo de datos de aplicación](#)
- [Uso de reglas de limpieza de flujo de datos y ejemplos](#)

1.6.7.1. Creación de una regla de limpieza de flujo de datos global

Los líderes en seguridad pueden administrar reglas de limpieza de flujo de datos globales. Las reglas de limpieza de flujo de datos globales se aplican a todos los análisis estáticos en el inquilino.

Las reglas de limpieza de flujo de datos están sujetas a las siguientes condiciones:

- Las reglas de limpieza de flujo de datos distinguen entre mayúsculas y minúsculas, y solo admiten caracteres alfanuméricos.
- Las reglas de limpieza de flujo de datos se aplican a los análisis que se inician después de la creación de la regla.

Para crear una regla de limpieza de flujo de datos global:

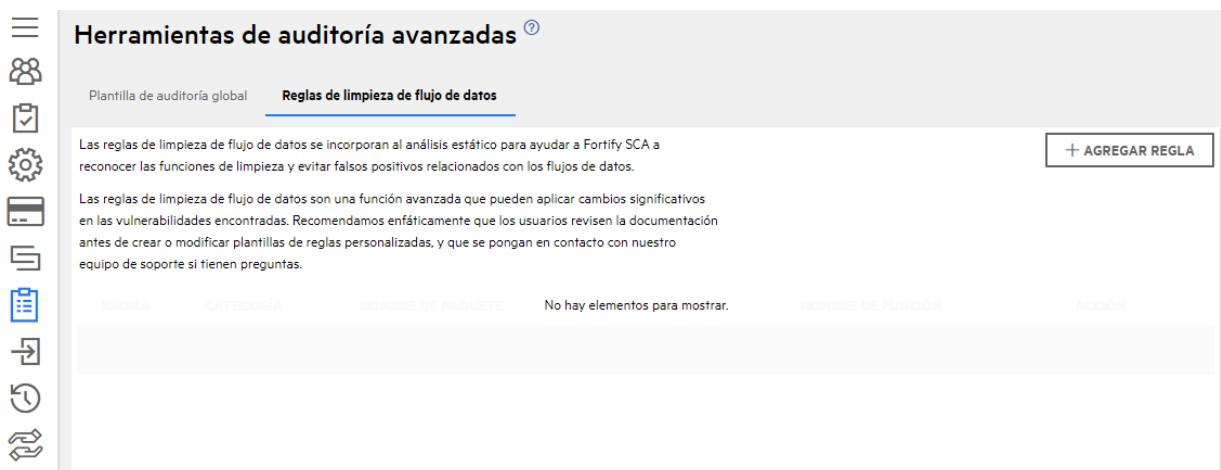
1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Herramientas de auditoría**.

Aparecerá la página Herramientas de auditoría avanzadas.

3. Seleccione la pestaña **Reglas de limpieza de flujo de datos**.



4. Siga los pasos descritos a continuación para agregar una regla. Puede agregar varias reglas.

1. Haga clic en **Agregar regla**.

Se abrirá la ventana Agregar regla.

Agregar regla

Idioma

(Elija uno) ▼

Categoría

(Elija una) ▼

Nombre de paquete ⓘ

Validación de datos ⓘ

(Elija uno) ▼

Nombre de clase ⓘ

Nombre de función ⓘ

GUARDAR

CANCELAR

2. Rellene los campos según sea necesario. Los campos son obligatorios a menos que se indique lo contrario.



Note

Las reglas no se aplican a interfaces ni superclases.

Campo	Descripción
Idioma	Seleccione el componente tecnológico.
Nombre de paquete	(Opcional) Escriba el nombre del paquete o el espacio de nombres que contiene la función de validación. Si no especifica un nombre de paquete, la regla solo responderá a funciones que no estén dentro del paquete.

Campo	Descripción
Nombre de clase	(Opcional) Escriba el nombre de la clase que contiene la función de validación. Si no especifica una clase de nombre, la regla solo responderá a funciones que no estén dentro de la clase. Para especificar una clase anidada, use la notación de puntos (por ejemplo, <code>ClaseExterna.ClaseAnidada</code>). Note Para los idiomas .NET, la convención para el nombre de una clase genérica consiste en agregar al nombre de clase el símbolo @ y el número de parámetros de tipo. Por ejemplo, para <code>System.Func<T, TResult></code> , el nombre de clase sería <code>Func@2</code> .
Nombre de función	Escriba el nombre de la función de validación.
Categoría	Seleccione la categoría de vulnerabilidad que corrige esta función de validación.

Campo	Descripción
Validación de datos	Seleccione los datos validados por la función: ▪ Valor devuelto: use esta opción para hacer referencia a <code>value</code> en <code>value = web.getWebInput(foo, bar)</code> ▪ Función de objeto: use esta opción para hacer referencia a <code>web</code> en <code>value = web.getWebInput(foo, bar)</code> o <code>object</code> en <code>object = new MyObject()</code> ▪ Argumento: use esta opción para referirse a argumentos de la función. Los argumentos se indexan comenzando por 0. Por ejemplo, indique 1 para hacer referencia a <code>bar</code> en <code>value = web.getWebInput(foo, bar)</code> Ejemplo: <pre>string filename = UploadedFile.FileName(); if (Validators.IsValidFileName(fil ename)) { System.IO.File.Delete(filename); }</pre> Uso de reglas de limpieza de flujo de datos y ejemplos: Las reglas de limpieza de flujo de datos globales y de aplicación se agrupan en un único conjunto de reglas que se aplican durante el análisis. Los problemas

Campo	Descripción
	eliminados a partir de las reglas no se muestran en el FPR. Los siguientes ejemplos muestran varias reglas de limpieza de flujo de datos y cómo se aplican: Example1: Lenguaje: Java Nombre de paquete: com.fortify.appsec Nombre de clase: Validation Nombre de función: validateAlphaNumeric Categoría: Inyección de código SQL Validación de datos: Valor devuelto Resultado: El valor devuelto por el método se considera limpio y no se marcará como problema de inyección de código SQL. Example2: Lenguaje: Java Nombre de paquete: java.util Nombre de clase: Map Nombre de función: clear Categoría: Inyección de código SQL Validación de datos: Función de objeto Resultado: los datos se consideran limpios tras una llamada al método Map.clear() y no se marcarán como problema de inyección de código SQL.

5. Cuando haya terminado de agregar reglas, haga clic en **Guardar**.

Se guardarán las reglas de limpieza de flujo de datos globales.

1.6.7.2. Creación de una regla de limpieza de flujo de datos de aplicación

Los usuarios que tienen el permiso de **Auditar problemas** pueden administrar las reglas de limpieza de flujo de datos para las aplicaciones a las que tienen acceso. Las reglas de limpieza de flujo de datos de aplicación se aplican a todos los análisis estáticos de la aplicación.

Las reglas de limpieza de flujo de datos están sujetas a las siguientes condiciones:

- Las reglas de limpieza de flujo de datos distinguen entre mayúsculas y minúsculas, y solo admiten caracteres alfanuméricos.
- Las reglas de limpieza de flujo de datos se aplican a los análisis que se inician después de la creación de la regla.

Para crear una regla de limpieza de flujo de datos de aplicación:

1. Seleccione la vista **Aplicación**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación para la que desea crear una plantilla de auditoría de aplicaciones.

3. Haga clic en **Herramientas de auditoría**.

Aparecerá la página Herramientas de auditoría avanzadas.

4. Seleccione la pestaña **Reglas de limpieza de flujo de datos**.



5. Siga los pasos descritos a continuación para agregar una regla. Puede agregar varias reglas.

1. Haga clic en **Agregar regla**.

Se abrirá la ventana Agregar regla.

Agregar regla
✕

Idioma

(Elija uno) ▼

Nombre de paquete ⓘ

Nombre de clase ⓘ

Nombre de función ⓘ

Categoría

(Elija una) ▼

Validación de datos ⓘ

(Elija uno) ▼

GUARDAR

CANCELAR

2. Rellene los campos según sea necesario. Los campos son obligatorios a menos que se indique lo contrario.



Note

Las reglas no se aplican a interfaces ni superclases.

Campo	Descripción
Idioma	Seleccione el componente tecnológico.
Nombre de paquete	(Opcional) Escriba el nombre del paquete o el espacio de nombres que contiene la función de validación. Si no especifica un nombre de paquete, la regla solo responderá a funciones que no estén dentro del paquete.

Campo	Descripción
Nombre de clase	(Opcional) Escriba el nombre de la clase que contiene la función de validación. Si no especifica una clase de nombre, la regla solo responderá a funciones que no estén dentro de la clase. Para especificar una clase anidada, use la notación de puntos (por ejemplo, <code>ClaseExterna.ClaseAnidada</code>).  Note Para los idiomas .NET, la convención para el nombre de una clase genérica consiste en agregar al nombre de clase el símbolo @ y el número de parámetros de tipo. Por ejemplo, para <code>System.Func<T, TResult></code> , el nombre de clase sería <code>Func@2</code> .
Nombre de función	Escriba el nombre de la función de validación.
Categoría	Seleccione la categoría de vulnerabilidad que corrige esta función de validación.

Campo	Descripción
Validación de datos	Seleccione los datos validados por la función: ▪ Valor devuelto: use esta opción para hacer referencia a <code>value</code> en <code>value = web.getWebInput(foo, bar)</code> ▪ Función de objeto: use esta opción para hacer referencia a <code>web</code> en <code>value = web.getWebInput(foo, bar)</code> o <code>object</code> en <code>object = new MyObject()</code> ▪ Argumento: use esta opción para referirse a argumentos de la función. Los argumentos se indexan comenzando por 0. Por ejemplo, indique 1 para hacer referencia a <code>bar</code> en <code>value = web.getWebInput(foo, bar)</code>

6. Cuando haya terminado de agregar reglas, haga clic en **Guardar**.

Se guardarán las reglas de limpieza de flujo de datos de aplicación.

1.6.7.3. Uso de reglas de limpieza de flujo de datos y ejemplos

Las reglas de limpieza de flujo de datos globales y de aplicación se agrupan en un único conjunto de reglas que se aplican durante el análisis. Los problemas eliminados a partir de las reglas no se muestran en el FPR.

Los siguientes ejemplos muestran varias reglas de limpieza de flujo de datos y cómo se aplican.

Ejemplo 1:

Lenguaje: **Java**

Nombre de paquete: `com.fortify.appsec`

Nombre de clase: `Validation`

Nombre de función: `validateAlphaNumeric`

Categoría: **Inyección de código SQL**

Validación de datos: **Valor devuelto**

Resultado: el valor devuelto por el método se considera limpio y no se marcará como problema de inyección de código SQL.

Ejemplo 2:

Lenguaje: **Java**

Nombre de paquete: `java.util`

Nombre de clase: `Map`

Nombre de función: `clear`

Categoría: **Inyección de código SQL**

Validación de datos: **Función de objeto**

Resultado: los datos se consideran limpios tras una llamada al método `Map.clear()` y no se marcarán como problema de inyección de código SQL.

1.6.8. Solicitud de un análisis de corrección

Una vez realizados los cambios para solucionar los problemas identificados en el análisis inicial, puede solicitar un análisis de corrección para comprobar si se solucionaron los problemas. Las evaluaciones incluyen uno o más análisis de corrección:

- Las evaluaciones únicas incluyen un análisis de corrección.
- Las suscripciones incluyen análisis de corrección ilimitados durante el periodo de análisis de corrección.
- El periodo de análisis de corrección es de 30 días después del análisis inicial. Las excepciones están indicadas en su contrato.

Para solicitar un análisis de corrección, seleccione **<tipo_evaluación> - Corrección** en la página Configuración del análisis. El análisis de corrección debe realizarse en la misma aplicación. Por ejemplo, si el análisis inicial se realizó en el sitio de preproducción, el análisis de corrección debe llevarse a cabo en el mismo sitio de preproducción. Un análisis de corrección tarda menos tiempo que un análisis inicial completo.



Note

Algunos campos del análisis dinámico están bloqueados para su edición. Para obtener más información, consulte [Edición de la configuración de análisis dinámico para análisis en curso y completados](#).

1.7. Paneles e informes

OpenText Core Application Security ofrece los resultados de las evaluaciones en distintos formatos para visualizar y analizar los datos.

Los paneles presentan una visualización de las métricas clave. Los usuarios pueden configurar varios paneles para mostrar los datos que sean relevantes según sus necesidades. Mientras que los paneles resultan útiles para realizar resúmenes generales, los usuarios pueden obtener una vista detallada de los resultados de las evaluaciones mediante informes. OpenText Core Application Security proporciona un conjunto de informes completo y personalizable.

Esta sección contiene los siguientes temas:

- [Paneles de Magellan](#)
- [Paneles heredados](#)
- [Informes](#)

1.7.1. Paneles de Magellan

El portal ha implementado paneles nuevos que aprovechan la plataforma de Magellan OpenText Core Application Security. Los paneles nuevos ofrecerán un resumen integral de programas de seguridad de aplicaciones, información sobre métricas de vulnerabilidad importantes y vistas de panel coherentes entre los productos del conjunto de Fortify. Los paneles de control de Magellan están disponibles junto con los paneles heredados.

Están disponibles los siguientes tipos de paneles predeterminados:

- Descripción ejecutiva
- Información general del programa

Un tablero de Magellan está compuesto por:

- Puntos de datos singulares de métricas clave.
- Gráficos individuales que visualizan una faceta específica de los datos de los inquilinos. Los mosaicos se pueden personalizar a un nivel granular.

Si corresponde, se pueden aplicar filtros a los datos representados en los gráficos. Los usuarios pueden descargar los datos del gráfico, ya sea como el propio gráfico o como datos sin procesar, en varios formatos.

Esta sección contiene los siguientes temas:

- [Visualización de los paneles de Magellan](#)
- [Tipos de paneles de Magellan](#)
- [Limitaciones del panel de Magellan](#)

1.7.1.1. Visualización de los paneles de Magellan

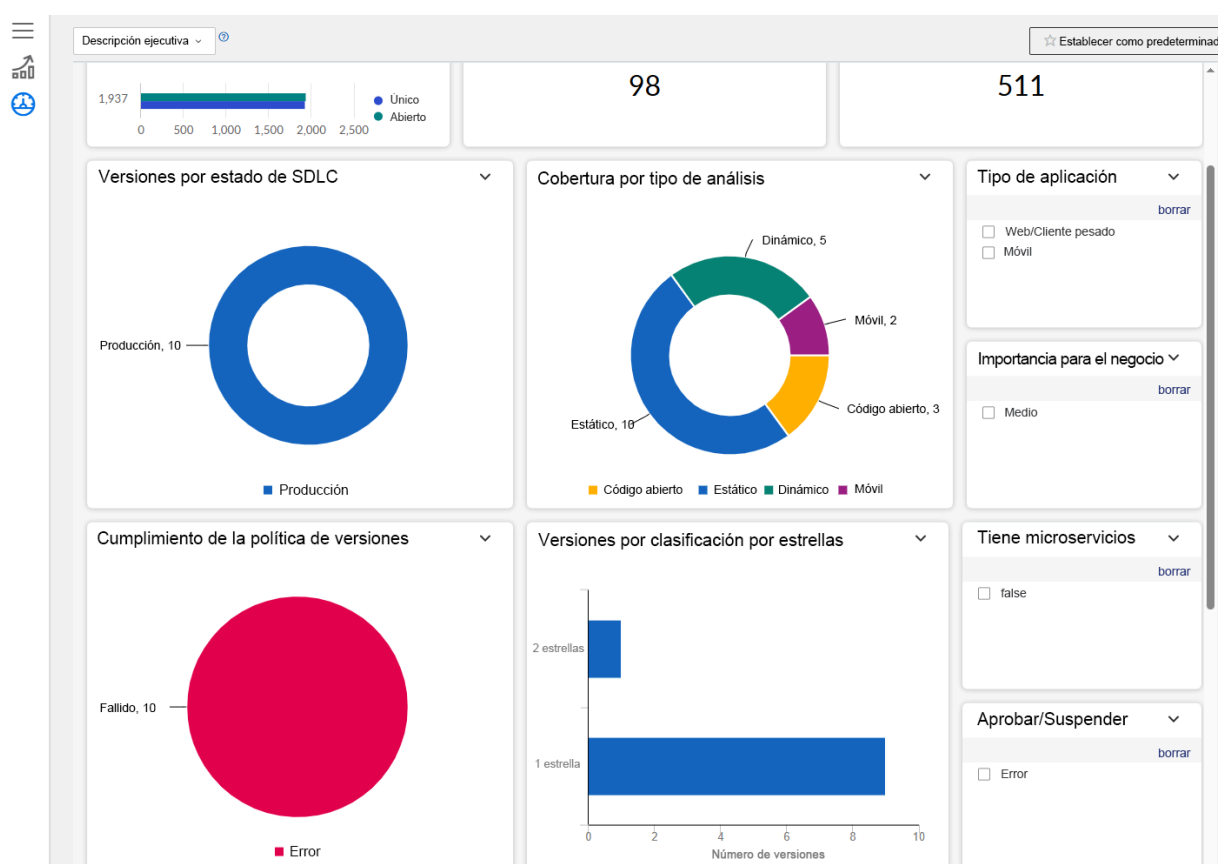
Para ver sus paneles de Magellan:

1. Seleccione la vista **Panel**.

Aparece la página del panel.

2. Haga clic en **Paneles nuevos** en el menú de la izquierda.

Se carga el panel predeterminado de Magellan.



En la siguiente tabla se describe cómo desplazarse por la página del panel de Magellan.

Tarea	Acción
Tareas del panel	
Establezca el panel actual como predeterminado	Haga clic en Establecer como predeterminado .
Filtrar todos los gráficos en el panel	Seleccione uno o más valores de filtro de los siguientes filtros de aplicación y versión: tipo de aplicación, importancia para el negocio, si tiene microservicios, aprobado/suspenso, clasificación por estrellas, estado de SDLC
Tareas de mosaico	
Actualizar los datos utilizados en un gráfico	Haga clic con el botón derecho en el encabezado y seleccione Actualizar .
Mostrar u ocultar el encabezado de un gráfico	Haga clic con el botón derecho en el encabezado y seleccione o deseleccione la casilla de verificación del Encabezado .
Maximizar un mosaico	Haga clic con el botón derecho en el encabezado y seleccione Maximizar.  Note Para restaurar el tamaño original de un gráfico, haga clic con el botón derecho en el encabezado y seleccione Restaurar.
Ajustar el tamaño de un mosaico	Coloque el cursor sobre el borde de un mosaico y haga clic y arrastre los controladores.

Tarea	Acción
Mostrar filtros aplicables a un gráfico	Haga clic con el botón derecho en el encabezado y seleccione Mostrar vínculos . Los filtros aplicables están resaltados con bordes discontinuos.
Tareas de gráficos	
Filtrar un gráfico por categorías.	Haga clic con el botón derecho en el gráfico y seleccione Filtro > Filtro y configure los ajustes.
Filtrar un gráfico por valores superiores e inferiores	Haga clic con el botón derecho en el gráfico y seleccione Filtro > N superior/inferior y configure los ajustes.
Cambiar un tipo de gráfico	Haga clic con el botón derecho en el gráfico y seleccione Cambiar tipo y configure los ajustes.
Editar el formato de un gráfico	Haga clic con el botón derecho en el gráfico y seleccione Formato de gráfico y configure los ajustes.
Exportar datos sin procesar de un gráfico	Haga clic con el botón derecho en el gráfico y seleccione Exportar datos y configure los ajustes. Note   Important Actualmente no se admite la exportación de datos.

Tarea	Acción
Exportar un gráfico (hay varios tipos de archivos disponibles)	Haga clic con el botón derecho en el gráfico, seleccione Exportar contenido y ajuste la configuración
Ver u ocultar los datos sin procesar de un gráfico	Haga clic con el botón derecho en el gráfico y seleccione Ver tabla de datos o bien Ocultar tabla de datos .
Detalles adicionales sobre los conjuntos de datos del gráfico	Coloque el cursor sobre un elemento visual y haga clic en el elemento cuando el cursor cambie a un cursor de mano.

1.7.1.2. Tipos de paneles de Magellan

Estos son los tipos de paneles disponibles:

- Descripción ejecutiva

El panel contiene los siguientes gráficos:



Note

Los gráficos interactivos contienen vínculos para obtener detalles adicionales sobre los conjuntos de datos.

- Versiones por estado de SDLC (sin incluir las versiones retiradas; interactivo)
- Cobertura por tipo de análisis (cubre SAST, SCA, DAST, MAST; interactivo)
- Cumplimiento de la política de versiones (sin incluir versiones retiradas; interactivo)
- Versiones por clasificación por estrellas (sin incluir lanzamientos retirados; interactivo)
- Estado de los problemas por importancia (sin incluir resultados suprimidos e informativos)
- Tendencia del estado de los problemas (sin incluir resultados suprimidos e informativos)

- Información general del programa

El panel contiene los siguientes gráficos:



Note

Los gráficos interactivos contienen vínculos para obtener detalles adicionales sobre los conjuntos de datos.

- Derechos activos
- Aplicaciones por pila tecnológica (las 10 de pilas tecnológicas principales)
- Actividad de análisis por tipo de análisis (cubre SAST, SCA, DAST, MAST; interactivo)

- Desglose de problemas por gravedad
- Los 10 problemas principales de la categoría: versiones de producción, los 10 principales de OWASP 2021, OWASP ASVS 4.0, OWASP 2014 Mobile
- Las 10 principales aplicaciones por problemas (interactivo)



Note

Los gráficos de tendencias no se muestran hasta que haya suficientes datos disponibles.

1.7.1.3. Limitaciones del panel de Magellan

La implementación actual de los paneles de Magellan tiene las siguientes limitaciones:

- No se admite la creación de paneles nuevos ni la personalización de paneles ya existentes.
- No se admiten las funciones de exportación, impresión y uso compartido.
- Los recuentos de problemas en los gráficos no tienen en cuenta la singularidad.
- No se admite la exportación de datos de gráficos.
- En el caso de los chats que no se pueden renderizar debido a datos insuficientes, aparece un mensaje no explicativo "Error al renderizar el gadget".
- No se admite el modo oscuro.

1.7.2. Paneles heredados

Un panel se compone de secciones individuales, cada una de las cuales representa una faceta específica de los datos como un elemento visual. En un principio, se le ofrece una de las siguientes configuraciones de panel predeterminado según su rol de usuario:

- Panel de desarrollo para los roles de desarrollador, desarrollador principal y líder en aplicaciones
- Panel de seguridad para los roles de líder en seguridad y TAM
- Panel de administración para los roles de ejecutivo y revisor
- Panel de administración para los roles personalizados

Puede editar el panel predeterminado, así como crear paneles adicionales.

Esta sección contiene los siguientes temas:

- [Visualización de paneles](#)
- [Tipos de gráfico del panel](#)
- [Creación de un panel](#)
- [Edición de un panel](#)
- [Eliminación de un panel](#)

1.7.2.1. Visualización de paneles

Para visualizar sus paneles:

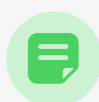
1. Seleccione la vista **Panel**.

Aparece la página del panel. Muestra el último panel que se cargó.



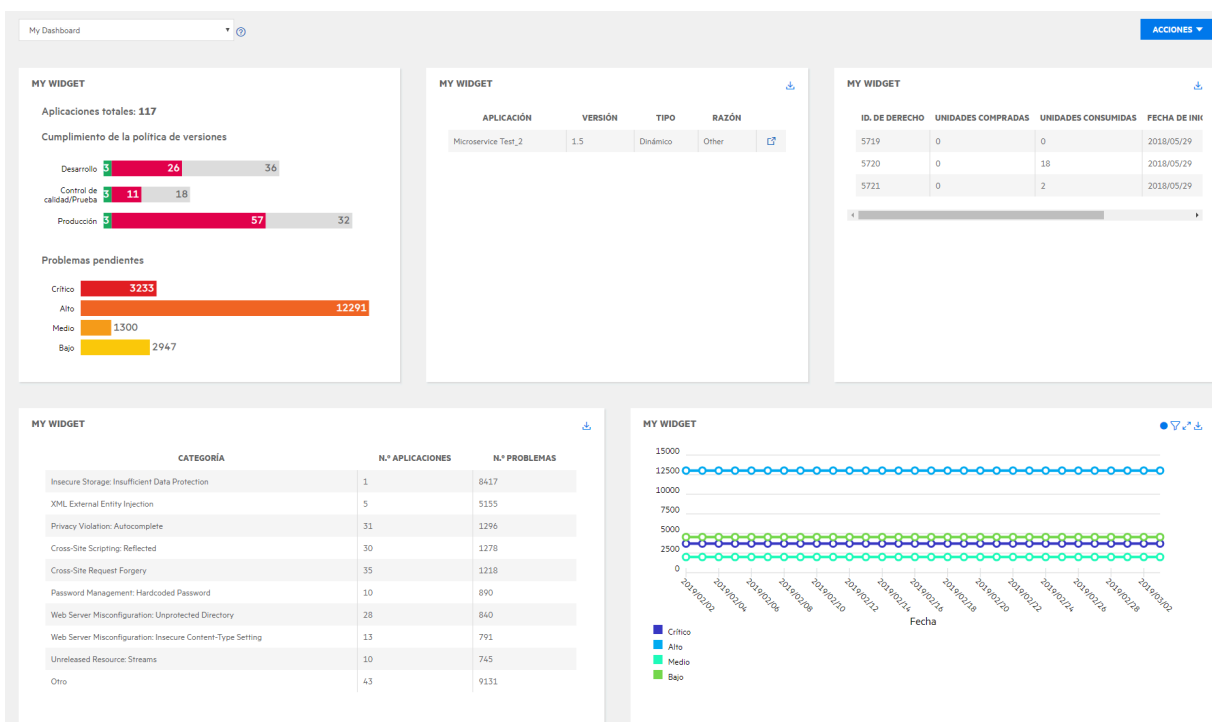
Note

Si aún no ha configurado ningún panel, se cargará la configuración de panel predeterminada basada en su rol de usuario.



Note

En el modo de prueba hay disponible un panel de ejemplo no editable para fines de visualización.



2. En la lista desplegable, seleccione el panel que desea ver.

Se cargará el panel seleccionado.

En la siguiente tabla, se describe cómo desplazarse por la página del panel.

Tarea	Acción
Crear un panel	Seleccione Acciones > Nuevo panel . Para obtener más información, consulte Creación de un panel .
Editar el panel	Seleccione Acciones > Editar panel . Para obtener más información, consulte Edición de un panel .
Generar un PDF del panel	Seleccione Acciones > Imprimir .
Mostrar u ocultar marcadores de punto de datos	Haga clic en  en una sección de gráfico de tendencias.
Ver los filtros aplicados a una sección	Haga clic en  .
Exportar los datos que componen una sección	Haga clic en  . El archivo .csv se guarda en forma local en la carpeta especificada en la configuración del navegador.
Ver los detalles de un análisis	Haga clic en  en una sección de cuadrícula de lista.
Ampliar una sección	Haga clic en  en una sección de gráfico de tendencias.

1.7.2.2. Tipos de gráfico del panel

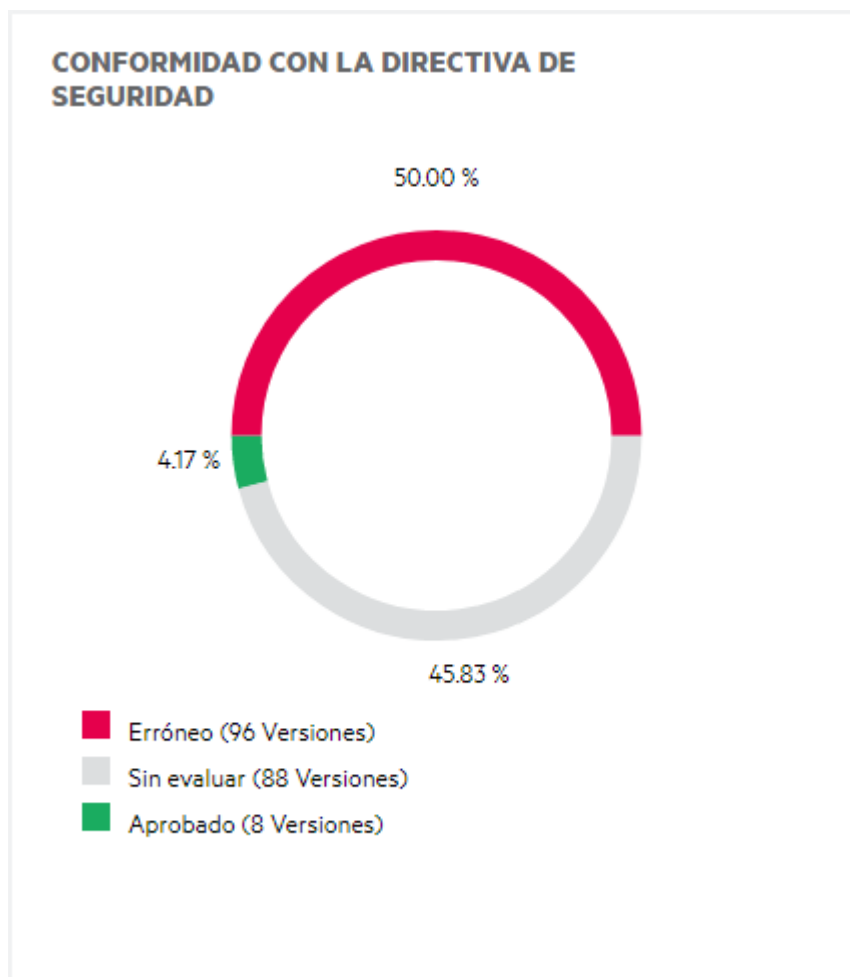
Estos son los tipos de secciones disponibles en un panel:

- Medidor
- Cuadrícula de lista
- Resumen
- Gráfico de tendencias

Medidor

La sección **Medidor** es un gráfico de medidor que resume uno de los siguientes elementos de datos: versiones evaluadas, estado del auditor, estado del desarrollador, uso de derechos, asignación de problemas y conformidad de seguridad.

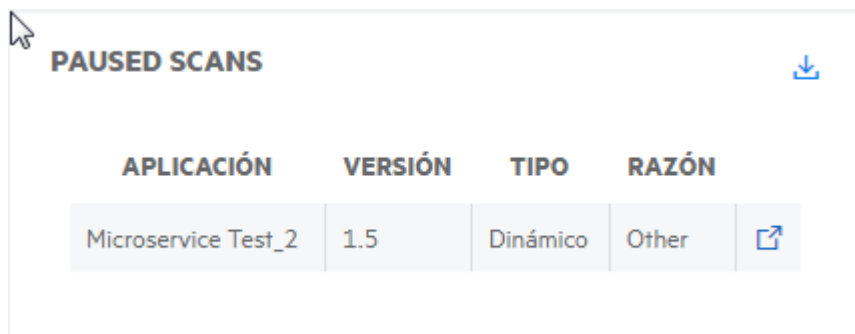
Tipo de elemento de datos	Descripción
Versiones evaluadas	Estado de evaluación de los problemas
Estado del auditor	Estado del auditor de los problemas
Estado del desarrollador	Estado del desarrollador de los problemas
Uso de derechos	Uso de derechos activos
Asignación de problemas	Estado de asignación de los problemas
Conformidad de seguridad	Estado de cumplimiento de directivas de las versiones



Cuadrícula de lista

La sección **Cuadrícula de lista** es una vista en forma de lista o cuadrícula de uno de los siguientes elementos de datos: derechos activos, análisis cancelados, análisis completados, análisis en curso, problemas más importantes, mis problemas, análisis detenidos y análisis programados. Para los análisis, la Cuadrícula de lista también contiene vínculos a la página Configuración del análisis relevante o a la página Análisis.

Tipo de elemento de datos	Descripción
Derechos activos	Derechos activos
Análisis cancelados	Análisis que se cancelaron
Análisis completados	Análisis que se completaron
Análisis en curso	Análisis en curso actualmente
Problemas más importantes	Los problemas más importantes en todas las aplicaciones
Mis problemas	Problemas asignados a la cuenta de usuario actual
Análisis detenidos	Análisis detenidos por el equipo de prueba
Análisis programados	Análisis que se han programado



PAUSED SCANS				
APLICACIÓN	VERSIÓN	TIPO	RAZÓN	
Microservice Test_2	1.5	Dinámico	Other	

Resumen

La sección **Resumen** es un resumen breve del riesgo de seguridad de sus versiones. Muestra el número total de aplicaciones en el portfolio y la siguiente información sobre las versiones de desarrollo, control de calidad y versiones de producción: conformidad con las directivas de seguridad y problemas pendientes (problemas que no tienen soluciones validadas o que no se han suprimido).

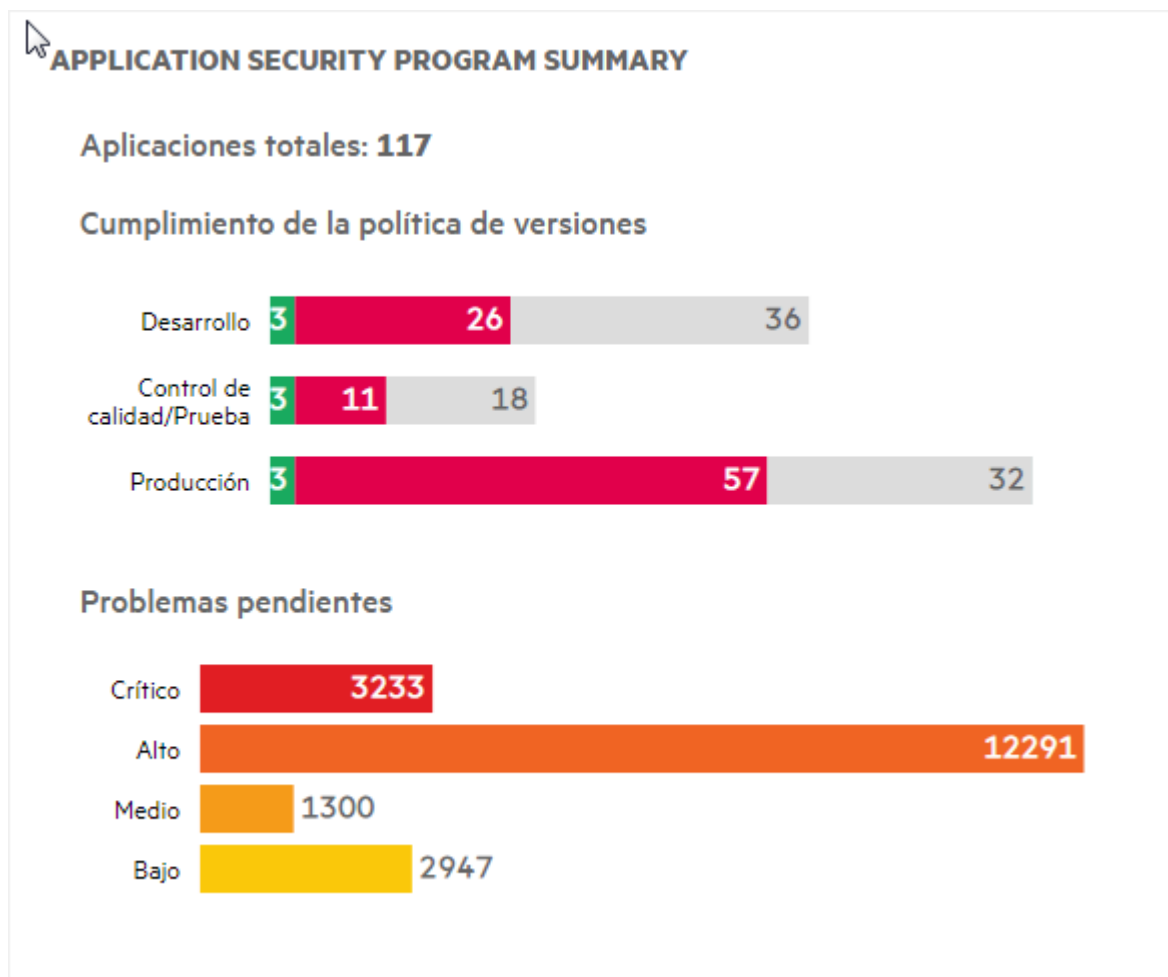
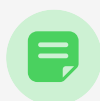


Gráfico de tendencias

La sección **Gráfico de tendencias** es un gráfico de líneas de uno de los siguientes elementos de datos a lo largo del tiempo: aplicaciones, derechos, problemas, versiones y análisis. La serie de datos está agrupada por un atributo especificado.

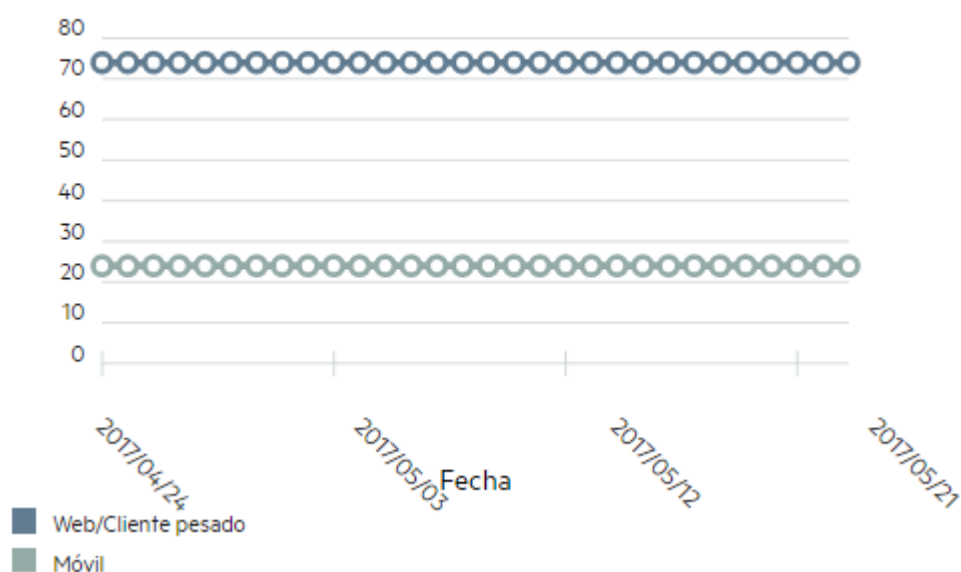


Note

Los puntos de datos de los elementos se miden por adición, exceptuando los análisis.

Tipo de elemento de datos	Descripción
Aplicaciones	Número de aplicaciones agrupadas por un atributo de aplicación
Derechos	Número de unidades de derechos agrupadas por unidades compradas, consumidas o disponibles
Problemas	Número de problemas agrupados por un atributo de problema
Versiones	Número de versiones agrupadas por un atributo de aplicación o versión
Análisis	Número de análisis agrupados por estado del análisis

APLICACIONES POR TIPO DE APLICACIÓN



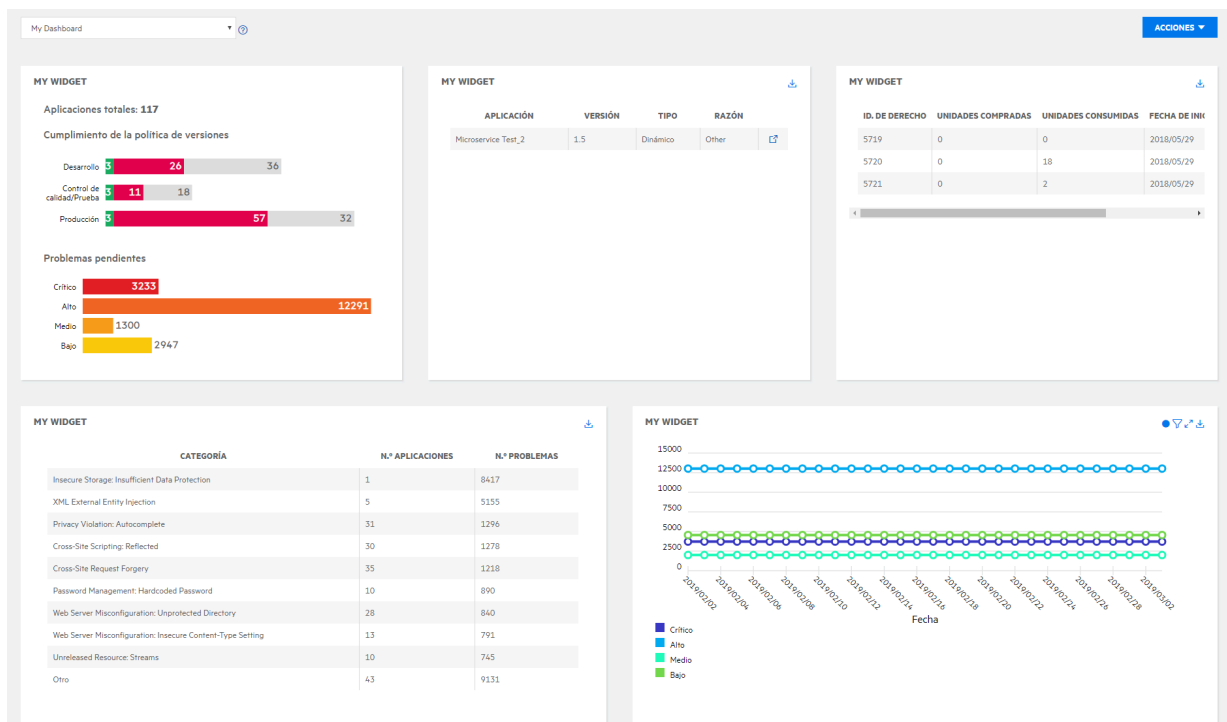
1.7.2.3. Creación de un panel

Puede crear paneles adicionales para organizar las distintas facetas de los datos. Puede tener hasta 10 paneles.

Para crear un panel:

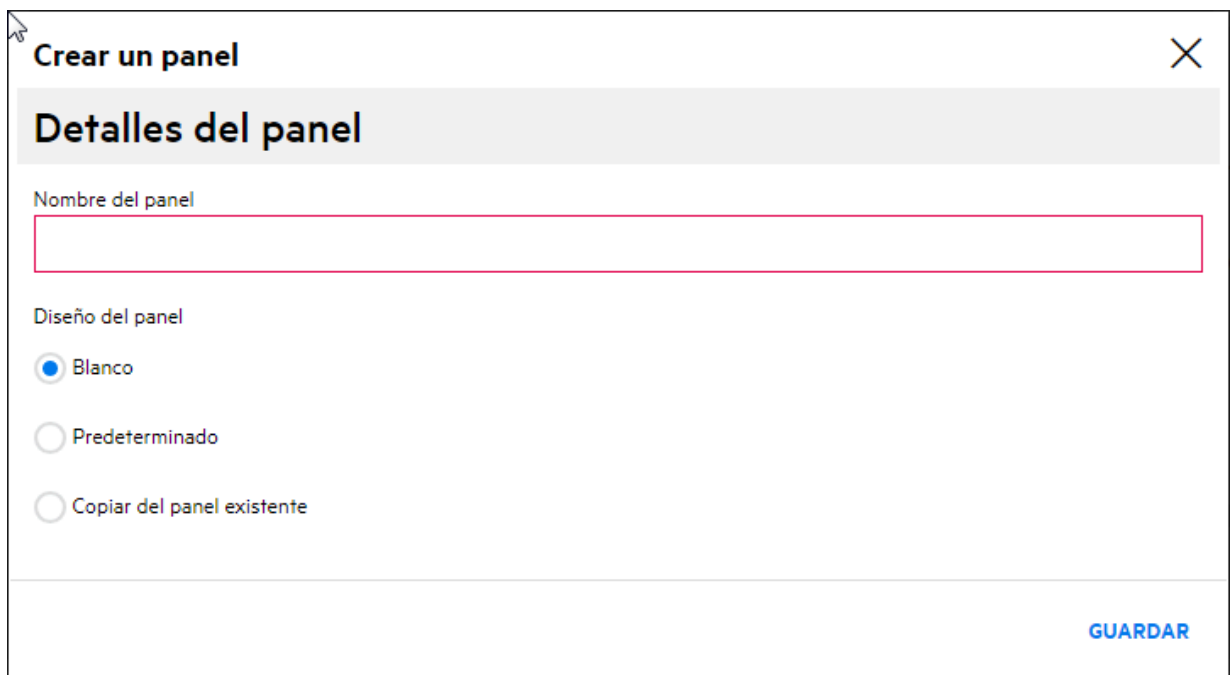
1. Seleccione la vista **Panel**.

Aparece la página del panel. Muestra el último panel que se cargó.



2. Seleccione **Acciones > Nuevo panel**.

Se abrirá la ventana Crear un panel.



Crear un panel

Detalles del panel

Nombre del panel

Diseño del panel

☒ Blanco

☐ Predeterminado

☐ Copiar del panel existente

GUARDAR

3. En el campo **Nombre de panel**, escriba un nombre para el nuevo panel.
 4. Seleccione el diseño inicial del nuevo panel:
 - **En blanco:** empiece con un panel vacío
 - **Predeterminado:** use la configuración de panel predeterminada para su rol de usuario.
 - **Copiar de un panel existente:** copie el diseño de un panel existente.
 5. Haga clic en **Guardar**.
- Aparecerá el nuevo panel.

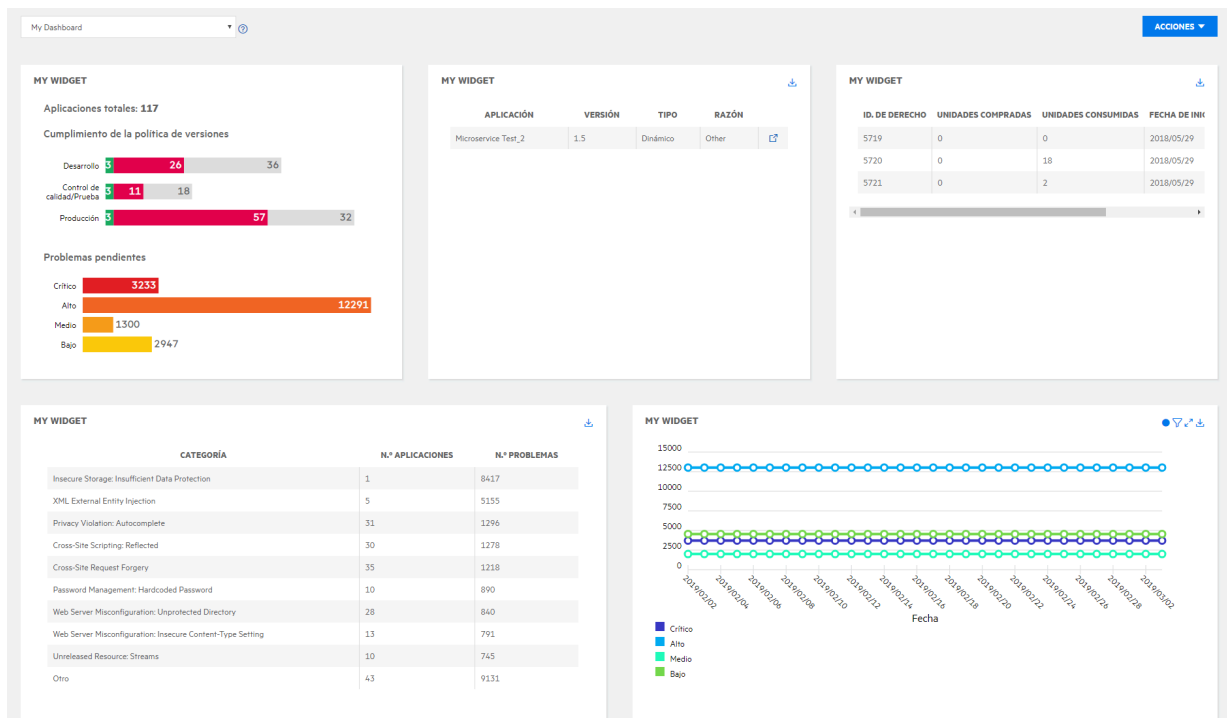
1.7.2.4. Edición de un panel

Puede editar un panel agregando, editando, reorganizando y eliminando filas y secciones. Un panel puede tener hasta diez secciones con un máximo de tres secciones por fila.

Para editar un panel:

1. Seleccione la vista **Panel**.

Aparece la página del panel. Muestra el último panel que se cargó.



2. En la lista desplegable, seleccione el panel que desee editar.

3. Seleccione **Acciones > Editar panel**.

El panel se actualiza en el modo de edición.

?
RESTABLECER VALORES PREDETERMINADOS
GUARDAR
CANCELAR
✕ ELIMINAR

✕

Nombre de mosaico

Tipo de mosaico

Resumen

Tipo

Portfolio

✕

Nombre de mosaico

Tipo de mosaico

Cuadrícula de lista

Tipo

Análisis detenidos

✕

Nombre de mosaico

Tipo de mosaico

Cuadrícula de lista

Tipo

Derechos activos

AGREGAR FILA

4. Realice una o varias de las siguientes tareas para editar el panel:

Tarea	Procedimiento
Agregar una sección	- Realice una de las siguientes acciones: - Haga clic en + en una fila para agregar una sección (si corresponde). - Haga clic en Agregar fila para agregar una sección en una nueva fila (si corresponde).  Note Cada fila puede contener hasta un máximo de tres secciones. - En el campo Nombre de sección, escriba un nombre para la sección. - Seleccione el tipo de sección en la lista Tipo de sección. Para obtener la descripción de los tipos de sección, consulte Tipos de gráfico del panel personalizado. - Realice la acción correspondiente en función del tipo de sección que haya seleccionado. - Si ha seleccionado Indicador, seleccione el elemento de datos que se representará en la lista Tipo.

Tarea	Procedimiento
	■ Si ha seleccionado Cuadrícula de lista, seleccione el elemento de datos que se representará en la lista Tipo. ■ Si ha seleccionado Resumen, seleccione el elemento de datos que se representará en la lista Tipo. El valor disponible actual es Portfolio. ■ Si ha seleccionado Gráfico de tendencias, seleccione el elemento de datos que se representará en la lista Tipo de datos, seleccione el periodo de tiempo del gráfico en la lista Resolución y, por último, seleccione los atributos según los cuales se agruparán los datos en las listas Agrupar por. 5. Si corresponde, haga clic en  y seleccione los valores de filtro que desea aplicar. Los filtros disponibles varían según el tipo de elemento de datos seleccionado.
Editar una sección	Seleccione una sección existente para editarla y actualizar los campos según corresponda.

Tarea	Procedimiento
Mover una fila o una sección	Haga clic en  y arrastre la fila o la sección a la ubicación deseada.  Note Puede mover una sección dentro de una misma fila, pero no puede moverla a una fila diferente.
Eliminar una fila o una sección	Haga clic en  que aparecer junto a la fila o la sección.
Restablecer los valores predeterminados del panel	Haga clic en Restablecer a los valores predeterminados.
Volver al modo de visualización sin guardar los cambios	Haga clic en Cancelar.

5. Haga clic en **Guardar.**

El panel se actualizará con los cambios realizados.

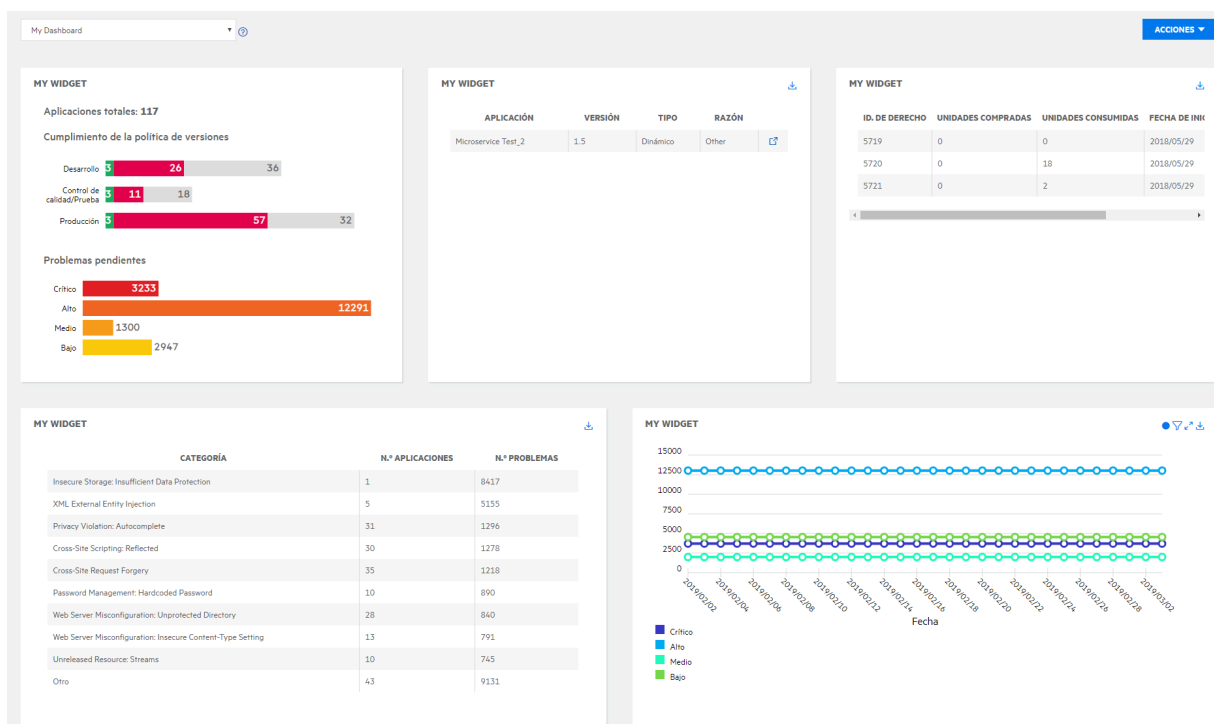
1.7.2.5. Eliminación de un panel

Para eliminar un panel, debe tener al menos otro panel. Si desea eliminar su único panel, primero deberá crear otro.

Para eliminar un panel:

1. Seleccione la vista **Panel**.

Aparece la página del panel. Muestra el último panel que se cargó.



2. En la lista desplegable, seleccione el panel que desee eliminar.

Se cargará el panel seleccionado.

3. Seleccione **Acciones > Editar panel**.

El panel se actualiza en el modo de edición.

?
RESTABLECER VALORES PREDETERMINADOS
GUARDAR
CANCELAR
✖ ELIMINAR

✖

Nombre de mosaico

Tipo de mosaico

Resumen

Tipo

Portfolio

✖

Nombre de mosaico

Tipo de mosaico

Cuadrícula de lista

Tipo

Análisis detenidos

✖

Nombre de mosaico

Tipo de mosaico

Cuadrícula de lista

Tipo

Derechos activos

AGREGAR FILA

4. Haga clic en **Eliminar**.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí**.

El panel se eliminará.

1.7.3. Informes

OpenText Core Application Security ofrece la capacidad de generar informes detallados de los resultados de evaluaciones. Se pueden generar los siguientes tipos de informes:

- Informes predefinidos del sistema
- Informes personalizados
- Exportaciones de datos de aplicaciones, versiones, análisis, problemas o uso de derechos
- Informes de proveedores si utiliza la característica Administración de proveedores



Note

Los informes de componentes de código abierto están disponibles a través de la funcionalidad de informes de OpenText Core Application Security. Puede utilizar la plantilla del sistema Componente de código abierto para generar un informe. La plantilla incluye los siguientes módulos:

- Lista de materiales de código abierto: la lista completa de los componentes detectados en la aplicación.
- Componentes de código abierto vulnerables: la lista de componentes con problemas de seguridad conocidos.

Esta sección contiene los siguientes temas:

- [Visualización de informes](#)
- [Generación de un informe](#)
- [Programación de informes generados automáticamente](#)
- [Plantillas](#)
- [Exportaciones de datos](#)

1.7.3.1. Visualización de informes

Existen dos maneras de acceder a los informes en el portal. Una es a través de la vista Informes, donde puede ver todos los informes generados para todas las aplicaciones y versiones en su inquilino. La otra es mediante la vista **Aplicaciones**, donde puede obtener detalles adicionales de cada aplicación y ver informes relativos a una aplicación o versión determinada.

Esta sección contiene los siguientes temas:

- [Visualización de todos los informes](#)
- [Filtrado de la página Sus informes](#)
- [Visualización de los informes de la aplicación](#)
- [Visualización de informes de la versión](#)

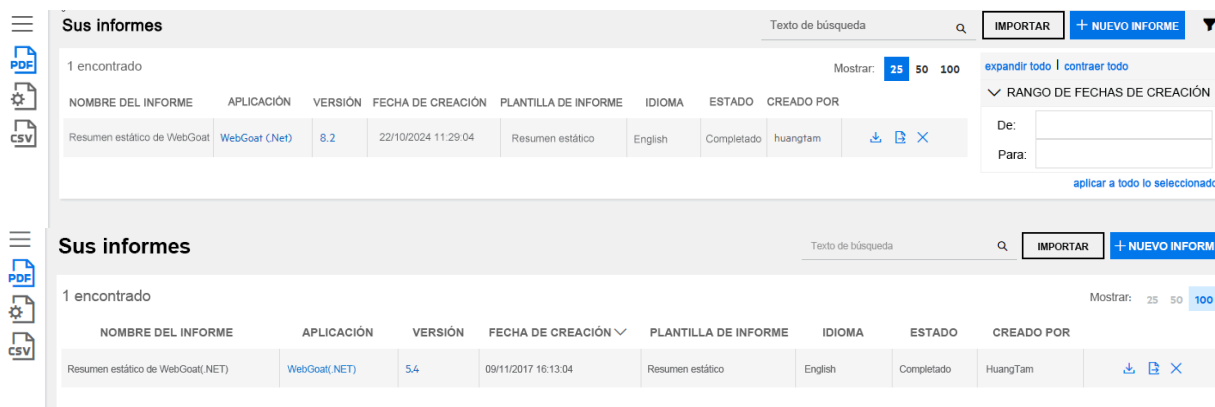
1.7.3.1.1. Visualización de todos los informes

La página Sus Informes es la página de destino predeterminada de la vista Informe, donde puede ver informes para todas sus aplicaciones a nivel de inquilino.

Para ver informes a nivel de inquilino:

1. Seleccione la vista Informes.

Aparecerá la página Sus informes. La página muestra la aplicación y la versión para la que es el informe, la fecha y la hora de creación del informe, el tipo de informe, el estado de generación del informe y el usuario que generó el informe.



The screenshot shows the 'Sus informes' (My Reports) page. It features a sidebar on the left with icons for PDF, CSV, and a settings gear. The main content area has a header with 'Sus informes', a search bar, and buttons for 'IMPORTAR' and '+ NUEVO INFORME'. Below the header, it shows '1 encontrado' (1 found) and a table of reports. The table has columns: NOMBRE DEL INFORME, APLICACIÓN, VERSIÓN, FECHA DE CREACIÓN, PLANTILLA DE INFORME, IDIOMA, ESTADO, and CREADO POR. The first row shows a report for 'WebGoat (Net)' version 8.2, created on 22/10/2024 at 11:29:04, with the status 'Completado' and created by 'huangtam'. To the right of the table, there are filters for 'RANGO DE FECHAS DE CREACIÓN' with 'De:' and 'Para:' fields, and a button 'aplicar a todo lo seleccionado'. The bottom of the page shows a second instance of the same page, but with a different report entry: 'Resumen estático de WebGoat (NET)' version 5.4, created on 09/11/2017 at 16:13:04, with the status 'Completado' and created by 'HuangTam'.

NOMBRE DEL INFORME	APLICACIÓN	VERSIÓN	FECHA DE CREACIÓN	PLANTILLA DE INFORME	IDIOMA	ESTADO	CREADO POR
Resumen estático de WebGoat	WebGoat (Net)	8.2	22/10/2024 11:29:04	Resumen estático	English	Completado	huangtam

NOMBRE DEL INFORME	APLICACIÓN	VERSIÓN	FECHA DE CREACIÓN	PLANTILLA DE INFORME	IDIOMA	ESTADO	CREADO POR
Resumen estático de WebGoat (NET)	WebGoat (NET)	5.4	09/11/2017 16:13:04	Resumen estático	English	Completado	HuangTam

En la siguiente tabla, se describe cómo desplazarse por la página Sus informes.

Tarea	Acción
Buscar en la lista de informes	Escriba una palabra clave o una frase en el campo Texto de búsqueda y pulse Intro. Para quitar los resultados de búsqueda, haga clic en la X. Para obtener más información sobre cómo usar el cuadro Texto de búsqueda, consulte Acerca de la búsqueda de aplicaciones.
Importar un informe personalizado	Haga clic en Importar .
Crear un informe	Haga clic en +Nuevo informe .
Mostrar u ocultar listas de filtros	Haga clic en  .
Expandir o contraer filtros	Haga clic en expandir todo o contraer todo en la flecha junto al nombre del filtro.
Aplicar filtros	Seleccione los valores de filtro deseados debajo del nombre del filtro. La página se actualizará automáticamente con los resultados filtrados. Para algunos filtros, haga clic en aplicar para actualizar la página. Para obtener más información sobre los valores de filtro, consulte Filtrado de la página Sus informes.
Quitar los filtros aplicados	Haga clic en la X que se encuentra junto a cada filtro que se haya aplicado o haga clic en Borrar filtros .

Tarea	Acción
Descargar un informe	Haga clic en  . El informe se descarga en la carpeta local especificada en la configuración del navegador.
Eliminar un informe	Haga clic en  .
Compartir un informe con un inquilino	Haga clic en . Compartir un informe está disponible si ha establecido una relación con otro inquilino. Consulte Administración de proveedores.  Note Compartir un informe que contiene varias versiones no está disponible actualmente.

1.7.3.1.2. Filtrado de la página Sus informes

De forma predeterminada, la página Sus informes muestra todos los informes creados en los últimos 7 días. Puede aplicar filtros para limitar los informes que se muestran. Los siguientes filtros están disponibles en la página Sus informes:



Note

Un filtro aparece en la lista de filtros solamente cuando los resultados contienen varios valores para ese filtro.

Filtro	Descripción	Valores
Aplicación	Aplicación del informe	Definido por el usuario
Rango de fechas de creación	Fecha de generación del informe.	
Creado por	Usuario que generó el informe	Definido por el usuario
Versión	Versión	
Plantilla de informe	Tipo de plantilla de informe	Definido por el sistema, definido por el usuario
Estado	Estado de creación del informe	En cola, Iniciado, Completado

1.7.3.1.3. Visualización de los informes de la aplicación

Puede ver informes para una aplicación seleccionada.

Para ver los informes de una aplicación:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación cuyos informes desee ver.

Aparecerá la página Información general de la aplicación.

WebGoat (.NET)

Cumplimiento de directivas
★☆☆☆☆ FALLIDO VER

Problemas en producción

CRÍTICO	ALTO	MEDIO	BAJO
135	151	11	74

Versiones

1 encontrados

SELECCIONAR TODO

INICIAR ANÁLISIS	VERSIÓN	COPIAR ESTADO DE VERSIÓN DE ORIGEN	ESTADO DE SDLC	CUMPLIMIENTO DE DIRECTIVAS	N.º PROBLEMAS	ESTÁTICO	CÓDIGO ABIERTO	DINÁMICO
☐ INICIAR ANÁLISIS >	5.4		Producción	★☆☆☆☆ FALLIDO	CRÍTICO 135 ALTO 151 MEDIO 11 BAJO 74	✓	⊖	⊗

3. Haga clic en Informes.

La página Informes, en la que se muestran todos los informes de la aplicación.

17.4 Application

Informes

Texto de búsqueda

PROGRAMAR INFORME AUTOMÁTICO + NUEVO INFORME

2 encontrados

Mostrar: 25 50 100

NOMBRE DE INFORME	APLICACIÓN	VERSIÓN	FECHA DE CREACIÓN	PLANTILLA DE INFORME	IDIOMA	ESTADO	CREADO POR
Sonatype 17.4 Application-2 (14619)	17.4 Application	2	2017/10/19 07:24:23	Open Source by Sonatype	English	Completado	kristine_tam
TestReport_2	17.4 Application	3	2017/10/27 09:36:21	Resumen estático	English	Completado	kristine_tam

4. Seleccione un informe de la lista.

1.7.3.1.4. Visualización de informes de la versión

Puede obtener más información de una aplicación y ver los informes únicamente de una versión seleccionada.

Para ver los informes de una versión:

1. Seleccione la vista **Aplicaciones**.

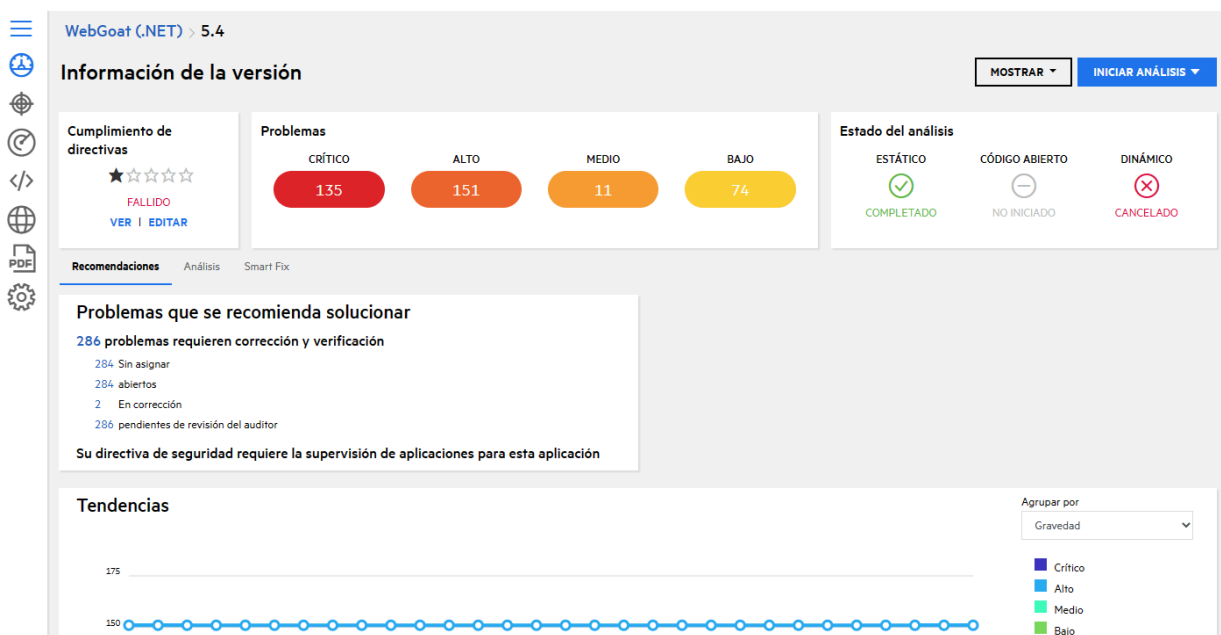
Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

3. Haga clic en el nombre de la versión para la que desee ver informes.

Aparecerá la página Información general de versión.



4. Haga clic en Informes.

Aparecerá la página Informes, en la que se muestran todos los informes de la versión.

Dynamic Beta > 1.0

Informes

Texto de búsqueda

IMPORTAR INFORME

+ NUEVO INFORME

3 encontrados

Mostrar: 25 50 100

NOMBRE DE INFORME	APLICACIÓN	VERSIÓN	FECHA DE CREACIÓN	PLANTILLA DE INFORME	IDIOMA	ESTADO	CREADO POR	
1.0_20160428_1117	Dynamic Beta	1.0	2016/04/28 11:17:26	Resumen dinámico	English	Completado	karellano	
1.0_20170728_0949	Dynamic Beta	1.0	2017/07/28 09:49:59	Resumen híbrido	English	Fallido	ka_sectead2	
RequestResponse	Dynamic Beta	1.0	2017/08/03 09:16:34	Solicitud/respuesta dinámica	English	Completado	kristine_tam	

5. Seleccione un informe de la lista.

1.7.3.2. Generación de un informe

Use una plantilla de informe predefinida o personalizada para generar el informe de una versión. Los informes están disponibles en formato PDF y HTML. En caso de que se produzca un error al generar un informe en formato PDF, se proporcionará automáticamente la versión HTML de este para su comodidad.

Para evitar fallos al generar informes PDF muy grandes, no se pueden generar informes PDF que incluyan los módulos de plantilla **Seguimiento del analista**, **Solicitud/Respuesta** o **Detalles de los problemas** y que contengan más de 5000 problemas. En su lugar, genere informes HTML o use otra plantilla de informe que no incluya estos módulos o que tenga filtros adicionales para reducir la cantidad de problemas.



Note

Para generar informes en un idioma concreto, debe especificarlo en la configuración de su cuenta. Para obtener más información, consulte [Edición de la información de Mi cuenta](#).

Para generar un informe:



Note

Las siguientes instrucciones describen cómo generar informes en la página **Sus informes**. También puede generar informes en las páginas **Informes de aplicación** e **Informes de versión**.

1. Seleccione la vista **Informes**.

Aparecerá la página **Sus informes**.

2. Haga clic en **+Nuevo informe**.

Aparece el asistente para crear informes.

3. **Seleccionar aplicación:** seleccione la aplicación y haga clic en **Siguiente**.

Crear informe



Seleccionar aplicación

Seleccionar versiones

Detalles del informe

Plantilla de informe

Resumen

22 encontrados

Texto de búsqueda



Mostrar: 25 **50** 100

APLICACIÓN ^

☐	API SBOM Import
☐	API Type Scan
☐	Application 1
☐	Audit Improvements Demo
☐	Dast
☐	DAST API
☐	Debricked Scan
☐	DemoMultiSelectCheckbox
☐	Dependency tree view
☐	Dynamic

ATRÁS

SIGUIENTE

GENERAR

- Seleccionar versiones:** seleccione las versiones y haga clic en **Siguiente**. Si selecciona varias versiones, se generará un informe para cada versión y los informes se empaquetarán en un archivo zip.

Crear informe



✓ Seleccionar aplicación

Seleccionar versiones

Detalles del informe

Plantilla de informe

Resumen

Texto de búsqueda



2 encontrados

Mostrar: 25 **50** 100

[SELECCIONAR TODO](#)

VERSIONES ▾

☐

3.1

☐

3.2

ATRÁS

SIGUIENTE

GENERAR

5. **Detalles del informe:** complete los campos y haga clic en **Siguiente**. Los campos son obligatorios a menos que se indique lo contrario.

Crear informe



✓ Seleccionar aplicación

✓ Seleccionar versiones

Detalles del informe

Plantilla de informe

Resumen

Nombre de informe

Notas

Tipo de archivo

ATRÁS

SIGUIENTE

GENERAR

Campo	Descripción
Nombre del informe	Proporcione el nombre del informe.
Notas	Proporcione notas para el informe.
Tipo de archivo	Seleccione el tipo de archivo del informe: PDF , HTML .

6. **Plantilla de informe:** seleccione un tipo de plantilla de informe y haga clic en **Siguiente**.

- Las plantillas de informes del sistema aparecen en azul; las plantillas de informes personalizados aparecen en negro.
- Si su versión solo contiene datos de problemas estáticos, solo estarán disponibles las plantillas de informes estáticos.
- Si su versión solo contiene datos de problemas dinámicos, solo estarán disponibles las plantillas de informes dinámicos.

Crear informe

- ✓ Seleccionar aplicación
- ✓ Seleccionar versiones
- ✓ Detalles del informe
- Plantilla de informe**
- Resumen

Plantilla de informe

ASVS 4.0

Conformidad con CWE Top 25 2023
Conformidad con CWE Top 25 2024
Integral dinámico
Detalles del problema dinámico
Solicitud/respuesta dinámica
Resumen dinámico
Integral híbrido
Detalles del problema híbrido
Resumen híbrido
Conformidad con NIST SP 800-53 Rev.5
Conformidad con la PCI 3.1 DSS
Conformidad con la PCI 3.2 DSS
Conformidad con la PCI 4.0 DSS
Conformidad con la PCI 4.0.1 DSS
Conformidad con la PCI SSF 1.2 DSS
Conformidad con STIG 6.1
Conformidad con STIG 6.2
Conformidad con STIG 6.3
Seguimiento de análisis estático
Integral estático
Detalles del problema estático

Atrás

Siguiente

Generar

7. **Resumen:** revise el resumen del informe y haga clic en **Generar**.

Crear informe



✓ Seleccionar aplicación

✓ Seleccionar versiones

✓ Detalles del informe

✓ Plantilla de informe

Resumen

Nombre de informe

Jeopardy Static Summary

Notas

Tipo de archivo

PDF

Aplicación

Jeopardy (PHP)

Versiones

3.2

Plantilla de informe

Resumen estático

ATRÁS

SIGUIENTE

GENERAR

Se le redirigirá a la página de Informes El informe está disponible una vez que aparece el estado "Completado".



Note

Puede hacer clic en para eliminar un informe mientras aún se está generando.

8. Haga clic en en la fila del informe una vez que se haya generado.
9. Un archivo PDF o zip (según el tipo de archivo) se guarda en la carpeta especificada en la configuración de su navegador.

1.7.3.3. Programación de informes generados automáticamente

Si tiene pensado ejecutar varias evaluaciones en una misma aplicación y desea generar los mismos informes cada vez, puede ahorrar tiempo con la función de informes generados automáticamente.

Para programar un informe generado automáticamente:

1. Seleccione la vista **Aplicaciones**.

Se mostrará la cuadrícula **Sus versiones** con una lista de sus versiones.

Sus versiones									
Texto de búsqueda									
+ Nueva aplicación Exportar									
TODO 10 Producción 10									
10 encontrado									
Mostrar: 25 50 100									
expandir todo contraer todo									
Seleccionar todo									
	Iniciar análisis	Aplicación	Versión	Copiar estado de versión de origen	N.º problemas				Estático
					Crítico	Alto	Medio	Bajo	
☐	Iniciar análisis >	Bricks	2.2		42	14	0	2	✓
☐	Iniciar análisis >	CloudGoat (IaC)	2.0		7	6	4	2	✓
☐	Iniciar análisis >	Fortify-IWA (.Net)	1.0		51	59	138	180	✓
☐	Iniciar análisis >	AndroGoat	21/04/2019		0	11	8	5	✓
☐	Iniciar análisis >	Fortify-IWA (.Java)	1.0		57	88	38	67	✓
☐	Iniciar análisis >	Go-Test-Bench	1.0		28	129	42	3	✓
☐	Iniciar análisis >	Juice Shop	30/06/2021		181	24	14	23	✓
☐	Iniciar análisis >	WebGoat (.Net)	8.2		5	36	0	5	✓

☐ Móvil (2)
☐ Web/Cliente pesado (8)

> Estado de análisis dinámico
 > Estado del análisis móvil
 > Aplicación de muestra
 > Tipo de análisis
 > Clasificación por estrellas
 > Fecha de creación de la aplicación

[aplicar a todo lo seleccionado](#)

2. Haga clic en el nombre de la aplicación para la que desea programar informes generados automáticamente.

3. Haga clic en Informes.

Aparecerá la página Informes.

4. Haga clic en **Programar informe automático**.

Aparecerá la ventana modal Programar un informe generado automáticamente.

Programar un informe generado automáticamente



Seleccione la plantilla de informe que se programará para generar automáticamente un informe cuando finalice el análisis estático de la aplicación.

(Informe no programado) ▼

Seleccione la plantilla de informe que se programará para generar automáticamente un informe cuando finalice el análisis dinámico de la aplicación.

(Informe no programado) ▼

Estado de SDLC

☐ Desarrollo ☐ Control de calidad/Prueba ☐ Producción

Tipo de archivo:

PDF ▼

☐ Enviar informe por correo electrónico tras su finalización

Lista de notificaciones

Escribir direcciones de correo electrónico separadas por punto y coma

GUARDAR

CANCELAR

5. Seleccione la plantilla de informe que se usará para generar un informe cuando se complete un análisis estático.
6. Seleccione la plantilla de informe que se usará para generar un informe cuando se complete un análisis dinámico o móvil.
7. Seleccione las casillas de verificación del estado de SDLC que activarán la generación del informe.
8. Seleccione el tipo de archivo de informe en la lista **Tipo de archivo**.
9. Para distribuir automáticamente los informes entre los destinatarios especificados, seleccione **Enviar informe por correo electrónico tras su**

finalización y, en el campo **Lista de notificaciones**, escriba las direcciones de correo electrónico que recibirán los informes.

10. Haga clic en **Guardar**.

Se guardarán los ajustes del informe generado automáticamente.

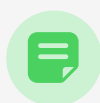
1.7.3.4. Plantillas

Los usuarios con el permiso Crear informe pueden ver, crear, editar y eliminar plantillas.

En la página Plantillas se muestra una lista de plantillas de informe existentes, con vínculos para ver, copiar o editar, y eliminar plantillas. Existen dos tipos de plantillas de informe: las del sistema y las personalizadas.

Hay plantillas de informe del sistema para informes dinámicos, híbridos y móviles, además de para informes de conformidad con PCI, STIG y FISMA. Las plantillas del sistema se pueden copiar y suprimir, pero no se pueden editar ni eliminar.

OpenText Core Application Security proporciona un **Asistente de plantilla** para crear plantillas de informe personalizadas. Puede configurar los filtros y módulos de informes para incluirlos en la plantilla y utilizarla para generar informes con la información más útil para su organización. Las plantillas de informe personalizadas se pueden editar y eliminar.



Note

Caso de uso: si su informe está destinado a una revisión de administración de alto nivel y los usuarios que lo leen no desean ver los detalles de su evaluación de seguridad, puede seleccionar la plantilla **Resumen estático**. Incluye: una página de título, un resumen ejecutivo, un desglose de problemas, una lista de problemas por tipo de análisis y el Top 10 de OWASP. No incluye informes de PCI, comentarios sobre los detalles de los problemas ni un informe de seguimiento de análisis (a menos que los agregue).

Esta sección aborda los siguientes temas:

- [Creación de una plantilla de informe personalizada](#)
- [Edición de una plantilla de informe personalizada](#)
- [Eliminación de una plantilla de informe personalizado](#)
- [Supresión de una plantilla de informe del sistema](#)

1.7.3.4.1. Creación de una plantilla de informe personalizada

Puede crear una plantilla de informe personalizada si crea una plantilla de informe desde cero o si modifica una plantilla del sistema para ajustarla a sus necesidades.

Para crear una plantilla de informe personalizada:

1. Seleccione la vista Informes.
2. Haga clic en el icono Plantillas.

Aparecerá la página Plantillas.

3. Realice una de las siguientes acciones:

- Haga clic en **+Nueva plantilla** para crear una plantilla desde cero.
- Haga clic en el icono  de la fila de la plantilla del sistema que desee para clonar la plantilla.

Aparecerá el asistente Agregar/Editar plantilla de informe.

4. **Detalles de la plantilla:** en el campo **Nombre de plantilla**, escriba el nombre de la nueva plantilla y haga clic en **Siguiente**.



5. **Filtros:** seleccione los filtros deseados y haga clic en **Siguiente**. Los campos son obligatorios a menos que se indique lo contrario.

✓ Detalles de la plantilla

Filtros

Módulos

Resumen

✕

▼ TIPO DE ANÁLISIS

☐ Estático

☐ Dinámico

☐ Móvil

☐ Código abierto

☐ Red

☐ Supervisión de aplicaciones

▼ GRAVEDAD

☐ Crítico

☐ Alto

☐ Medio

☐ Bajo

☐ Mejor procedimiento

☐ Información

▼ ESTADO DEL PROBLEMA

☐ Nuevo

☐ Existente

☐ Volver a abrir

ATRÁS

SIGUIENTE

GUARDAR

Campo	Descripción
Tipo de análisis	Tipo de análisis
Gravedad	(Opcional) Gravedad de los problemas
Estado del problema	(Opcional) Estado de los problemas (Nuevo, Existente o Reabierto)
Estado del desarrollador	(Opcional) Estado del desarrollador de los problemas
Estado del auditor	(Opcional) Estado del auditor de los problemas
Antigüedad del problema	(Opcional) Días transcurridos desde que se introdujeron los problemas por primera vez
Categoría	(Opcional) Categoría de vulnerabilidad de los problemas
Se ha suprimido	(Opcional) Estado de supresión de problemas (el valor predeterminado es False)
Desafío de falso positivo	(Opcional) Estado del desafío de falso positivo de los problemas

6. **Módulos:** seleccione los módulos del informe que se incluirán en la plantilla y haga clic en **Siguiente**.

- Arrastre los módulos que desee incluir desde la columna **Módulos disponibles** hasta la columna **Diseño del informe**. Los módulos disponibles varían según el tipo de análisis seleccionado.
- Arrastre y suelte elementos en la columna **Diseño de informes** para cambiar el orden de los módulos en el informe generado.

Agregar/Editar plantilla de informe

✓ Detalles de la plantilla

✓ Filtros

Módulos

Resumen

Módulos disponibles

Desglose de problemas de CWE Top 25 2023

Desglose de problemas de CWE Top 25 2024

Página de título de CWE Top 25 2023

Página de título de CWE Top 25 2024

Resumen ejecutivo de DISA STIG 6.1

Resumen ejecutivo de DISA STIG 6.2

Resumen ejecutivo de DISA STIG 6.3

Desglose de problemas de DISA STIG 6.1

Desglose de problemas de DISA STIG 6.2

Desglose de problemas de DISA STIG 6.3

Página de título de DISA STIG 6.1

Página de título de DISA STIG 6.2

Página de título de DISA STIG 6.3

Diseño del informe

arrastrar módulos aquí

Atrás

Siguiente

Guardar

7. **Resumen:** revise el resumen de la plantilla y haga clic en **Guardar**.

This PDF was generated on February 12, 2026

Page 513 of 784

Agregar/Editar plantilla de informe



✓ Detalles de la plantilla ✓ Filtros ✓ Módulos Resumen	Detalles de la plantilla	Filtros
	Nombre de plantilla WebDetails	Tipo de análisis Estático
	Módulos	Gravedad
	Desglose de problemas Desglose de problemas de DISA STIG 4.1 Desglose de problemas de PCI 3.0 Detalle de la supervisión de aplicaciones continua Detalles del problema	Crítico Alto Medio Bajo Se ha suprimido Falso

[ATRÁS](#) [SIGUIENTE](#) [GUARDAR](#)

La plantilla de informe personalizada aparecerá en la lista de plantillas. Si es necesario, realice una búsqueda del nombre para encontrarla.

1.7.3.4.2. Edición de una plantilla de informe personalizada

Puede editar una plantilla de informe personalizada existente con el asistente Agregar/Editar plantilla de informe.

Para editar una plantilla de informe personalizada:

1. Seleccione la vista Informes.

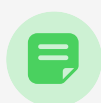
2. Haga clic en Plantillas.

Aparecerá la página Plantillas.

3. Haga clic en el icono  en la fila de la plantilla que desea editar.

Aparecerá el asistente Agregar/Editar plantilla de informe.

4. Edite los campos en cada paso del asistente según sea necesario. Para obtener más información, consulte [Creación de una plantilla de informe personalizado](#).



Note

La eliminación de los módulos obsoletos es permanente y no se puede deshacer después de haber guardado la plantilla.

5. Haga clic en **Guardar**.

Se guardarán los cambios aplicados a la plantilla.

1.7.3.4.3. Eliminación de una plantilla de informe personalizado

Puede eliminar cualquiera de las plantillas de informe personalizadas en el inquilino.

Para eliminar una plantilla de informe personalizada:

1. Seleccione la vista **Informes**.

2. Haga clic en Plantillas.

Aparecerá la página Plantillas.

3. Busque la plantilla personalizada que desee eliminar en la lista de plantillas.

4. Haga clic en el icono  en la fila de la plantilla.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí** para eliminar la plantilla.

1.7.3.4.4. Supresión de una plantilla de informe del sistema

Los líderes en seguridad pueden evitar que los usuarios del portal vean o usen una plantilla de informe del sistema en la creación de informes mediante la supresión de esta plantilla.

1. Seleccione la vista Informes.

2. Haga clic en Plantillas.

Aparecerá la página Plantillas.

3. Haga clic en el icono  junto a la plantilla del sistema que desee suprimir.

Aparecerá un mensaje de confirmación.

4. Haga clic en **Sí** para confirmar la supresión de la plantilla de informe del sistema.

La plantilla de informe del sistema se mostrará como suprimida. Puede hacer clic en el icono  para restaurar la plantilla de informe del sistema para los usuarios del portal.

1.7.3.5. Exportaciones de datos

La exportación de datos es una lista completa de datos relevantes de una categoría específica (aplicaciones, versiones, análisis, problemas o uso de derechos) en el inquilino. Los usuarios con el permiso Exportar datos pueden generar exportaciones de datos. La exportación de datos se proporciona como un archivo CSV.

Esta sección aborda los siguientes temas:

- [Vista de exportaciones de datos](#)
- [Creación de una plantilla de exportación de datos](#)
- [Generación de una exportación de datos](#)

1.7.3.5.1. Vista de exportaciones de datos

Para ver exportaciones de datos:

1. Haga clic en la vista Informes.

Aparecerá la página Sus informes.

2. Haga clic en **Exportación de datos**.

Aparecerá la página Exportación de datos.

PDF

CSV

Exportación de datos

+ NUEVA EXPORTACIÓN DE DATOS

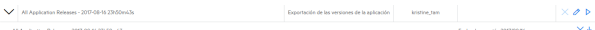
74 encontrados

1 2 → →

Mostrar: 25 50 100

NOMBRE	TIPO	CREADO POR	FECHA DE LA PRÓXIMA EJECUCIÓN	
> All Application Releases - 2015-12-02 14h48m36s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2015-12-03 16h15m01s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2016-01-27 19h11m11s	Exportación de las versiones de la aplicación	ka_seclead2		✕ ↗ ▶
> All Application Releases - 2016-01-28 22h42m48s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2016-05-16 21h27m21s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2016-05-16 21h29m24s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2016-05-17 23h14m40s	Exportación de las versiones de la aplicación	ka_seclead2		✕ ↗ ▶
> All Application Releases - 2016-06-25 01h18m08s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2016-07-23 02h44m56s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2016-10-20 01h38m00s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶
> All Application Releases - 2016-11-03 05h43m43s	Exportación de las versiones de la aplicación	kristine_tam		✕ ↗ ▶

En la siguiente tabla se describe cómo desplazarse por la página Exportación de datos.

Tarea	Acción
Crear una plantilla de exportación de datos	Haga clic en +Nueva exportación de datos . Para obtener más información, consulte Creación de un Plantilla para la exportación de datos .
Generar una exportación de datos mediante una plantilla existente	Haga clic en  en la fila de una plantilla. Para obtener más información, consulte Generación de una exportación de datos .
Editar una plantilla de exportación de datos	Haga clic en  en la fila de una plantilla.
Eliminar una plantilla de exportación de datos	Haga clic en  en la fila de una plantilla. No se puede eliminar una plantilla si contiene una exportación de datos.
Ver las exportaciones de datos generados para una plantilla	Haga clic en  en la fila de una plantilla para ver los archivos que generaron durante los tres últimos meses para la plantilla. 
Eliminar una exportación de datos	Haga clic en  en la fila de una exportación de datos. Si aún se está ejecutando una exportación de datos, se cancelará.
Descargar un archivo de exportación de datos	Haga clic en  en la fila de una exportación de datos.

1.7.3.5.2. Creación de una plantilla de exportación de datos

La plantilla de exportación de datos se usa como base para generar exportaciones de datos. Puede aplicar filtros y programar exportaciones de datos periódicas.

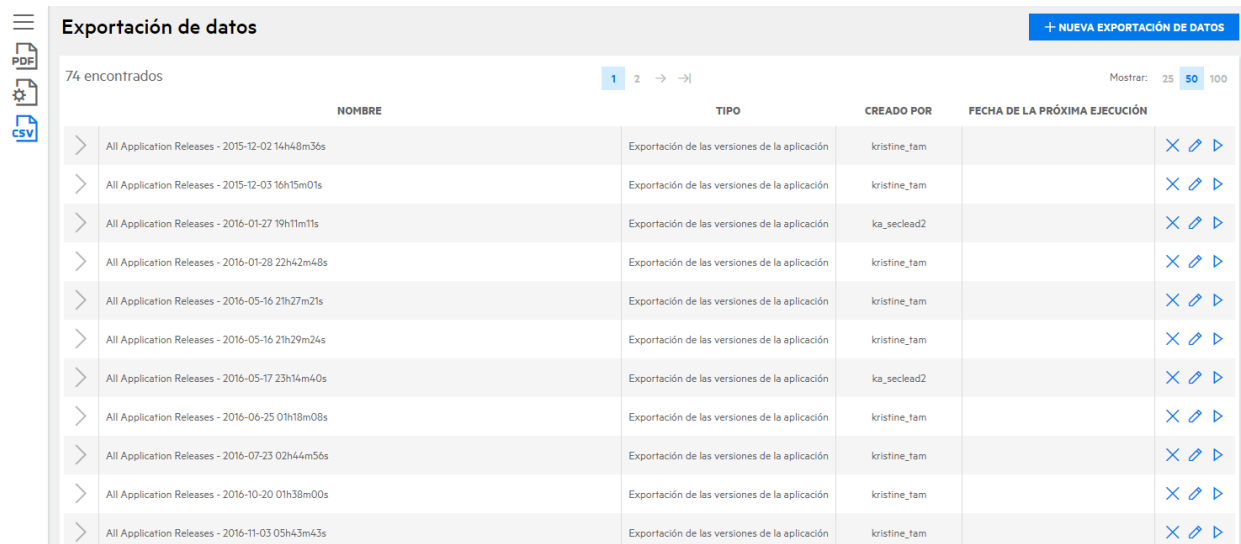
Para crear una plantilla de exportación de datos:

1. Haga clic en la vista Informes.

Aparecerá la página Sus informes.

2. Haga clic en **Exportación de datos**.

Aparecerá la página Exportación de datos.



The screenshot shows the 'Exportación de datos' (Data Export) page. On the left, there are icons for PDF, CSV, and a settings gear. The main area has a header 'Exportación de datos' and a '+ NUEVA EXPORTACIÓN DE DATOS' button. Below the header, it says '74 encontrados' and shows pagination controls (1, 2, →, →|). A 'Mostrar:' dropdown is set to '25' with options for 25, 50, and 100. The table has four columns: 'NOMBRE', 'TIPO', 'CREADO POR', and 'FECHA DE LA PRÓXIMA EJECUCIÓN'. Each row represents a data export template, with a 'NOMBRE' starting with 'All Application Releases -', a 'TIPO' of 'Exportación de las versiones de la aplicación', a 'CREADO POR' of 'kristine_tam' or 'ka_seclead2', and a 'FECHA DE LA PRÓXIMA EJECUCIÓN' column. Each row ends with three icons: a close icon (X), an edit icon (pencil), and a delete icon (trash).

NOMBRE	TIPO	CREADO POR	FECHA DE LA PRÓXIMA EJECUCIÓN
All Application Releases - 2015-12-02 14h48m36s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2015-12-03 16h15m01s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2016-01-27 19h11m11s	Exportación de las versiones de la aplicación	ka_seclead2	
All Application Releases - 2016-01-28 22h42m48s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2016-05-16 21h27m21s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2016-05-16 21h29m24s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2016-05-17 23h14m40s	Exportación de las versiones de la aplicación	ka_seclead2	
All Application Releases - 2016-06-25 01h18m08s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2016-07-23 02h44m56s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2016-10-20 01h38m00s	Exportación de las versiones de la aplicación	kristine_tam	
All Application Releases - 2016-11-03 05h43m43s	Exportación de las versiones de la aplicación	kristine_tam	

3. Haga clic en **+Nueva exportación de datos**.

Aparecerá el Asistente para la exportación de datos.

4. **Página de inicio:** complete los campos y haga clic en **Siguiente**.

Asistente para la exportación de datos

Página de inicio
Filtro
Columnas
Resumen

Nombre

Problemas filtrados: 17/03/2025 15h38m19s

Plantilla

Problemas

Programación

☒ Cola actual
☐ Periódica
☐ Habilitado

Atrás

Siguiente

Guardar

Campo	Descripción
Nombre	Escriba el nombre de la plantilla de exportación de datos.
Plantilla	Seleccione un tipo de plantilla de exportación de datos: ◦ Aplicaciones: lista de aplicaciones ◦ Versiones de la aplicación: lista de versiones. ◦ Análisis: lista de análisis. ◦ Problemas: lista de problemas. ◦ Uso de derechos: lista de análisis en los que se usaron derechos, incluidos los análisis eliminados, cancelados y en curso.

Campo	Descripción
Programación	Seleccione una de las siguientes opciones para programar la exportación de datos: ◦ Cola actual: pone en cola la exportación de datos inmediatamente. ◦ Periódica: genera la exportación de datos según una programación que se configura en el asistente. Cuando se selecciona esta opción, la casilla Habilitado está disponible. Active la casilla para generar la exportación de datos automáticamente según la programación (predeterminada). De lo contrario, deberá generar manualmente la exportación de datos.

5. **Filtro:** seleccione el valor de ámbito y haga clic en **Siguiente**. Los filtros que están disponibles varían según el tipo de plantilla seleccionado.

Asistente para la exportación de datos

✓

Página de inicio

Filtro

Columnas

Resumen

expandir todo | contraer todo

✓

Fecha de introducción

☒

De:

☐

Duración:

Últimos 7 días

▼

Para:

>

Categoría

>

CWE

>

Top 25 de CWE 2023

>

FISMA

>

Con datos adjuntos

>

Se ha suprimido

>

NIST SP 800-53 Rev. 5

>

OWASP 2021

>

OWASP ASVS 4.0

>

PCI 4.0

>

PCI SSF 1.2

Atrás

Siguiente

Guardar

Asistente para la exportación de datos

X

✓ Página de inicio

Filtro

Resumen

expandir todo | contraer todo

▼ Fecha de inicio

☒ De:

 A:

☐ Duración:

Últimos 7 días ▼

Atrás

Siguiente

Guardar



Note

Se requiere el filtro **Fecha de inicio de análisis** para la exportación de los datos de análisis. Se requiere el filtro **Fecha de introducción** para la exportación de los datos de problemas.

La **fecha de inicio** es necesaria para la exportación de datos de uso de los derechos.

6. **Columna** (disponible para las exportaciones de datos de problemas y análisis): seleccione las columnas para incluir en la exportación de datos y haga clic en **Siguiente**.

Asistente para la exportación de datos

✓ Página de inicio
✓ Filtro
Columnas
Resumen

seleccionar todo | anular toda la selección | invertir selección

- ☒ Id. de análisis
- ☒ Aplicación
- ☒ Id. de aplicación
- ☒ Fecha de creación de la aplicación
- ☒ Descripción de aplicación
- ☒ Nombre de microservicios
- ☒ Clasificación por estrellas
- ☒ Versión
- ☒ Id. de versión
- ☒ Fecha de creación de la versión
- ☒ Descripción de la versión
- ☒ Tipo de análisis
- ☒ Recuento de Crítico
- ☒ Recuento de Alto
- ☒ Recuento de Medio
- ☒ Recuento de Bajo
- ☒ IssueCountRD

Atrás Siguiente Guardar

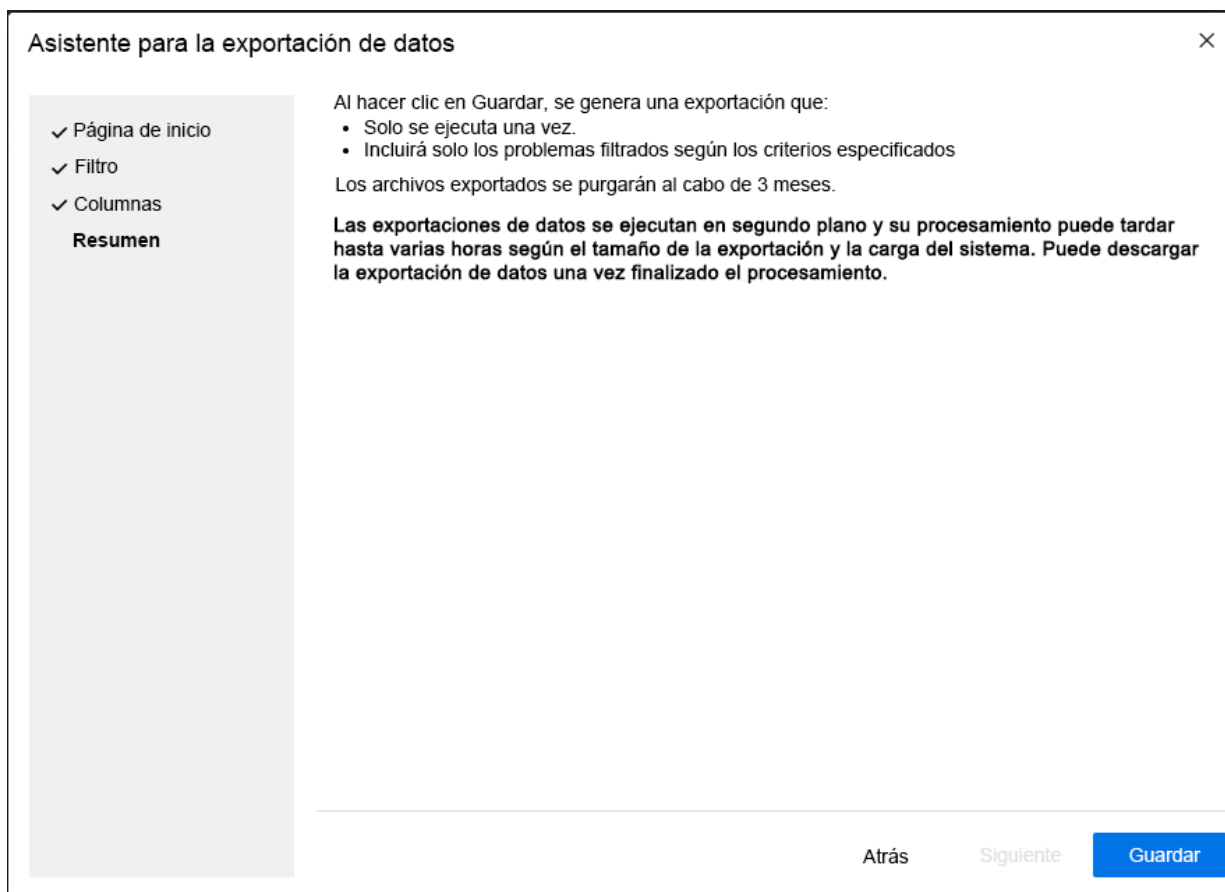
7. **Programación** (disponible para exportaciones de datos periódicas): seleccione la frecuencia de repetición y el día o la fecha en los que se generará la exportación de datos. Haga clic en **Siguiente**.



Note

Las exportaciones de datos se ejecutan a las 24:00 (hora del servidor).

8. **Resumen**: revise el resumen de la exportación de datos y haga clic en **Guardar**.



La plantilla de exportación de datos aparecerá en la lista de exportación de datos.

1.7.3.5.3. Generación de una exportación de datos

Genere una exportación de datos con una plantilla de exportación de datos existente.



Note

Una exportación de datos solo contiene los resultados de las evaluaciones completadas en el momento en el que se genera dicha exportación, a excepción de la exportación de datos del uso de derechos.

Para generar una exportación de datos:

1. Haga clic en la vista Informes.

Aparecerá la página Sus informes.

2. Haga clic en **Exportación de datos**.

Aparecerá la página Exportación de datos.

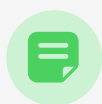
Exportación de datos				+ NUEVA EXPORTACIÓN DE DATOS	
74 encontrados				Mostrar: 25 50 100	
	NOMBRE	TIPO	CREADO POR	FECHA DE LA PRÓXIMA EJECUCIÓN	
>	All Application Releases - 2015-12-02 14h48m36s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2015-12-03 16h15m01s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2016-01-27 19h11m11s	Exportación de las versiones de la aplicación	ka_seclead2		X ↗ ↘
>	All Application Releases - 2016-01-28 22h42m48s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2016-05-16 21h27m21s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2016-05-16 21h29m24s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2016-05-17 23h14m40s	Exportación de las versiones de la aplicación	ka_seclead2		X ↗ ↘
>	All Application Releases - 2016-06-25 01h18m08s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2016-07-23 02h44m56s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2016-10-20 01h38m00s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘
>	All Application Releases - 2016-11-03 05h43m43s	Exportación de las versiones de la aplicación	kristine_tam		X ↗ ↘

3. Haga clic en  en la fila de una plantilla de exportación de datos.

La exportación de datos se pondrá en cola para la generación.

4. Haga clic en  junto a la plantilla para ver las exportaciones de datos generadas.

Aparecerá un estado "Procesando" hasta que la exportación de datos esté disponible.



Note

Puede hacer clic [X](#) para cancelar una exportación de datos de ejecución prolongada.

5. Haga clic en [↓](#) en la fila de la exportación de datos una vez que se haya generado.

El archivo CSV se guarda en la carpeta especificada en la configuración del navegador.

1.8. Administración

La administración del inquilino se realiza desde el portal. El rol del usuario determina el acceso y los privilegios.

Esta sección contiene los siguientes temas:

- [Administración del portal](#)
- [Administración de usuarios](#)
- [Administración de directivas](#)
- [Registro único \(SSO\)](#)
- [Administración de proveedores](#)

1.8.1. Administración del portal

Los líderes en seguridad pueden administrar el portal, lo que incluye establecer la configuración del portal, configurar la seguridad y revisar el registro de eventos de administración.

Esta sección aborda los siguientes temas:

- [Configuración de la seguridad de usuarios](#)
- [Administración de claves de API](#)
- [Administración de atributos](#)
- [Gestión de redes de OpenText Core Application Security Connect](#)
- [Visualización de derechos](#)
- [Visualización del registro de eventos de administración](#)
- [Configuración del estado del auditor de SAST Aviator](#)

1.8.1.1. Configuración de la seguridad de usuarios

Los líderes en seguridad pueden configurar los siguientes ajustes de seguridad de usuarios:

- Frecuencia de restablecimiento de contraseña
- Duración máxima de los tokens de acceso personales
- Autenticación en dos fases
- Restricciones de IP



Note

La función de restricciones de IP está deshabilitada para 24.3

Para configurar los ajustes de seguridad de usuarios:

1. Seleccione la vista **Administración**.

Aparecerá la página Configuración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la página Configuración.

3. Seleccione la pestaña **Seguridad**.

Configuración

Atributos

Seguridad

API

Fortify on Demand Connect

Configurar el estado del auditor de SAST Aviator

Frecuencia de restablecimiento de contraseña (de 1 a 9999 días)

7

Días

Duración máxima de los tokens de acceso personales (de 1 a 9999 días)

180

Días

Autenticación en dos fases

Habilitar autenticación en dos fases

Sí

☐ Correo electrónico

☒ SMS

☒ TOTP

Frecuencia

Cada inicio de sesión

Restricción de IP

Habilitar restricción de inicio de sesión:

No

Permitir el acceso del servicio de soporte técnico desde cualquier dirección IP:

Denegar

Direcciones IP permitidas:

Nombre	Dirección IP
+ Agregar	

Su dirección IP: 129.231.129.56

Los formatos de IPV4 válidos son 127.0.0.1, 127.0.0.* y 127.0.0.[0-255].

Guardar

4. Edite los campos según sea necesario.

Sección	Procedimiento
Frecuencia de caducidad de la contraseña	Para especificar la frecuencia de restablecimiento de las contraseñas nuevas: En el campo Frecuencia de restablecimiento de contraseña, especifique el valor correspondiente. El nuevo valor sobrescribirá el predeterminado de 180 días.
Duración máxima de los tokens de acceso personales	Para especificar la duración máxima de los tokens de acceso personales para nuevos PAT: En el campo Duración máxima de los tokens de acceso personales, especifique el valor correspondiente. El nuevo valor sobrescribirá el predeterminado de 180 días.

Sección	Procedimiento
Autenticación en dos fases	Proteja las cuentas de usuario configurando la autenticación en dos fases. Una vez configurada, todos los usuarios deberán iniciar sesión mediante la autenticación en dos fases. Realice lo siguiente para configurar la autenticación en dos fases: 1. En el campo Habilitar autenticación en dos fases, mueva el control deslizante de No a Sí para habilitar la autenticación en dos fases. 2. Seleccione si los usuarios pueden recibir el código de inicio de sesión por correo electrónico, SMS, TOTP o los tres métodos. Cuando intenta iniciar sesión por primera vez después de que el responsable de seguridad habilite TOTP, aparecerá una nueva página de Core Application Security con un código QR. 3. Seleccione la frecuencia con la que se le pide al usuario un código de autenticación en dos fases en la lista Frecuencia: Cada inicio de sesión, 4 horas, 8 horas, 12 horas o 24 horas.

Sección	Procedimiento
Restricciones de IP	Limite el acceso al inquilino restringiendo el acceso a los usuarios que inician sesión desde direcciones IP determinadas. Para restringir el acceso a direcciones IP concretas: 1. En el campo Habilitar restricción de inicio de sesión, mueva el control deslizante de No a Sí para habilitar la restricción de IP. 2. En el campo Permitir que los administradores de cuentas técnicos (TAMs) accedan desde cualquier dirección IP, mueva el control deslizante de No a Sí para permitir que un TAM pueda acceder al inquilino desde cualquier dirección IP. 3. Realice las siguientes tareas para administrar las direcciones IP que pueden acceder al inquilino:
Tarea	Procedimiento
Agregar una dirección IP a la lista de direcciones permitidas	Haga clic en +Agregar y escriba la dirección IP y un nombre para esta (no se permiten caracteres especiales). Los formatos válidos de las direcciones IP son 127.0.0.1, 127.0.0.* y 127.0.0.[0-255].

Sección	Procedimiento
Eliminar una dirección IP existente de la lista de direcciones permitidas	Haga clic en la x que se encuentra junto a una dirección IP en la lista Direcciones IP permitidas .

5. Haga clic en **Guardar**.

Se guardará la configuración de la seguridad de usuarios.

1.8.1.2. Administración de claves de API

Las claves de API se usan para autenticarse en la OpenText Core Application Security API. Los líderes en seguridad pueden administrar las claves de API.



Note

Esta sección cubre la administración de claves de API. Para obtener información sobre el uso de la API de OpenText Core Application Security, consulte [Interfaz de programación de aplicaciones \(API\)](#).

Esta sección aborda los siguientes temas:

- [Creación de una clave de API](#)
- [Roles de la clave de API](#)
- [Edición o eliminación de una clave de API](#)

1.8.1.2.1. Creación de una clave de API

Los líderes en seguridad pueden crear claves de API.

Para crear una clave de API:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la pestaña **Atributos** de la página Configuración.

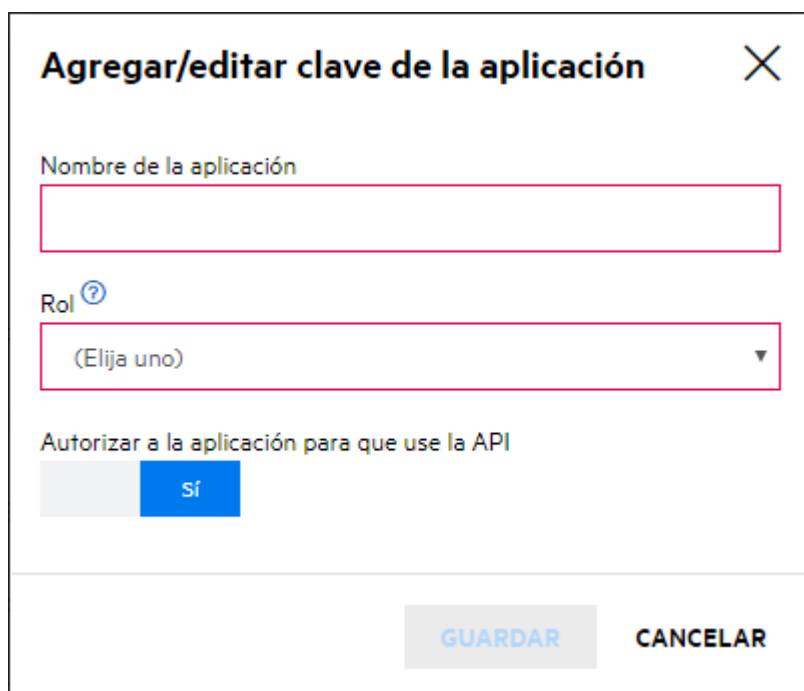
3. Seleccione la pestaña **API**.



NOMBRE	CLAVE DE API	TIPO DE CONCESIÓN	ROL	FECHA DE ÚLTIMO INICIO DE SESIÓN	DIRECCIÓN IP DE ÚLTIMO INICIO DE SESIÓN	AUTORIZADA
ManageApplications	ee2828c6-e1c-4ca6-8ea2-4643bdDeab78	Credenciales de cliente	Administrar aplicaciones	2022/04/14	15.122.108.150	Sí
ReadOnly	c6599566-be40-4612-9804-6ccce1a97b83	Credenciales de cliente	Solo lectura			Sí
ReadOnly for 22.1	95f2661d-3ff-4edf-bfa9-dad49290b823	Credenciales de cliente	Solo lectura	2022/04/07	15.122.101.250	Sí
SecurityLead	ffc06c71-2b45-4f74-a9bf-d76cb8935f7f	Credenciales de cliente	Líder en seguridad			Sí
StartScans	ec527d4a-4737-4e9f-8d26-9b0aa0ae9cc2	Credenciales de cliente	Iniciar análisis			Sí

4. Haga clic en **+Agregar clave**.

Se abrirá la ventana **Agregar/editar clave de la aplicación**.



Agregar/editar clave de la aplicación

Nombre de la aplicación

Rol ?

Autorizar a la aplicación para que use la API

☐ ☒ Sí

GUARDAR CANCELAR

5. Complete los campos. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Nombre de la aplicación	Nombre de la aplicación.
Rol	Seleccione el rol que tenga los permisos de clave de API adecuados. Consulte Roles de la clave de API .
Autorizar a la aplicación para que use la API	Seleccione Sí para habilitar la clave. Seleccione No para deshabilitar la clave si no se está utilizando.

6. Haga clic en **Guardar**.

Se abrirá la ventana Clave secreta.

7. Copie el código secreto con codificación Base64. El código secreto se muestra una sola vez.

8. Haga clic en **Cerrar**.

La nueva clave de API aparece en la lista de claves de API.



Note

De forma predeterminada, una clave de API tiene acceso a todas las aplicaciones. Consulte [Edición o eliminación de una clave de API](#) para obtener información sobre cómo asignar aplicaciones a una clave de API.

1.8.1.2.2. Roles de la clave de API

Una clave de API dedicada se asocia a un rol que tenga un conjunto predefinido de permisos que no se pueda modificar. Las claves de API pueden acceder a todas las aplicaciones de un inquilino; las aplicaciones se pueden asignar a claves de API para actualizar el acceso a la aplicación.

En la siguiente tabla se enumera el conjunto de permisos de cada rol de clave de API.

Rol	Permisos	Ejemplo de uso
Líder en seguridad	Todos los permisos	Acceso total a la funcionalidad y la infraestructura asociada del programa AppSec
Administrar aplicaciones	Ver aplicaciones de terceros, Administrar aplicaciones, Auditar problemas, Crear informes, Iniciar análisis estáticos/dinámicos/móviles	Integración con sistemas personalizados o internos con todas las características sin poder administrar usuarios
Iniciar análisis	Ver aplicaciones de terceros, Ver aplicaciones, Ver problemas, Ver informes, Iniciar análisis estáticos/dinámicos/móviles	Integración continua y servidores de compilación
Solo lectura	Ver aplicaciones de terceros, Ver aplicaciones, Ver problemas, Ver informes	Importación de datos en sistemas de administración de vulnerabilidades o de gobierno, administración de riesgos y cumplimiento (GRC)

1.8.1.2.3. Edición o eliminación de una clave de API

Los líderes en seguridad pueden realizar las siguientes tareas para las claves de API:

- Generar un nuevo secreto
- Editar la configuración de la clave de API
- Asignar y cancelar la asignación de aplicaciones



Note

Las claves de API con el rol de líder en seguridad tienen acceso a todas las aplicaciones; esto no se puede cambiar.

- Eliminar claves de API

Para realizar cambios en una clave de API:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la pestaña **Atributos** de la página Configuración.

3. Seleccione la pestaña **API**.

Configuración

AtributosSeguridadAPI

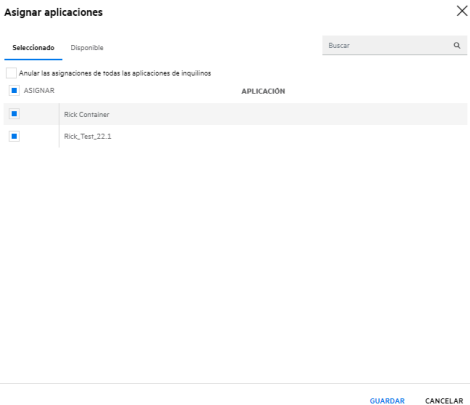
+ AGREGAR CLAVE

NOMBRE	CLAVE DE API	TIPO DE CONCESIÓN	ROL	FECHA DE ÚLTIMO INICIO DE SESIÓN	DIRECCIÓN IP DE ÚLTIMO INICIO DE SESIÓN	AUTORIZADA				
ManageApplications	ee2828c6-e71c-4ca6-8ea2-f643bd0eab78	Credenciales de cliente	Administrar aplicaciones	2022/04/14	15.122.108.150	SI	NUEVO SECRETO	EDITAR	ELIMINAR	ASIGNAR APLICACIONES
ReadOnly	c6599566-be40-4612-9804-6cece1a97b83	Credenciales de cliente	Solo lectura			SI	NUEVO SECRETO	EDITAR	ELIMINAR	ASIGNAR APLICACIONES
ReadOnly for 22.1	95f2661d-3ff4-4edf-bfa9-dad49290b823	Credenciales de cliente	Solo lectura	2022/04/07	15.122.101.250	SI	NUEVO SECRETO	EDITAR	ELIMINAR	ASIGNAR APLICACIONES
SecurityLead	ff06c71-2945-4774-a9bf-d76cb8935f7f	Credenciales de cliente	Líder en seguridad			SI	NUEVO SECRETO	EDITAR	ELIMINAR	ASIGNAR APLICACIONES
StartScans	ec527d4a-4737-4e9f-8d26-9b0aa0ae9cc2	Credenciales de cliente	Iniciar análisis			SI	NUEVO SECRETO	EDITAR	ELIMINAR	ASIGNAR APLICACIONES

4. Puede realizar las siguientes tareas:

Tarea	Procedimiento
Generar nuevo secreto	1. Haga clic en Nuevo secreto. Aparecerá un mensaje de confirmación. 2. Haga clic en Sí. Esto anulará el secreto actual.
Editar la configuración de la clave de API	1. Haga clic en Editar. Se abrirá la ventana Agregar/editar clave de la aplicación. 2. Edite los campos según sea necesario.
Eliminar clave de API	1. Haga clic en Eliminar. Aparecerá un mensaje de confirmación. 2. Haga clic en Sí.

Tarea	Procedimiento
Asignar aplicaciones a la clave de API	- Haga clic en Asignar aplicaciones. - Seleccione la pestaña Disponible.  - Realice las siguientes acciones para seleccionar aplicaciones: - Marque la casilla de verificación junto a las aplicaciones individuales. - Marque la casilla de verificación ASIGNAR para seleccionar las aplicaciones mostradas. - Marque la casilla de verificación Asignar todas las aplicaciones de inquilinos para seleccionar todas las aplicaciones. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones. - Haga clic en Guardar.

Tarea	Procedimiento
Cancelar la asignación de aplicaciones de la clave de API	- Haga clic en Asignar aplicaciones. - Seleccione la pestaña Seleccionados.  - Realice las siguientes acciones para eliminar aplicaciones: - Desactive la casilla de verificación junto a las aplicaciones individuales. - Desactive la casilla de verificación ASIGNAR para eliminar las aplicaciones mostradas. - Seleccione la casilla de verificación Anular las asignaciones de todas las aplicaciones de inquilinos para eliminar todas las aplicaciones. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones. - Haga clic en Guardar.

1.8.1.3. Administración de atributos

Los atributos proporcionan información adicional acerca de las aplicaciones; se utilizan como filtros para ayudar a hacer un seguimiento de aplicaciones, versiones, microservicios, problemas y análisis. Los atributos tienen una finalidad informativa y no afectan de ningún modo al proceso de evaluación.

Los líderes en seguridad pueden agregar, editar y eliminar los atributos. Los atributos a nivel del sistema están predefinidos y no se pueden eliminar; algunos atributos del sistema son editables.

Estos son los tipos de atributo disponibles:

- Atributos de la aplicación. Los atributos de las aplicaciones son atributos del sistema y personalizados.
- Atributos de microservicio. Los atributos de microservicio son atributos personalizados.
- Atributos de versión. Los atributos de versión son atributos del sistema.
- Atributos de problema. Los atributos de problema son atributos del sistema. También se pueden editar los siguientes atributos de problema: **Estado del auditor (abierto)**, **Estado del auditor (cerrado)**, **Estado de desarrollador (abierto)**, y **Estado de desarrollador (cerrado)**.
- Atributos de análisis: los atributos de análisis son atributos personalizados.

Esta sección aborda los siguientes temas:

- [Adición de un atributo](#)
- [Edición de un atributo](#)
- [Eliminación de un atributo](#)

1.8.1.3.1. Adición de un atributo

Los líderes en seguridad pueden agregar los atributos de microservicio y aplicación.

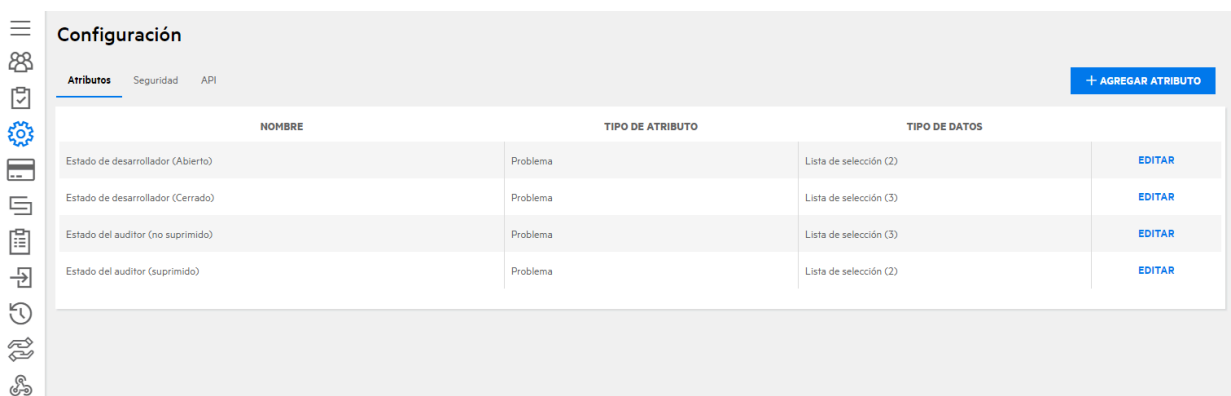
Realice lo siguiente para agregar un atributo:

1. Seleccione la vista **Administración**.

Aparecerá la página Configuración de usuarios.

2. Haga clic en **Configuración**.

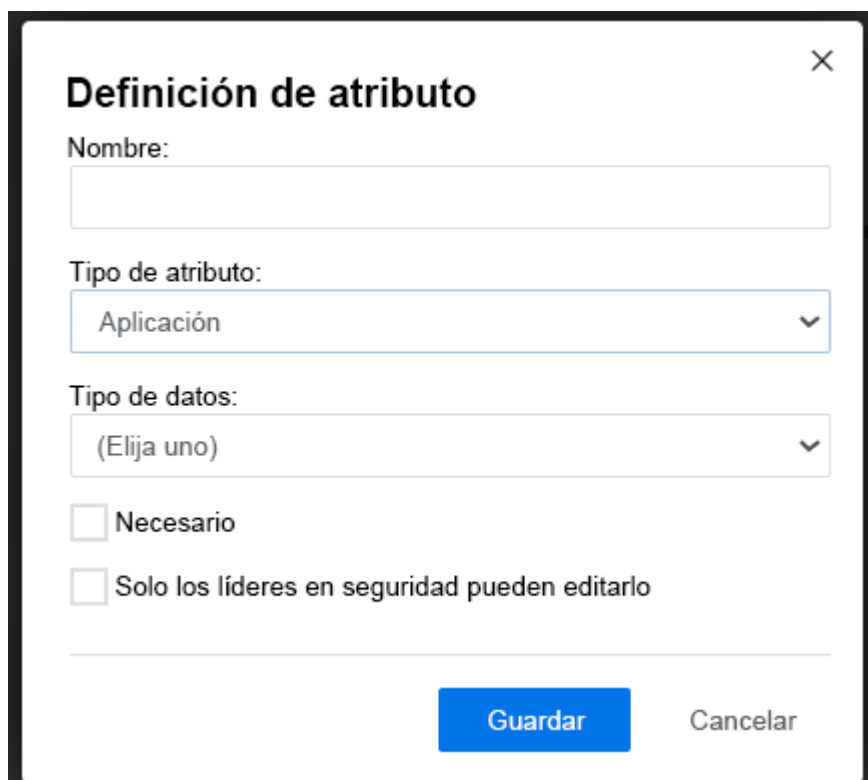
Aparecerá la pestaña **Atributos** de la página Configuración.



NOMBRE	TIPO DE ATRIBUTO	TIPO DE DATOS	
Estado de desarrollador (Abierto)	Problema	Lista de selección (2)	EDITAR
Estado de desarrollador (Cerrado)	Problema	Lista de selección (3)	EDITAR
Estado del auditor (no suprimido)	Problema	Lista de selección (3)	EDITAR
Estado del auditor (suprimido)	Problema	Lista de selección (2)	EDITAR

3. Haga clic en **+Agregar atributo**.

Aparecerá la ventana Definición de atributo.



Definición de atributo

Nombre:

Tipo de atributo:

Aplicación

Tipo de datos:

(Elija uno)

☐ Necesario

☐ Solo los líderes en seguridad pueden editarlo

Guardar Cancelar

4. Rellene los siguientes campos. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Nombre	Especifique el nombre del nuevo atributo.
Tipo de atributo	Seleccione un tipo de atributo. Las opciones disponibles son: ◦ Aplicación ◦ Microservicio ◦ Versión ◦ Problema ◦ Análisis

Campo	Descripción
Tipo de datos	Seleccione el tipo de datos: ◦ Lista de selección: este tipo de atributo permite la selección de un valor de una lista. Deberá definir los valores posibles del atributo, que aparecerán como una lista desplegable de dicho atributo. ◦ Texto: este tipo de atributo permite el texto de formato libre. Este tipo de valor es el más indicado si desea asignar un número de vale u otro tipo de identificación específica a cada nueva versión. ◦ Booleano: este tipo de atributo permite la selección de valores binarios (verdadero/falso). ◦ Fecha: este tipo de atributo permite la selección de una fecha de un calendario. ◦ Usuario: este tipo de atributo permite seleccionar un usuario de una lista de todos los usuarios activos del inquilino.
Necesario (opcional)	Active la casilla para designar el atributo según sea necesario. Este campo no está disponible para los atributos de problema y análisis.

Campo	Descripción
Solo los líderes en seguridad pueden editarlo (opcional)	Active la casilla para restringir el uso a los líderes en seguridad. Esta opción anula el permiso Administrar aplicaciones.  Note Esta selección excluye la posibilidad de establecer que un atributo sea obligatorio, ya que esto infringiría el permiso Crear aplicación para los usuarios que no son líderes en seguridad.

5. Haga clic en **Guardar**.

El nuevo atributo aparecerá en la lista de atributos.

1.8.1.3.2. Edición de un atributo

Los responsables de seguridad pueden editar valores de lista de selección y determinados ajustes para los atributos existentes. No puede cambiar el nombre del atributo ni el tipo de atributo.



Note

Puede editar los valores de los atributos de problema. Para el atributo **Estado de desarrollador (Abierto)**, los valores predeterminados de **Abierto** y **En corrección** no pueden editarse.

Para editar un atributo:

1. Seleccione la vista **Administración**.

Aparecerá la página Configuración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la pestaña **Atributos** de la página Configuración.

Configuración			
Atributos Seguridad API + AGREGAR ATRIBUTO			
NOMBRE	TIPO DE ATRIBUTO	TIPO DE DATOS	
Estado de desarrollador (Abierto)	Problema	Lista de selección (2)	EDITAR
Estado de desarrollador (Cerrado)	Problema	Lista de selección (3)	EDITAR
Estado del auditor (no suprimido)	Problema	Lista de selección (3)	EDITAR
Estado del auditor (suprimido)	Problema	Lista de selección (2)	EDITAR

3. Haga clic en **Editar** en la fila del atributo que desee editar.

Se mostrará la página **Definición de atributo**.

Definición de atributo

Nombre:

Region

Tipo de datos:

Lista de selección

☐ Necesario

☐ Solo los líderes en seguridad pueden editarlo

Valores (uno por línea)

+

^

v

↕

×

Americas

Emea

Apj

Aus

↕

GUARDAR

CANCELAR

4. Edite los campos según sea necesario. Los campos pueden variar en función del tipo de datos.

Tipo de datos	Acciones disponibles
Lista de selección	◦ Haga clic en  para agregar un nuevo valor. ◦ Use   para reorganizar los valores que aparecen en la lista. ◦ Haga clic en  para ordenar los valores alfabéticamente. ◦ Haga clic en  para quitar un valor de la lista.
Lista de selección, Texto, Booleano, Fecha, Usuario	Active o desactive las siguientes casillas: ◦ Necesario: designe el atributo según corresponda. ◦ Solo los líderes en seguridad pueden editarlo: restrinja el uso del atributo a los líderes en seguridad. Esta opción anula el permiso Administrar aplicaciones.  Note Esta selección excluye la posibilidad de establecer que un atributo sea obligatorio, ya que esto infringiría el permiso Crear aplicación para los usuarios que no son líderes en seguridad.

5. Haga clic en **Guardar**.

Se guardarán los cambios en el atributo.

1.8.1.3.3. Eliminación de un atributo

Puede eliminar los atributos personalizados. Los atributos a nivel de sistema no se pueden eliminar.

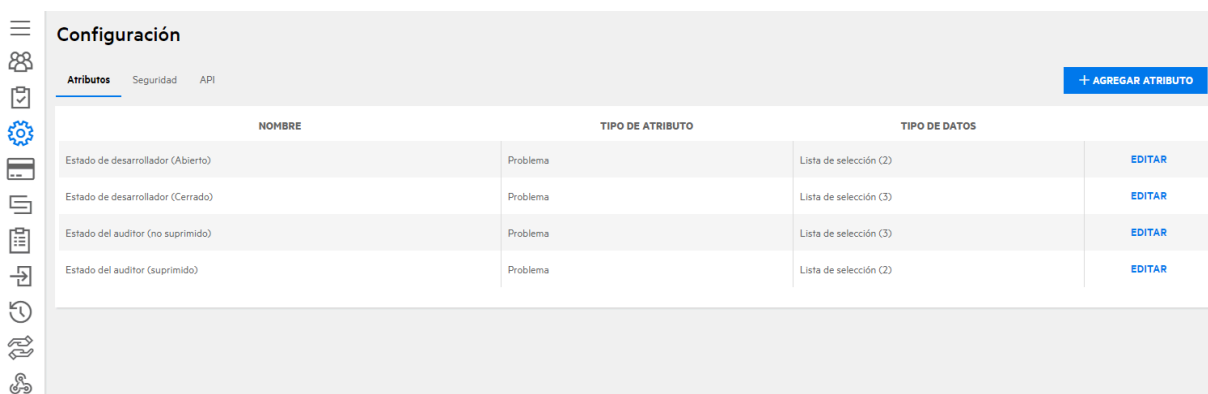
Para eliminar un atributo:

1. Seleccione la vista **Administración**.

Aparecerá la página Configuración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la pestaña **Atributos** de la página Configuración.



Configuración			
Atributos Seguridad API			
NOMBRE	TIPO DE ATRIBUTO	TIPO DE DATOS	
Estado de desarrollador (Abierto)	Problema	Lista de selección (2)	EDITAR
Estado de desarrollador (Cerrado)	Problema	Lista de selección (3)	EDITAR
Estado del auditor (no suprimido)	Problema	Lista de selección (3)	EDITAR
Estado del auditor (suprimido)	Problema	Lista de selección (2)	EDITAR

3. Haga clic en **Eliminar** en la fila del atributo que desee editar.

Aparecerá un mensaje de confirmación.

4. Haga clic en **Sí**.

El atributo y todos los valores asociados se eliminarán.

1.8.1.4. Gestión de redes de OpenText Core Application Security Connect

OpenText Core Application Security Connect se puede usar para establecer VPN de sitio a sitio para evaluaciones dinámicas. Los líderes en seguridad pueden administrar redes de OpenText Core Application Security Connect, que se utilizan para registrar clientes VPN con el servidor VPN.

1.8.1.4.1. Agregar una red de OpenText Core Application Security Connect

Los líderes de seguridad pueden agregar las redes de OpenText Core Application Security Connect a las que se hace referencia en la configuración de VPN de sitio a sitio.



Note

Para obtener información sobre la configuración de OpenText Core Application Security Connect para una evaluación individual, consulte [Configuración de OpenText Core Application Security Connect](#).

Para agregar una red de OpenText Core Application Security Connect:

1. Seleccione la vista **Administración**.

Aparecerá la página Configuración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la pestaña **Atributos** de la página Configuración.

3. Seleccione la pestaña **OpenText Core Application Security Conectar**.

NOMBRE DE RED	NOMBRE DE USUARIO	
test_net	administrador	VER COMANDOS DE DOCKER ELIMINAR
demo_network	administrador	VER COMANDOS DE DOCKER ELIMINAR
simt2_second	administrador	VER COMANDOS DE DOCKER ELIMINAR

4. Haga clic en **+Agregar red**.

Aparece la ventana Agregar red.

Agregar red

Nombre de red

Nombre de usuario

Contraseña

Confirmar contraseña

GUARDAR

CANCELAR

5. Rellene los siguientes campos. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Nombre de red	Especifique el nombre de la red.
Nombre de usuario	Especifique un nombre de usuario de la red de OpenText Core Application Security Connect.
Contraseña	Especifique una contraseña de la red de OpenText Core Application Security Connect. Los caracteres permitidos son letras mayúsculas y minúsculas y números. Escriba la contraseña entre comillas dobles para salvar la existencia caracteres especiales, con la excepción de \$ (signo de dólar), ` (comilla diagonal) y \ (barras diagonales).
Confirmar contraseña	Especifique la contraseña de nuevo.

6. Haga clic en **Guardar**.

La nueva red aparecerá en la lista de redes. El vínculo disponible **Ver comandos de Docker** contiene el código para que el comando de Docker ejecute el cliente VPN e inicialice la conexión entre el cliente VPN y el servidor VPN.

1.8.1.4.2. Borrando una red de OpenText Core Application Security Connect

Los líderes en seguridad pueden eliminar las redes de OpenText Core Application Security Connect.



Note

Las redes de OpenText Core Application Security Connect no se pueden editar. Si necesita actualizar una red existente, debe eliminar la red y agregar una nueva.

Para eliminar una red de OpenText Core Application Security Connect:

1. Seleccione la vista **Administración**.

Aparecerá la página Configuración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la pestaña **Atributos** de la página Configuración.

3. Seleccione la pestaña **OpenText Core Application Security Conectar**.

Configuración		
		+ AGREGAR RED
Atributos Seguridad API Fortify on Demand Connect Configurar el estado del auditor de SAST Aviator		
NOMBRE DE RED	NOMBRE DE USUARIO	
test_net	administrador	VER COMANDOS DE DOCKER ELIMINAR
demo_network	administrador	VER COMANDOS DE DOCKER ELIMINAR
simt2_second	administrador	VER COMANDOS DE DOCKER ELIMINAR

4. Haga clic en **Eliminar** en la fila de la red que desea eliminar.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí**.

La red se elimina.

1.8.1.5. Visualización de derechos

Los líderes en seguridad pueden ver una lista de derechos caducados y activos del inquilino.

Para ver los derechos del inquilino:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Derechos**.

Aparecerá la página Derecho. La pestaña **Derechos de Fortify** muestra los derechos de OpenText Core Application Security; la pestaña **Derechos de Sonatype** muestra los derechos de Sonatype; la pestaña **Derechos de Debricked** muestra los derechos de OpenText Core SCA.



ID. DE DERECHO	CANTIDAD COMPRADA	CANTIDAD CONSUMIDA	FECHA DE INICIO	FECHA DE FINALIZACIÓN	FECHA DE RECORDATORIO	DESCRIPCIÓN	ACCIÓN
7069	200	0	22/10/2024	21/11/2027			EDITAR

3. Puede realizar las siguientes tareas:

Tarea	Procedimiento
Agregar o editar la descripción del derecho	Haga clic en Editar en la fila de un derecho y proporcione una descripción. La descripción puede tener hasta 50 caracteres.
Agregar o editar recordatorios por correo electrónico para derechos que caducan	Haga clic en Establecer/Editar recordatorios. Rellene los siguientes campos: ◦ Primer recordatorio (días): seleccione el número de días antes de que caduque un derecho en el que se enviará el recordatorio. ◦ Segundo recordatorio (días): si desea agregar otro recordatorio, seleccione la casilla de verificación y seleccione la cantidad de días antes de que caduque un derecho en el que se enviará el recordatorio. ◦ Enviar correo electrónico a: especifique las direcciones de correo electrónico separadas por una coma. Una vez configurados, los recordatorios se aplican a todos los derechos del inquilino.

1.8.1.6. Visualización del registro de eventos de administración

Los líderes en seguridad pueden ver el registro de eventos de administración. En el registro de eventos de administración se registran todos los eventos relacionados con aplicaciones, así como los siguientes eventos relacionados con la administración:

- inicios de sesión del usuario correctos y erróneos, y cierres de sesión del usuario
- creación, actualización y eliminación de usuarios
- creación, actualización y eliminación de grupos
- creación, actualización y eliminación de roles
- exportaciones de registros de eventos y de panel
- Creación, actualización y eliminación de clave de API y token de acceso personal, y generación de nuevo secreto
- autenticación de API correcta o errónea
- Cambios en la configuración de administración y de SSO

Realice lo siguiente para ver el registro de eventos de administración:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Registro de eventos**.

Aparecerá la página Registro de eventos.

Registro de eventos

FECHA DEL EVENTO DESDE: 2022/11/28 X FECHA DEL EVENTO HASTA: 2022/11/29 X BORRAR FILTROS

9 encontrados Mostrar: 25 50 100

FECHA DEL EVENTO	TIPO	USUARIO	APLICACIÓN	NOTAS
2022/11/29 10:55:27	Proyecto actualizado	HuangTam	Microservice App 1	ApplicationName = "Microservice App 1", ApplicationType = "Web/Thick-Client", ApplicationBusinessCriticality = "1", ApplicationRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Applications/15461", Origin = "WebUI"
2022/11/29 10:55:03	Atributo añadido	HuangTam		Name = "MS Attr2"
2022/11/29 10:43:50	Versión creada	HuangTam	Microservice App 1	ReleaseName = "v1", SDLCStatus = "3", ReleaseRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Releases/18102", ApplicationName = "Microservice App 1", ApplicationType = "Web/Thick-Client", ApplicationBusinessCriticality = "1", ApplicationRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Applications/15461"
2022/11/29 10:43:49	Proyecto creado	HuangTam	Microservice App 1	ApplicationName = "Microservice App 1", ApplicationType = "Web/Thick-Client", ApplicationBusinessCriticality = "1", ApplicationRedirectUri = "https://fodqa9-tenant.fortifyfodqa9.local/redirect/Applications/15461"
2022/11/29 09:44:58	Atributo añadido	HuangTam		Name = "MS Attr1"

expandir todo | contraer todo

FECHA DEL EVENTO

De: 2022/11/28

Para: 2022/11/29

3. Puede realizar las siguientes tareas:

Tarea	Acción
Exportar el registro de eventos de los últimos 13 meses	Haga clic en Exportar . El archivo .csv se guarda en forma local en la carpeta especificada en la configuración del navegador.
Buscar en el registro de eventos	Escriba una palabra clave o una frase en el campo de texto de búsqueda y pulse Intro .
Mostrar u ocultar la lista de filtros	Haga clic en  .
Expandir o contraer filtros	Haga clic en expandir todo contraer todo  o en la flecha junto al nombre del filtro.
Quitar los filtros aplicados	Haga clic en X o en Borrar filtros en la parte superior de la página. El filtro está configurado para las últimas 24 horas de forma predeterminada.

Temas relacionados:

Para obtener más información sobre cómo ver eventos relacionados con una aplicación específica, consulte [Visualización del registro de eventos de aplicaciones](#).

1.8.1.7. Configuración del estado del auditor de SAST Aviator

Los responsables de seguridad pueden configurar el estado del auditor, lo que permite a los clientes gestionarlo ellos mismos.

Para configurar el estado del auditor de SAST Aviator:

1. Seleccione la vista **Administración**.

Aparecerá la página Configuración de usuarios.

2. Haga clic en **Configuración**.

Aparecerá la pestaña **Atributos** de la página Configuración.

3. Seleccione la pestaña **Configurar el estado del auditor de SAST Aviator**.

Tier	Resultado de Aviator	Estado del auditor
1	Verdadero positivo	VP de prueba
1	Falso positivo	FP de prueba
1	No seguro	Prueba No seguro1
2	Verdadero positivo	VP de prueba12
2	Falso positivo	FP de prueba12
2	No seguro	Prueba No seguro2

Guardar

4. Rellene los siguientes campos. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Tier	Indica el nivel de Aviator ◦ Tier1: Lenguajes como Java y .NET ◦ Tier2: Resto de idiomas
Resultado de Aviator	Indica el resultado de Aviator
Estado del auditor	Seleccionar el estado de Aviator En función del estado seleccionado, Aviator configura el estado del auditor.

- Haga clic en **Guardar** para guardar los mapeos de configuración. Puede configurar los mapeos a cualquier estado del auditor disponible en el portal.

1.8.2. Administración de usuarios

Los líderes en seguridad y los usuarios con los permisos Administrar usuarios pueden administrar los usuarios en OpenText Core Application Security. Los líderes en seguridad pueden realizar todas las tareas de administración de usuarios. Los usuarios con los permisos Administrar usuarios pueden administrar cuentas y grupos de usuarios, pero no roles.

Esta sección aborda los siguientes temas:

- [Roles y permisos](#)
- [Usuarios](#)
- [Grupos](#)

1.8.2.1. Roles y permisos

Los roles controlan las acciones de usuario en OpenText Core Application Security. Los roles son recopilaciones de permisos que especifican las acciones que se pueden realizar. Cada usuario se asigna a un rol específico. Los líderes en seguridad pueden administrar roles, lo que incluye la asignación de usuarios a roles y la creación, la edición y la eliminación de roles.

Hay seis roles predeterminados disponibles. Las organizaciones también pueden definir roles personalizados que se ajusten mejor a sus necesidades. Los roles personalizados pueden utilizarse para alinear los roles de usuario con los roles existentes en una organización, así como para ampliar o limitar las responsabilidades de los usuarios. Las pequeñas organizaciones podrían emplear roles con más permisos, mientras que las organizaciones grandes o muy estructuradas podrían utilizar roles con permisos más restringidos.

Esta sección aborda los siguientes temas:

- [Permisos](#)
- [Roles predeterminados](#)
- [Visualización de roles](#)
- [Creación de un rol](#)
- [Edición de un rol](#)
- [Eliminación de un rol](#)

1.8.2.1.1. Permisos

Los permisos especifican las acciones que un usuario puede realizar. En OpenText Core Application Security, los permisos se dividen en dos tipos: permisos de nivel de inquilino y permisos a nivel de aplicación.

- Los **Permisos a nivel de inquilino** son permisos que se aplican en el nivel del Inquilino, como administración de usuarios, exportación de datos y descarga de herramientas. Para ver una lista detallada de los permisos a nivel de inquilino, consulte [Permisos a nivel de inquilino](#).
- Los **permisos a nivel de aplicación** son permisos que se aplican a las aplicaciones, como creación de aplicaciones, inicio de análisis, edición de problemas y administración de informes. Para ver una lista detallada de los permisos de nivel de aplicación, consulte [Permisos a nivel de aplicación](#).

Permisos a nivel de inquilino

La siguiente tabla muestra los permisos a nivel de inquilino disponibles para un rol. Cualquier permiso a nivel de inquilino puede asignarse a un rol personalizado (excepto Administración, que está asociado al rol de líder en seguridad).

Categoría	Permisos	Acciones permitidas
Administración	N/C (solo para líderes en seguridad)	• Administrar directivas de seguridad • Administrar atributos • Configurar la seguridad de usuarios • Administrar claves de API • Configurar Application Defender • Configurar SSO • Ver registro de eventos de administración • Administrar roles • Administrar plantillas de auditoría globales • Descargar la carga de análisis estático para todas las aplicaciones

Categoría	Permisos	Acciones permitidas
Acceso a las aplicaciones	• Manual: las aplicaciones no se asignan de forma predeterminada. Las aplicaciones deben asignarse a un usuario o a un grupo. Si se selecciona Manual, Administrar usuarios, Exportar datos Administración de proveedores se establecerán como Denegar. • Todo: permite acceder a todas las aplicaciones. No hay restricciones sobre los permisos a nivel de inquilino.	Se determina mediante los permisos a nivel de aplicación asignados al rol.

Categoría	Permisos	Acciones permitidas
Administrar usuarios	Denegar, Permitir (requiere que Acceso a las aplicaciones se establezca como Todo).	• Agregar, editar y eliminar usuarios (solo los líderes en seguridad pueden editar otros líderes en seguridad) • Exportar datos de usuario • Administrar grupos • Asignar cursos de formación a usuarios • Ver informe de formación
Exportar datos	Denegar, Permitir (requiere que Acceso a las aplicaciones se establezca como Todo).	• Ver pestaña Exportaciones de datos • Crear exportaciones de datos • Editar plantillas de exportación de datos • Eliminar plantillas de exportación de datos • Generar exportaciones de datos • Descargar exportaciones de datos • Eliminar archivos de exportación de datos

Categoría	Permisos	Acciones permitidas
Administración de proveedores	Denegar, Permitir (requiere que Acceso a las aplicaciones se establezca como Todo).	• Comprobar y aprobar proveedor • Solicitud para ser proveedor • Publicar informe para proveedor
Descargar herramientas	Denegar, Permitir	Ver página Herramientas
Acceder a la formación	Denegar, Permitir	Tomar cursos de formación
Visualización de aplicaciones de terceros	Denegar, Permitir	Ver componentes de código abierto que se usan en todas las aplicaciones
Configurar webhooks	Denegar, Permitir (requiere que Acceso a las aplicaciones se establezca como Todo).	Administrar webhooks
Paneles	Vista, Crear	Ver los paneles de Magellan Administrar los paneles de Magellan (próximamente)

Permisos a nivel de aplicación

La siguiente tabla muestra los permisos a nivel de aplicación disponibles para un rol. Cualquier permiso a nivel de aplicación puede asignarse a un rol predeterminado.

Categoría	Permisos	Acciones permitidas
Aplicaciones	Ver, Administrar, Crear	Vista • Ver problemas, análisis e informes • Descargar resultados de análisis (FPR y SBOM) Administrar • Todas las acciones del permiso Ver • Editar configuración de la aplicación (excepto el nombre de la aplicación) • Ver usuarios asignados a la aplicación • Crear versión • Editar configuración de la versión • Eliminar versión • Ver y exportar registro de eventos de la aplicación • Importar resultados de análisis (FPR y SBOM) Crear • Todas las acciones del permiso Administrar • Crear nueva aplicación • Editar el nombre de la aplicación

Categoría	Permisos	Acciones permitidas
		Eliminar aplicación
Problemas	Ver, Editar, Auditar	Vista - Agregar y eliminar captura de pantalla - Exportar la lista de problemas Editar - Todas las acciones de Ver - Editar los campos Usuario asignado y Estado del desarrollador, agregar un comentario - Enviar error Auditar - Todas las acciones de Editar - Editar campos Gravedad y Estado del auditor - Crear y editar plantilla de auditoría de aplicaciones

Categoría	Permisos	Acciones permitidas
Informes	Ver, Crear	Vista • Ver informes principales • Descargar informes principales • Ver informes de proveedores • Descargar informes de proveedores • Exportar panel de inquilino • Exportar la página Sus versiones Crear • Crear informes • Eliminar informes • Ver plantillas de informe • Crear plantillas de informe • Editar plantillas de informe

Categoría	Permisos	Acciones permitidas
Iniciar análisis dinámicos	Denegar, Configurar, Permitir	Configure • Editar página de configuración de análisis dinámico Permitir • Programar un análisis dinámico • Cancelar análisis dinámico
Iniciar análisis estáticos	Denegar, Configurar, Permitir	Configure • Editar página de configuración de análisis estático Permitir • Cargar la carga de un análisis estático • Cancelar análisis estático • Descargar la carga de análisis estático para las aplicaciones asignadas

Categoría	Permisos	Acciones permitidas
Iniciar análisis móviles	Denegar, Configurar, Permitir	Configure • Editar página de configuración de análisis móvil Permitir • Programar un análisis móvil • Cancelar análisis móvil
Enviar un desafío de falso positivo	Denegar, Permitir	Enviar desafíos de falso positivo
Consumir derechos	Denegar, Permitir	Consumir derechos al iniciar un análisis

1.8.2.1.2. Roles predeterminados

OpenText Core Application Security se configura con seis roles predeterminados. Los roles predeterminados se pueden editar o eliminar (excepto los roles Líder en seguridad y Desarrollador).

- **Líder en seguridad:** acceso completo. El líder en seguridad puede acceder a todas las aplicaciones y realizar todas las tareas, lo que incluye crear aplicaciones y versiones, trabajar con datos, auditar problemas y administrar informes. El líder en seguridad es el único rol que tiene el permiso Administración, el cual incluye la capacidad a de administrar roles, directivas de seguridad y otras opciones administrativas.
- **Desarrollador:** acceso limitado. El desarrollador puede acceder a las aplicaciones asignadas al usuario. El desarrollador puede trabajar con datos de problemas y administrar informes. El desarrollador es el rol predeterminado de los nuevos usuarios.
- **Desarrollador principal:** acceso de nivel medio. El desarrollador principal puede crear nuevas aplicaciones, pero solo puede acceder a las aplicaciones asignadas al usuario. El desarrollador principal puede trabajar con datos de problemas, iniciar análisis y administrar informes.
- **Líder en aplicaciones:** acceso de nivel medio. El líder en aplicaciones tiene el mismo acceso que el desarrollador principal, además de la posibilidad de auditar problemas.
- **Ejecutivo:** acceso de solo lectura. El ejecutivo tiene acceso de solo lectura a las aplicaciones asignadas al usuario.
- **Revisor:** acceso de solo lectura. El revisor tiene acceso de solo lectura a todas las aplicaciones.

En la siguiente tabla se muestra el conjunto de permisos de cada rol predeterminado.

Permiso	Líder en seguridad	principal	Desarrollador principal (editable)	Líder en aplicaciones (editable)	Ejecutivo (editable)	Revisor (editable)
Permisos a nivel de inquilino						
Administración	X					
Acceso a las aplicaciones	Todo	Manual	Manual	Manual	Manual	Todo
Administrar usuarios	X					
Exportar datos	X					
Administración de proveedores	X					
Descargar herramientas	X	X	X	X		
Acceder a educación	X	X	X	X	X	X

Permiso	Líder en seguridad	principal	Desarrollador principal (editable)	Líder en aplicaciones (editable)	Ejecutivo (editable)	Revisor (editable)
Visualización de aplicaciones de terceros	X					
Configurar webhooks	X					
Permisos a nivel de aplicación						
Aplicaciones	Crear	Vista	Crear	Crear	Vista	Vista
Problemas	Auditar	Editar	Editar	Auditar	Vista	Vista
Informes	Crear	Crear	Crear	Crear	Vista	Vista
Iniciar análisis dinámicos	Iniciar	Denegar	Iniciar	Iniciar	Denegar	Denegar
Iniciar análisis estáticos	Iniciar	Denegar	Iniciar	Iniciar	Denegar	Denegar

Permiso	Líder en seguridad	principal	Desarrollador principal (editable)	Líder en aplicaciones (editable)	Ejecutivo (editable)	Revisor (editable)
Iniciar análisis móviles	Iniciar	Denegar	Iniciar	Iniciar	Denegar	Denegar
Configurar servidor de compilación	X					
Enviar un desafío de falso positivo	X					
Consumir derechos	X	X	X	X	X	X

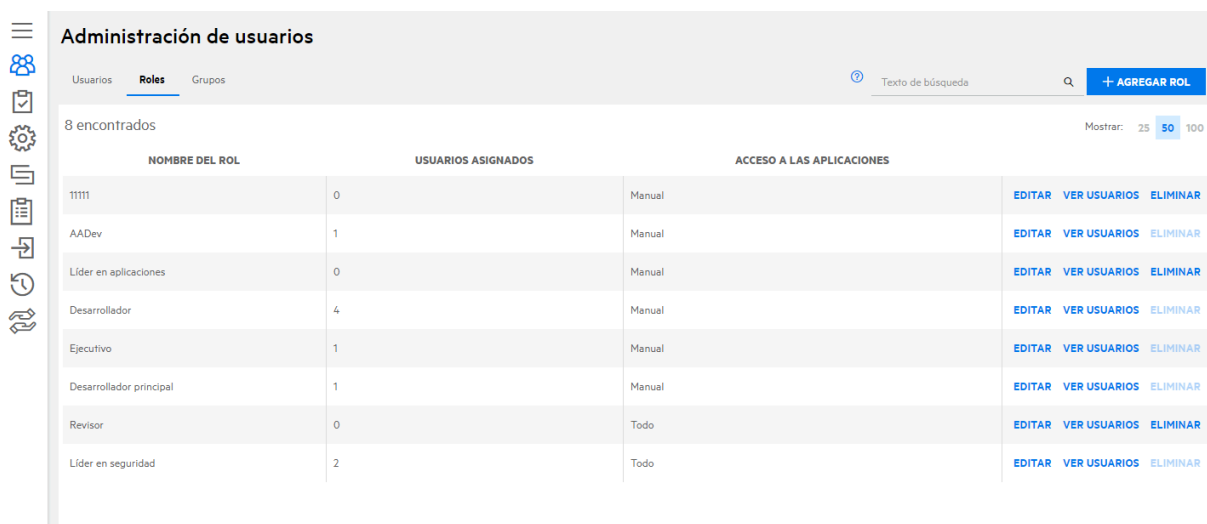
1.8.2.1.3. Visualización de roles

Realice lo siguiente para ver los roles en el inquilino:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Seleccione la pestaña **Roles**.



Administración de usuarios			
Usuarios Roles Grupos Texto de búsqueda + AGREGAR ROL			
8 encontrados			
NOMBRE DEL ROL	USUARIOS ASIGNADOS	ACCESO A LAS APLICACIONES	
11111	0	Manual	EDITAR VER USUARIOS ELIMINAR
AADev	1	Manual	EDITAR VER USUARIOS ELIMINAR
Líder en aplicaciones	0	Manual	EDITAR VER USUARIOS ELIMINAR
Desarrollador	4	Manual	EDITAR VER USUARIOS ELIMINAR
Ejecutivo	1	Manual	EDITAR VER USUARIOS ELIMINAR
Desarrollador principal	1	Manual	EDITAR VER USUARIOS ELIMINAR
Revisor	0	Todo	EDITAR VER USUARIOS ELIMINAR
Líder en seguridad	2	Todo	EDITAR VER USUARIOS ELIMINAR

En la siguiente tabla se describe cómo desplazarse por la pestaña **Roles**.

Tarea	Acción
Buscar en la lista de roles	Escriba una palabra clave o una frase en el campo de búsqueda y pulse Intro . Para quitar los resultados de búsqueda, elimine el texto del campo de búsqueda y pulse Intro .
Crear un rol	Haga clic en Agregar rol . Para obtener más información, consulte Creación de un rol .
Ver usuarios asignados a un rol	Haga clic en Ver usuarios en la columna de acciones.
Editar un rol	Haga clic en Editar en la columna de acciones. Para obtener más información, consulte Edición de un rol .
Eliminar un rol	Haga clic en Eliminar en la columna de acciones. Para obtener más información, consulte Eliminar un rol .

1.8.2.1.4. Creación de un rol

Realice lo siguiente para crear un rol:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Seleccione la pestaña **Roles**.

NOMBRE DEL ROL	USUARIOS ASIGNADOS	ACCESO A LAS APLICACIONES	
11111	0	Manual	EDITAR VER USUARIOS ELIMINAR
AADev	1	Manual	EDITAR VER USUARIOS ELIMINAR
Líder en aplicaciones	0	Manual	EDITAR VER USUARIOS ELIMINAR
Desarrollador	4	Manual	EDITAR VER USUARIOS ELIMINAR
Ejecutivo	1	Manual	EDITAR VER USUARIOS ELIMINAR
Desarrollador principal	1	Manual	EDITAR VER USUARIOS ELIMINAR
Revisor	0	Todo	EDITAR VER USUARIOS ELIMINAR
Líder en seguridad	2	Todo	EDITAR VER USUARIOS ELIMINAR

3. Haga clic en **+Agregar rol**.

Aparece la ventana Agregar/editar rol.

Agregar/editar rol

Nombre del rol

Permisos a nivel de inquilino

Acceso a las aplicaciones	Manual	Todo
Administrar usuarios	Denegar	
Exportar datos	Denegar	
Administración de proveedores	Denegar	
Descargar herramientas	Denegar	
Acceder a la formación	Denegar	
Ver aplicaciones de terceros	Denegar	

Permisos a nivel de aplicación

Aplicaciones	Ver	Administrar	Crear
Problemas	Ver	Editar	Auditar
Informes	Ver	Crear	
Iniciar análisis dinámicos		Denegar	
Iniciar análisis estáticos		Denegar	
Iniciar análisis móviles		Denegar	
Enviar desafío de falso positivo		Denegar	

GUARDAR CANCELAR

4. En el campo **Nombre del rol**, escriba el nombre del nuevo rol.

5. Seleccione los permisos a nivel de aplicación y de inquilino para el rol. Para obtener más información sobre permisos específicos, consulte [Permisos](#).

6. Haga clic en **Guardar**.

El nuevo rol aparecerá en la lista de roles.

1.8.2.1.5. Edición de un rol

Realice lo siguiente para editar un rol:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Seleccione la pestaña **Roles**.

NOMBRE DEL ROL	USUARIOS ASIGNADOS	ACCESO A LAS APLICACIONES	
11111	0	Manual	EDITAR VER USUARIOS ELIMINAR
AADev	1	Manual	EDITAR VER USUARIOS ELIMINAR
Líder en aplicaciones	0	Manual	EDITAR VER USUARIOS ELIMINAR
Desarrollador	4	Manual	EDITAR VER USUARIOS ELIMINAR
Ejecutivo	1	Manual	EDITAR VER USUARIOS ELIMINAR
Desarrollador principal	1	Manual	EDITAR VER USUARIOS ELIMINAR
Revisor	0	Todo	EDITAR VER USUARIOS ELIMINAR
Líder en seguridad	2	Todo	EDITAR VER USUARIOS ELIMINAR

3. Haga clic en **Editar** en la fila del rol que desea editar.

Aparecerá la ventana modal Agregar/Editar rol.

Agregar/editar rol ?

Nombre del rol

Permisos a nivel de inquilino

Acceso a las aplicaciones	Manual	Todo
Administrar usuarios	Denegar	
Exportar datos	Denegar	
Administración de proveedores	Denegar	
Descargar herramientas	Denegar	
Acceder a la formación	Denegar	
Ver aplicaciones de terceros	Denegar	

Permisos a nivel de aplicación

Aplicaciones	Ver	Administrar	Crear
Problemas	Ver	Editar	Auditar
Informes	Ver	Crear	
Iniciar análisis dinámicos	Denegar		
Iniciar análisis estáticos	Denegar		
Iniciar análisis móviles	Denegar		
Enviar desafío de falso positivo	Denegar		

GUARDAR CANCELAR



Note

Los conjuntos de permisos de los roles de líder en seguridad y desarrollador no pueden editarse.

4. Edite los campos según sea necesario.

5. Haga clic en **Guardar**

Se guardarán los cambios aplicados a los roles.

1.8.2.1.6. Eliminación de un rol

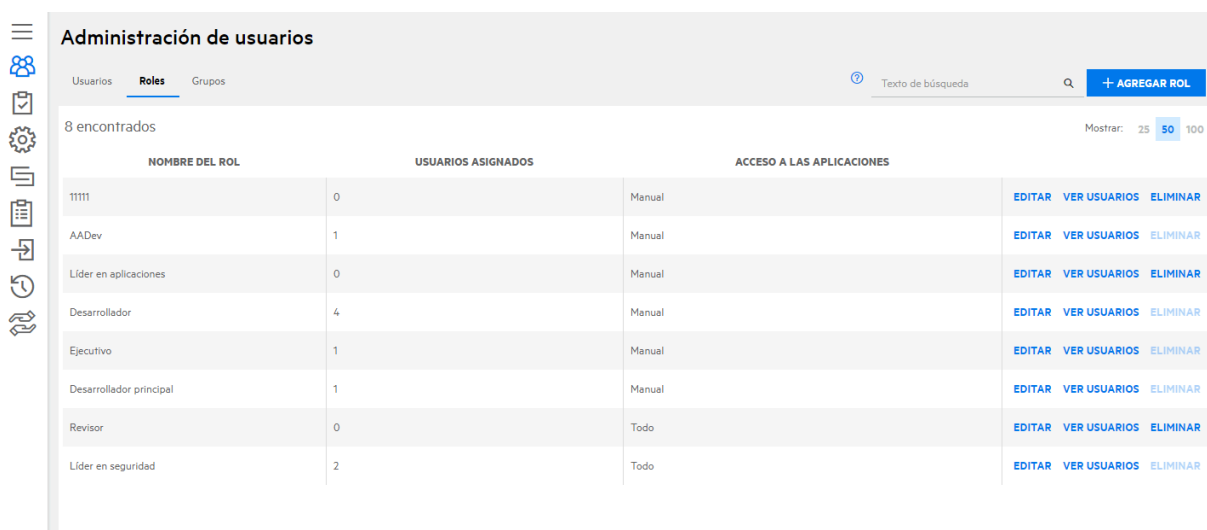
No pueden eliminarse tanto los roles de líder en seguridad y de desarrollador como los roles a los que se asignan usuarios.

Realice lo siguiente para eliminar un rol:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Seleccione la pestaña **Roles**.



Administración de usuarios					
Usuarios Roles Grupos			Texto de búsqueda		
8 encontrados			Mostrar: 25 50 100		
NOMBRE DEL ROL	USUARIOS ASIGNADOS	ACCESO A LAS APLICACIONES			
11111	0	Manual	EDITAR	VER USUARIOS	ELIMINAR
AADev	1	Manual	EDITAR	VER USUARIOS	ELIMINAR
Líder en aplicaciones	0	Manual	EDITAR	VER USUARIOS	ELIMINAR
Desarrollador	4	Manual	EDITAR	VER USUARIOS	ELIMINAR
Ejecutivo	1	Manual	EDITAR	VER USUARIOS	ELIMINAR
Desarrollador principal	1	Manual	EDITAR	VER USUARIOS	ELIMINAR
Revisor	0	Todo	EDITAR	VER USUARIOS	ELIMINAR
Líder en seguridad	2	Todo	EDITAR	VER USUARIOS	ELIMINAR

3. Haga clic en **Eliminar** en la fila del rol que desea eliminar.

Aparecerá un mensaje de confirmación.

4. Haga clic en **Sí**.

El rol se eliminará.

1.8.2.2. Usuarios

Los usuarios con permiso para Administrar usuarios pueden administrar usuarios y grupos.

Esta sección aborda los siguientes temas:

- [Visualización de usuarios](#)
- [Crear un usuario](#)
- [Edición de una cuenta de usuario](#)
- [Administración de la asignación de aplicaciones a un usuario](#)
- [Eliminación de una cuenta de usuario](#)

1.8.2.2.1. Visualización de usuarios

Realice lo siguiente para ver los usuarios en el inquilino:

1. Seleccione la vista **Administración**.

Aparecerá la pestaña **Usuarios** de la página Administración de usuarios. La pestaña muestra la lista de usuarios.



The screenshot shows the 'Administración de usuarios' (User Administration) page. The 'Usuarios' (Users) tab is selected. The page displays a search bar, an 'Exportar' (Export) button, and a '+ Agregar usuario' (Add user) button. Below the search bar, it indicates '1 encontrado' (1 found) and a 'seleccionar todo' (select all) link. A table lists the user details, and a 'Mostrar' (Show) dropdown is set to 25 items.

	Nombre de usuario	Nombre de pila	Apellido	Correo electrónico	Número de teléfono	Nombre de rol	Estado	Fecha de creación	Fecha de último inicio de sesión	Creado mediante	
☐	saislead	Sai	Fu	sai@gogame.com		Lider en seguridad	Activo	22/10/2024	23/10/2024		Editar Asignar aplicaciones Ver aplicaciones Eliminar

En la siguiente tabla se describe cómo desplazarse por la pestaña **Usuarios**.

Tarea	Acción
Buscar en la lista de usuarios	Escriba una palabra o frase en el campo de búsqueda y pulse Intro . Para quitar los resultados de búsqueda, elimine el texto del campo de búsqueda y pulse Intro .
Exporte la lista de usuarios.	Haga clic en Exportar . Un archivo CSV que contiene detalles sobre todos los usuarios se guarda en una carpeta local especificada en la configuración del navegador.
Agregar un usuario	Haga clic en Agregar usuario . Para obtener más información, consulte Agregar una cuenta de usuario .
Administrar aplicaciones asignadas a un usuario	Haga clic en Asignar aplicaciones en la columna de acciones. Para obtener más información, consulte Administrar la asignación de aplicaciones para un usuario .
Ver aplicaciones asignadas a un usuario	Haga clic en Ver aplicaciones en la columna de acciones.
Editar un usuario	Haga clic en Editar en la columna de acciones. Para obtener más información, consulte Edición de una cuenta de usuario .
Eliminar un usuario	Haga clic en Eliminar en la columna de acciones. Para obtener más información, consulte Eliminación de una cuenta de usuario .

1.8.2.2.2. Crear un usuario

Realice lo siguiente para crear un usuario:

1. Seleccione la vista **Administración**.

Aparecerá la pestaña **Usuarios** de la página Administración de usuarios.

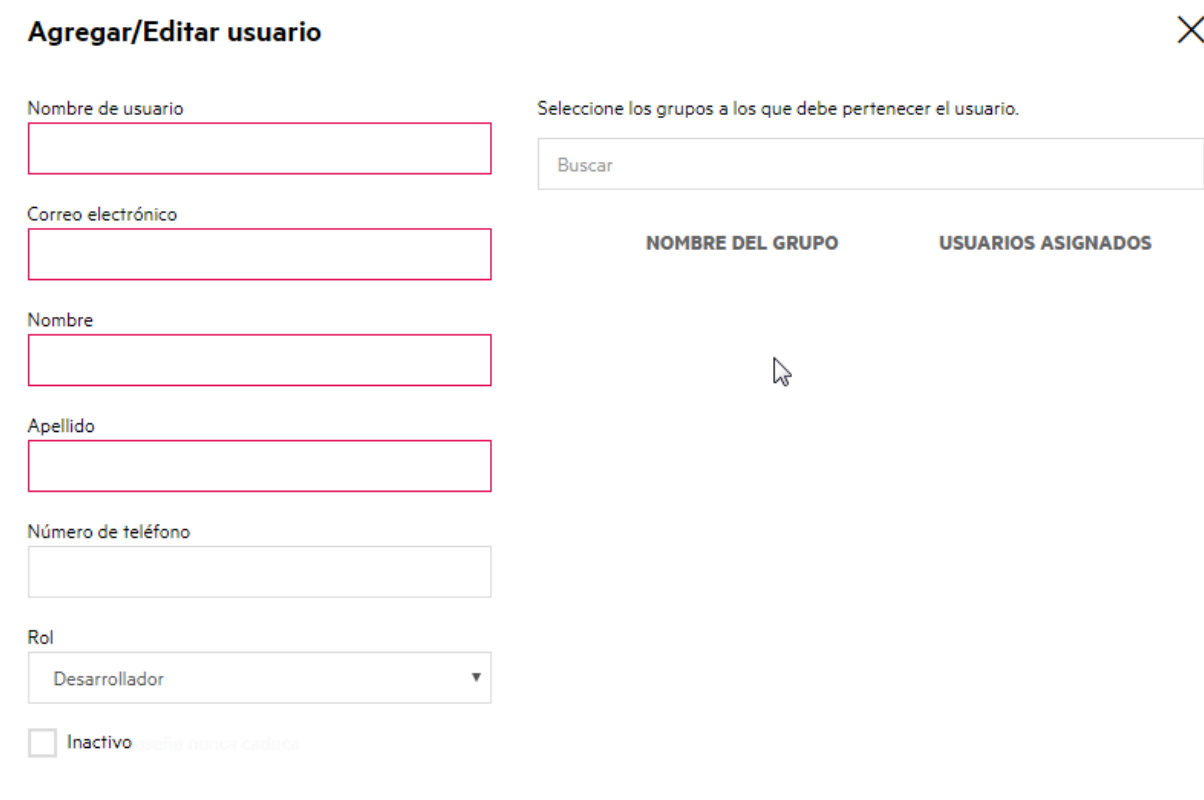


The screenshot shows the 'Administración de usuarios' interface. It has a sidebar with icons for users, roles, and groups. The main area has tabs for 'Usuarios', 'Roles', and 'Grupos'. Below the tabs, there's a search bar and a '+ Agregar usuario' button. A table lists users with columns: Nombre de usuario, Nombre de pila, Apellido, Correo electrónico, Número de teléfono, Nombre de rol, Estado, Fecha de creación, Fecha de último inicio de sesión, and Creado mediante. One user is listed: 'saislead' with role 'Lider en seguridad' and state 'Activo'.

Nombre de usuario	Nombre de pila	Apellido	Correo electrónico	Número de teléfono	Nombre de rol	Estado	Fecha de creación	Fecha de último inicio de sesión	Creado mediante
saislead	Sai	Fu	sai@gogame.com		Lider en seguridad	Activo	22/10/2024	23/10/2024	

2. Haga clic en **+ Agregar usuario**.

Aparece la ventana Agregar/Editar usuario.



The screenshot shows the 'Agregar/Editar usuario' modal. It has a title bar with a close button. The form is divided into two columns. The left column contains input fields for 'Nombre de usuario', 'Correo electrónico', 'Nombre', 'Apellido', 'Número de teléfono', and a dropdown for 'Rol' (currently set to 'Desarrollador'). There is also a checkbox for 'Inactivo' with the text 'usuario nunca caduca'. The right column has a search bar labeled 'Buscar' and a table with two columns: 'NOMBRE DEL GRUPO' and 'USUARIOS ASIGNADOS'.

GUARDAR

CANCELAR

3. Rellene los campos según sea necesario. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Nombre de usuario	Escriba un nombre de usuario único. El nombre de usuario no se puede cambiar una vez creado.
Correo electrónico	Escriba la dirección de correo electrónico del usuario.
Nombre de pila	Escriba el nombre del usuario.
Apellido	Escriba el apellido del usuario.
Número de teléfono	(Opcional) Escriba el número de teléfono del usuario. No se aceptan guiones ni otros separadores.
Rol	Seleccione el rol del usuario (el rol predeterminado es Desarrollador). Para obtener más información sobre los roles de usuario, consulte Roles .
La contraseña nunca caduca	(Opcional) Active la casilla para que la contraseña sea permanente.
Inactivo	(Opcional) Active la casilla para marcar el usuario como inactivo. El usuario no podrá iniciar sesión en OpenText Core Application Security.

4. (Opcional) Seleccione los grupos a los que se asignará el usuario. Puede usar el cuadro de búsqueda para filtrar la lista de grupos.

5. Haga clic en **Guardar**.

El nuevo usuario aparecerá en la lista de usuarios.

1.8.2.2.3. Edición de una cuenta de usuario

Puede editar una cuenta de usuario existente, lo que incluye restablecer la contraseña del usuario.

1. Seleccione la vista **Administración**.

Aparecerá la pestaña **Usuarios** de la página Administración de usuarios.



The screenshot shows the 'Administración de usuarios' (User Management) interface. It features a sidebar with navigation icons and a main content area. The main area has tabs for 'Usuarios', 'Roles', and 'Grupos'. Below the tabs, there is a search bar, an 'Exportar' button, and a '+ Agregar usuario' button. A table displays user information with columns: 'Nombre de usuario', 'Nombre de pila', 'Apellido', 'Correo electrónico', 'Número de teléfono', 'Nombre de rol', 'Estado', 'Fecha de creación', 'Fecha de último inicio de sesión', and 'Creado mediante'. The table shows one user: 'saislead' (Sai Fu) with email 'sai@gogame.com'. Action buttons 'Editar', 'Asignar aplicaciones', 'Ver aplicaciones', and 'Eliminar' are visible for the user.

Nombre de usuario	Nombre de pila	Apellido	Correo electrónico	Número de teléfono	Nombre de rol	Estado	Fecha de creación	Fecha de último inicio de sesión	Creado mediante
saislead	Sai	Fu	sai@gogame.com		Líder en seguridad	Activo	22/10/2024	23/10/2024	

2. Haga clic en **Editar** en la fila del usuario que desea editar.

Se abrirá la ventana Agregar/Editar usuario.

Agregar/editar usuario

Nombre de usuario

Correo electrónico

Nombre de pila

Apellido

Número de teléfono

Rol

Líder en seguridad

Contraseña

Confirmar contraseña

☐ Se debe cambiar la próxima vez que inicie sesión

☒ La contraseña nunca caduca

☐ Inactivo

☐ Restablecer el código TOTP

Selecione los grupos a los que debe pertenecer el usuario.

	Nombre del grupo	Usuarios asignados
☐	Grupo	4

Guardar

Cancelar

- Edite los campos según sea necesario. Los siguientes campos se usan para restablecer la contraseña de un usuario.

4.

Campo	Descripción
Contraseña	Escriba una nueva contraseña para el usuario. La contraseña debe cumplir con los requisitos de complejidad.
Confirmar contraseña	Vuelva a escribir la misma contraseña.
Se debe cambiar la próxima vez que inicie sesión	Marque la casilla si desea que el usuario cambie la contraseña de la cuenta la próxima vez que inicie sesión.
La contraseña nunca caduca	Seleccione la casilla de verificación si no desea que la contraseña de la cuenta de usuario caduque.
Inactivo	Seleccione la casilla de verificación si desea que el usuario esté inactivo.
Restablecer el código TOTP	Seleccione la casilla de verificación para restablecer el código TOTP para el usuario en particular.

5. Haga clic en **Guardar**.

Se guardarán los cambios aplicados a los usuarios.

1.8.2.2.4. Administración de la asignación de aplicaciones a un usuario

Los usuarios con el permiso **Administrar usuarios** pueden administrar el acceso a las aplicaciones de un usuario desde la vista Administración.

Para administrar el acceso a las aplicaciones de un usuario:

1. Seleccione la vista **Administración**.

Aparecerá la pestaña **Usuario** de la página Administración de usuarios.



Administración de usuarios										
Usuarios Roles Grupos										
Texto de búsqueda										Exportar
1 encontrado										Mostrar: 25 50 100
seleccionar todo										
	Nombre de usuario	Nombre de pila	Apellido	Correo electrónico	Número de teléfono	Nombre de rol	Estado	Fecha de creación	Fecha de último inicio de sesión	Creado mediante
☐	saislead	Sai	Fu	sai@gogame.com		Líder en seguridad	Activo	22/10/2024	23/10/2024	
										Editar Asignar aplicaciones Ver aplicaciones Eliminar

2. Haga clic en **Asignar aplicaciones** en la fila del usuario del que desea editar el acceso a las aplicaciones.

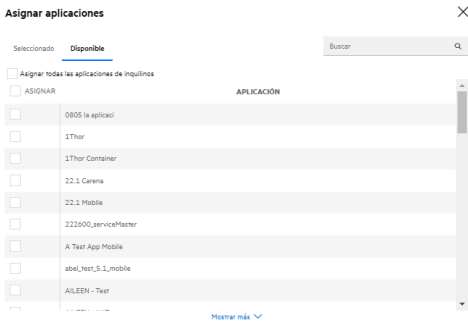
Aparece la ventana Asignar aplicación.

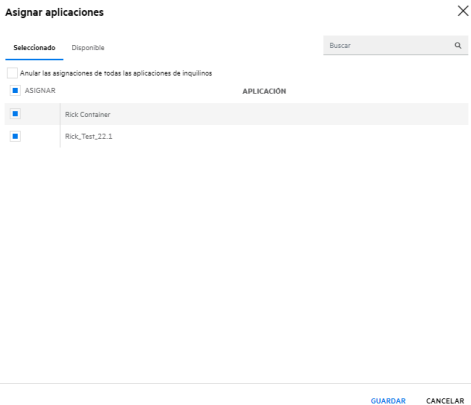


Note

El vínculo no está disponible si a un usuario se le asigna un rol con el permiso **Acceso a todas las aplicaciones**.

3. Puede realizar las siguientes tareas:

Tarea	Procedimiento
Asignar aplicaciones al usuario	Seleccione la pestaña Disponible.  Realice las siguientes acciones para seleccionar aplicaciones: ■ Marque la casilla de verificación junto a las aplicaciones individuales. ■ Marque la casilla de verificación ASIGNAR para seleccionar las aplicaciones mostradas. ■ Marque la casilla de verificación Asignar todas las aplicaciones de inquilinos para seleccionar todas las aplicaciones. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones.

Tarea	Procedimiento
Quitar las aplicaciones del usuario	- Haga clic en Asignar aplicaciones. - Seleccione la pestaña Seleccionados.  - Realice las siguientes acciones para eliminar aplicaciones: - Desactive la casilla de verificación junto a las aplicaciones individuales. - Desactive la casilla de verificación ASIGNAR para eliminar las aplicaciones mostradas. - Seleccione la casilla de verificación Anular las asignaciones de todas las aplicaciones de inquilinos para eliminar todas las aplicaciones. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones.

4. Haga clic en **Guardar**.

Se guardan los cambios aplicados a las aplicaciones asignadas del usuario.

Temas relacionados

Para administrar el acceso de los usuarios a las aplicaciones a nivel de aplicación, consulte [Administrar la asignación de usuarios para una aplicación](#).

1.8.2.2.5. Eliminación de una cuenta de usuario

Para eliminar una cuenta de usuario:

1. Seleccione la vista **Administración**.

Aparecerá la pestaña **Usuarios** de la página Administración de usuarios.



The screenshot shows the 'Administración de usuarios' interface. It has a sidebar with icons for users, roles, and groups. The main area has tabs for 'Usuarios', 'Roles', and 'Grupos'. Below the tabs, there's a search bar and a '+ Agregar usuario' button. A table lists users with columns: Nombre de usuario, Nombre de pila, Apellido, Correo electrónico, Número de teléfono, Nombre de rol, Estado, Fecha de creación, Fecha de último inicio de sesión, and Creado mediante. One user is listed: 'saislead' with email 'sai@gogame.com' and role 'Líder en seguridad'. Action buttons 'Editar', 'Asignar aplicaciones', 'Ver aplicaciones', and 'Eliminar' are at the end of the row.

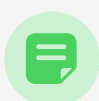
Nombre de usuario	Nombre de pila	Apellido	Correo electrónico	Número de teléfono	Nombre de rol	Estado	Fecha de creación	Fecha de último inicio de sesión	Creado mediante
saislead	Sai	Fu	sai@gogame.com		Líder en seguridad	Activo	22/10/2024	23/10/2024	

2. Haga clic en **Eliminar** en la fila del usuario que desea eliminar.

Aparecerá un mensaje de confirmación.

3. Haga clic en **Sí**.

El usuario se eliminará.



Note

Cuando se elimina un usuario, se quitan las instancias de nombre de usuario, nombre completo, dirección de correo electrónico y número de teléfono (excepto cuando sean necesarias para mantener la integridad referencial) y se sustituyen por un identificador de usuario único.

1.8.2.3. Grupos

Los usuarios se pueden ordenar en grupos a los que pueden asignarse aplicaciones. Esto permite agilizar la asignación de aplicaciones. Los grupos pueden diseñarse en torno a grupos empresariales, regiones y otras estructuras organizativas.

Esta sección aborda los siguientes temas:

- [Visualización de grupos](#)
- [Creación de un grupo](#)
- [Edición de un grupo](#)
- [Administrar la asignación de aplicaciones para un grupo](#)
- [Eliminación de un grupo](#)

1.8.2.3.1. Visualización de grupos

Realice lo siguiente para ver los grupos en el inquilino:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Seleccione la pestaña **Grupos**.



Administración de usuarios			
Usuarios	Roles	Grupos	
20 encontrados		Mostrar: 25 50 100	
NOMBRE DEL GRUPO	USUARIOS ASIGNADOS	APLICACIONES ASIGNADAS	
19.2	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR
1test	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR

En la siguiente tabla se describe cómo desplazarse por la pestaña **Grupos**.

Tarea	Acción
Buscar en la lista de grupos	Escriba una palabra clave o una frase en el campo de búsqueda y pulse Intro . Para quitar los resultados de búsqueda, elimine el texto del campo de búsqueda y pulse Intro .
Exportar datos como archivo .csv	Haga clic en Exportar . Un archivo CSV que contiene detalles sobre los grupos de usuarios se guarda en una carpeta local especificada en la configuración del navegador.
Agregar un grupo	Haga clic en Agregar grupo . Para obtener más información, consulte Creación de un grupo .
Editar el nombre de un grupo y los usuarios asignados	Haga clic en Editar en la columna de acciones. Para obtener más información, consulte Edición de un grupo .
Asignar y cancelar la asignación de aplicaciones	Haga clic en Asignar aplicaciones en la columna de acciones. Para obtener más información, consulte Administrar la asignación de aplicaciones para un grupo .
Eliminar un grupo	Haga clic en Eliminar en la columna de acciones. Para obtener más información, consulte Eliminar un grupo .

1.8.2.3.2. Creación de un grupo

Realice lo siguiente para crear un grupo:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Seleccione la pestaña **Grupos**.

Administración de usuarios

Usuarios

Roles

Grupos

?

Texto de búsqueda

Q

EXPORTAR

+ AGREGAR GRUPO

20 encontrados

Mostrar: 2550100

NOMBRE DEL GRUPO	USUARIOS ASIGNADOS	APLICACIONES ASIGNADAS	
19.2	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR
1test	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR

3. Haga clic en **+Agregar grupo**.

Aparece la ventana Agregar/editar grupo.

Agregar/editar grupo ?



Nombre del grupo

Descripción del grupo

Seleccionado **Disponible**



AssignmentControl

☐ Asignar todos los usuarios de inquilinos

☐ ASIGNAR

APELLIDO

NOMBRE

CORREO ELECTRÓNICO

NOMBRE DEL ROL

☐	DaBaer	Brown	brownd@fod.com	Test
☐	Huang	julie	julieh@fod.com	Desarrollador principal
☐	Smith	James	james@fod.com	Líder en aplicaciones

4. En el campo **Nombre del grupo**, especifique el nombre del grupo.
5. En el campo **Descripción del grupo**, especifique una descripción del grupo (opcional).
6. Puede realizar las siguientes acciones para seleccionar aplicaciones:
 - Marque las casillas situadas junto a cada usuario.

- Seleccione la casilla de verificación **ASIGNAR** para seleccionar los usuarios mostrados.
- Marque la casilla **Asignar todas las aplicaciones de inquilinos** para seleccionar todos los usuarios.

7. Haga clic en **Guardar**.

El nuevo grupo aparecerá en la lista de grupos.

1.8.2.3.3. Edición de un grupo

Para editar un nombre de grupo y administrar la asignación de usuarios para un grupo:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Seleccione la pestaña **Grupos**.

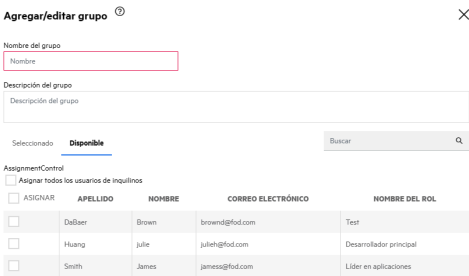


Administración de usuarios			
Usuarios	Roles	Grupos	
20 encontrados		Mostrar: 25 50 100	
NOMBRE DEL GRUPO	USUARIOS ASIGNADOS	APLICACIONES ASIGNADAS	
19.2	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR
1test	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR

3. Haga clic en **Editar** en la fila del grupo que desea editar.

Se abre la ventana Agregar/editar grupo.

4. Puede realizar las siguientes tareas:

Tarea	Procedimiento
Editar el nombre del grupo	En el campo Nombre del grupo , escriba el nuevo nombre del grupo.
Asignar usuarios al grupo	1. Seleccione la pestaña Disponible.  2. Realice las siguientes acciones para seleccionar aplicaciones: ■ Marque las casillas situadas junto a cada usuario. ■ Seleccione la casilla de verificación ASIGNAR para seleccionar los usuarios mostrados. ■ Marque la casilla Asignar todos los usuarios de inquilinos para seleccionar todos los usuarios. Puede usar el campo de búsqueda para filtrar la lista de usuarios.

Tarea	Procedimiento
Anular la asignación de usuarios del grupo	1. Seleccione la pestaña Seleccionados.  2. Realice las siguientes acciones para quitar usuarios: ■ Desactive la casilla de verificación situada junto a cada usuario. ■ Desactive la casilla de verificación ASIGNAR para quitar los usuarios mostrados. ■ Seleccione la casilla de verificación Anular las asignaciones de todos los usuarios de inquilinos para quitar todos los usuarios. Puede usar el campo de búsqueda para filtrar la lista de usuarios.

5. Haga clic en **Guardar**.

Se guardarán los cambios aplicados en el grupo.

1.8.2.3.4. Administrar la asignación de aplicaciones para un grupo

Los usuarios con el permiso **Administrar usuarios** pueden administrar la asignación de aplicaciones para un grupo desde la vista Administración.

Para administrar la asignación de aplicaciones para un grupo:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Seleccione la pestaña **Grupos**.



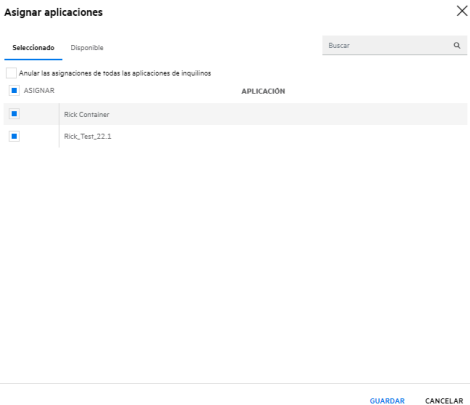
Administración de usuarios			
Usuarios	Roles	Grupos	
20 encontrados		Mostrar: 25 50 100	
NOMBRE DEL GRUPO	USUARIOS ASIGNADOS	APLICACIONES ASIGNADAS	
19.2	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR
1test	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR

3. Haga clic en **Asignar aplicaciones** en la fila del grupo al que desea asignar las aplicaciones.

Se abre la ventana Asignar aplicaciones.

4. Puede realizar las siguientes tareas:

Tarea	Procedimiento
Asignar aplicaciones al grupo	1. Haga clic en Asignar aplicaciones. 2. Seleccione la pestaña Disponible. 3. Realice las siguientes acciones para seleccionar aplicaciones: ▪ Marque la casilla de verificación junto a las aplicaciones individuales. ▪ Marque la casilla de verificación ASIGNAR para seleccionar las aplicaciones mostradas. ▪ Marque la casilla de verificación Asignar todas las aplicaciones de inquilinos para seleccionar todas las aplicaciones. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones. 4. Haga clic en Guardar.

Tarea	Procedimiento
Cancelar la asignación de aplicaciones del grupo	- Haga clic en Asignar aplicaciones. - Seleccione la pestaña Seleccionados.  - Realice las siguientes acciones para eliminar aplicaciones: - Desactive la casilla de verificación junto a las aplicaciones individuales. - Desactive la casilla de verificación ASIGNAR para eliminar las aplicaciones mostradas. - Seleccione la casilla de verificación Anular las asignaciones de todas las aplicaciones de inquilinos para eliminar todas las aplicaciones. Puede usar el campo de búsqueda para filtrar la lista de aplicaciones. - Haga clic en Guardar.

5. Haga clic en **Guardar**.

Se guardan los cambios aplicados a las aplicaciones asignadas del grupo.

Temas relacionados:

Para obtener más información acerca de cómo asignar varios grupos a la vez, consulte Edición múltiple de grupos desde la página Aplicaciones.

1.8.2.3.5. Eliminación de un grupo

Realice lo siguiente para eliminar un grupo:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Seleccione la pestaña **Grupos**.



Administración de usuarios			
Usuarios	Roles	Grupos	
20 encontrados			Mostrar: 25 50 100
NOMBRE DEL GRUPO	USUARIOS ASIGNADOS	APLICACIONES ASIGNADAS	
19.2	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR
1test	4	3	EDITAR ASIGNAR APLICACIONES ELIMINAR

3. Haga clic en **Eliminar** en la fila del grupo que desea eliminar.

Aparecerá un mensaje de confirmación.

4. Haga clic en **Sí**.

El grupo se eliminará.

1.8.3. Administración de directivas

Los líderes en seguridad pueden configurar el modo en que se aplican las directivas de seguridad a las aplicaciones de un inquilino. También pueden crear y administrar directivas de seguridad personalizadas.

Esta sección aborda los siguientes temas:

- [Creación de una directiva de seguridad](#)
- [Configuración de la directiva de seguridad](#)
- [Eliminación de una directiva de seguridad](#)

1.8.3.1. Creación de una directiva de seguridad

Para crear una directiva de seguridad personalizada:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Administración de directivas**.

Aparecerá la pestaña **Ámbito** de la página Administración de directivas.

3. Seleccione la pestaña **Directivas**.



The screenshot shows the 'Administración de directivas' (Policy Administration) page. On the left is a sidebar with icons for navigation. The main header has a tab for 'Directivas' (Policies) and a '+ AGREGAR DIRECTIVA' (Add Policy) button. Below the header is a table with the following data:

NOMBRE DE DIRECTIVA	CLASIFICACIÓN POR ESTRELLAS	REQUISITOS DE CONFORMIDAD	
Business Criticality High	Al menos 4 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Business Criticality Low	Al menos 2 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Business Criticality Medium	Al menos 3 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Directiva predeterminada del sistema	Al menos 3 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Static Test	Al menos 3 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Test Policy	Al menos 2 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR

4. Haga clic en **+Agregar directiva**.

Aparecerá el asistente **Agregar/editar directiva**.

5. En la página Detalles de política, complete los campos y haga clic en **Siguiente**.

Agregar/editar directiva

- Detalles de directiva**
- Tipos de evaluación
- Servicios complementarios
- Versiones de desarrollo
- Versiones de QA/prueba
- Versiones de producción
- Resumen

Nombre de directiva

Clasificación por estrellas i

Al menos 3 estrellas

Requisitos de conformidad

Todas las categorías de vulnerabilidad

Atrás

Siguiente

Guardar

Campo	Descripción
Nombre de directiva	Escriba un nombre para la directiva.
Clasificación por estrellas	Seleccione la clasificación por estrellas mínima que debe recibir una aplicación para considerarla como aprobada. Para obtener información sobre las clasificaciones por estrellas, consulte Clasificación de la evaluación de cinco estrellas .
Requisitos de conformidad	Seleccione las vulnerabilidades que se incluyen al determinar el estado aprobado/suspenso de una aplicación. Puede conservar el valor predeterminado de todas las vulnerabilidades o solo incluir los problemas etiquetados con un requisito de conformidad concreto, como OWASP 2021 o PCI 3.2.  Note El estado aprobado/fallido incorpora problemas de código abierto.

- En la página Tipos de evaluación, seleccione los tipos de evaluación que están disponibles para las aplicaciones en las que se implementó la directiva. La opción **Permitir todos los tipos de evaluación** está seleccionada de manera predeterminada. Déjela seleccionada para que la directiva de seguridad permita todos los tipos de evaluación, incluidos aquellos agregados después de crear la directiva. Anule la selección de **Permitir todos los tipos de evaluación** para seleccionar individualmente los tipos de evaluación. Haga clic en **Siguiente**.

Agregar/editar directiva

✓ Detalles de política

Tipos de evaluación

Servicios complementarios

Versiones de desarrollo

Versiones de QA/prueba

Versiones de producción

Resumen

Tipos de evaluación permitidos

☒ Permitir todos los tipos de evaluación

Estático

☐ AugStatic: análisis único

☐ AugStatic: suscripción

☐ AUTO-STATIC: análisis único

☐ AUTO-STATIC: suscripción

☐ Auto-Static1715-20200409367: análisis único

☐ Auto-Static1715-20200409367: suscripción

☐ Auto-Static2355-20200409367: análisis único

☐ Auto-Static2355-20200409367: suscripción

☐ Auto-Static3183-20200409367: análisis único

☐ Auto-Static3183-20200409367: suscripción

☐ Auto-Static3669-2020041078: análisis único

☐ Auto-Static3669-2020041078: suscripción

Atrás

Siguiente

Guardar



Note

Si se actualiza la directiva de una aplicación que tiene una suscripción activa o una corrección disponible para un tipo de evaluación que la directiva actual no admite, la suscripción o la corrección estarán disponibles hasta que caduquen o se usen.

- En la página Servicios complementarios, seleccione los servicios complementarios que están disponibles para las aplicaciones en las que se implementó la directiva. Las restricciones no se aplican a las aplicaciones que tenían servicios complementarios habilitados antes de que se aplicara una política.

Agregar/editar directiva
×

✓ Detalles de política

✓ Tipos de evaluación

Servicios complementarios

Versiones de desarrollo

Versiones de QA/prueba

Versiones de producción

Resumen

Servicios complementarios

☒ Permitir Fortify Aviator
 ☐ Permitir complementos de DAST automatizada

(Incluye grabación de macros con inicio de sesión único y revisión de resultados por parte de expertos)

Atrás

Siguiente

Guardar

Campo	Descripción
Permitir SAST Aviator	Permitir la selección de SAST Aviator en la configuración del análisis. Esta opción está seleccionada de forma predeterminada si se ha habilitado SAST Aviator para el inquilino; si no es así, la opción no está habilitada.  Note Si SAST Aviator se ejecutó en un análisis antes de que se aplicara una restricción de política, la configuración del análisis de la aplicación seguirá permitiendo la selección de SAST Aviator.
Permitir complementos de DAST automatizada	Permitir la selección de complementos de DAST automatizada en la configuración del análisis. Esta opción está seleccionada de forma predeterminada si las evaluaciones de DAST automatizada están habilitadas para el inquilino; si no es así, la opción no está habilitada.

8. En la página Versiones de desarrollo, rellene los campos que correspondan a las versiones con el estado de desarrollo. Haga clic en **Siguiente**.

Agregar/editar directiva
✕

✓ Detalles de política
✓ Tipos de evaluación
✓ Servicios complementarios
Versiones de desarrollo
Versiones de QA/prueba
Versiones de producción
Resumen

Periodo de gracia de corrección (0-365 días)

Crítico
Días

Alto
Días

Frecuencia de análisis necesaria (0-365 días)

Estático
Días

Dinámico
Días

Móvil
Días

Atrás

Siguiente

Guardar

Campo	Descripción
Periodo de gracia de corrección (0-365 días)	Especifique el periodo de gracia de corrección del problema de cada nivel de gravedad de problemas. Cuando un problema en una versión de Desarrollo se encuentra en el periodo de gracia, este no afectará al estado aprobado/suspenso de la versión.  Note La clasificación por estrellas especificada anteriormente determina los niveles de gravedad de problemas que se muestran.
Frecuencia de análisis necesaria (0-365 días)	Especifique la frecuencia de análisis necesaria de cada tipo de análisis. Se producirá un error en una versión de Desarrollo si esta no completa un análisis durante el periodo designado del tipo de análisis. Un valor de 0 indica que no es preciso realizar el análisis.

9. En la página Versiones de QA/prueba, complete los campos que se apliquen a las versiones con el estado Control de calidad/Prueba. Haga clic en **Siguiente**.

Agregar/editar directiva

✓ Detalles de política
✓ Tipos de evaluación
✓ Servicios complementarios
✓ Versiones de desarrollo
Versiones de QA/prueba
Versiones de producción
Resumen

Periodo de gracia de corrección (0-365 días)

Crítico

0

Días

Alto

0

Días

Frecuencia de análisis necesaria (0-365 días)

Estático

0

Días

Dinámico

0

Días

Móvil

0

Días

Atrás

Siguiente

Guardar

Campo	Descripción
Periodo de gracia de corrección (0-365 días)	Especifique el periodo de gracia de corrección del problema de cada nivel de gravedad de problemas. Cuando un problema en una versión de Control de calidad/Prueba se encuentra en el periodo de gracia, este no afectará al estado aprobado/suspenso de la versión.  Note La clasificación por estrellas especificada anteriormente determina los niveles de gravedad de problemas que se muestran.
Frecuencia de análisis necesaria (0-365 días)	Especifique la frecuencia de análisis necesaria de cada tipo de análisis. Se producirá un error en una versión de Control de calidad/Prueba si esta no completa un análisis durante el periodo designado del tipo de análisis. Un valor de 0 indica que no es preciso realizar el análisis.

10. En la página Versiones de producción, complete los campos que se apliquen a las versiones con el estado Producción. Haga clic en **Siguiente**.

Agregar/editar directiva

- ✓ Detalles de política
- ✓ Tipos de evaluación
- ✓ Servicios complementarios
- ✓ Versiones de desarrollo
- ✓ Versiones de QA/prueba
- Versiones de producción**
- Resumen

Periodo de gracia de corrección (0-365 días)

Crítico

0

Días

Alto

0

Días

Frecuencia de análisis necesaria (0-365 días)

Estático

0

Días

Dinámico

0

Días

Móvil

0

Días

Atrás

Siguiente

Guardar

Campo	Descripción
Periodo de gracia de corrección (0-365 días)	Especifique el periodo de gracia de corrección del problema de cada nivel de gravedad de problemas. Cuando un problema en una versión de Producción se encuentra en el periodo de gracia, este no afectará al estado aprobado/suspenso de la versión.  Note La clasificación por estrellas especificada anteriormente determina los niveles de gravedad de problemas que se muestran.
Frecuencia de análisis necesaria (0-365 días)	Especifique la frecuencia de análisis necesaria de cada tipo de análisis. Se producirá un error en una versión de Producción si esta no completa un análisis durante el periodo designado del tipo de análisis. Un valor de 0 indica que no es preciso realizar el análisis.

11. En la página Resumen, revise los ajustes de directiva. Haga clic en **Guardar**.

Agregar/editar directiva

✓ Detalles de política
✓ Tipos de evaluación
✓ Servicios complementarios
✓ Versiones de desarrollo
✓ Versiones de QA/prueba
✓ Versiones de producción
Resumen

Detalles de política

Nombre de directiva
Nueva directiva

Clasificación por estrellas
Al menos 3 estrellas

Requisitos de conformidad
Todas las categorías de vulnerabilidad

Supervisión de aplicaciones
No necesario

Tipos de evaluación

Permitir todos los tipos de evaluación

Servicios complementarios

Permitir Fortify Aviator

Versiones de desarrollo

Periodo de gracia de corrección
Crítico: 0 días
Alto: 0 días

Frecuencia de análisis necesaria
Estático: ninguno
Dinámico: ninguno
Móvil: ninguno

Versiones de QA/prueba

Periodo de gracia de corrección
Crítico: 0 días
Alto: 0 días

Frecuencia de análisis necesaria
Estático: ninguno
Dinámico: ninguno
Móvil: ninguno

Versiones de producción

Periodo de gracia de corrección
Crítico: 0 días
Alto: 0 días

Frecuencia de análisis necesaria
Estático: ninguno
Dinámico: ninguno
Móvil: ninguno

Atrás
Siguiente
Guardar

La nueva directiva aparece en la pestaña **Directivas**.

Temas relacionados:

- Para obtener información sobre cómo reemplazar manualmente la configuración de aprobado/suspensión, consulte [Reemplazo de la directiva de seguridad de una versión](#).

This PDF was generated on February 12, 2026

Page 632 of 784

1.8.3.2. Configuración de la directiva de seguridad

Siga los siguientes pasos para configurar la directiva de seguridad del inquilino:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Haga clic en **Administración de directivas**.

Aparecerá la pestaña **Asignación de directivas** de la página **Administración de directivas**.

3. Haga clic en **Editar**.

Se abrirá la ventana modal **Editar ámbito de asignación**.

Editar ámbito de asignación



Ámbito

GUARDAR

CANCELAR

4. Seleccione el ámbito para determinar cómo se aplican las directivas en la lista **Ámbito**. Solo se puede aplicar un ámbito por inquilino. Los valores disponibles son los siguientes:

- **Importancia para el negocio:** agrupa las aplicaciones según su nivel asignado de Importancia para el negocio. Para obtener más información sobre los niveles de importancia para el negocio, consulte [Creación de una aplicación](#).
- **Tipo de aplicación:** agrupa las aplicaciones como web/cliente pesado o móvil.
- **Atributo de aplicación:** agrupa las aplicaciones según los valores del atributo de aplicación que se seleccionó de la lista **Atributo**. Este valor no es válido si no se crea ningún atributo de aplicación en el inquilino.



Note

La selección se limita a atributos de tipo de lista de selección que tienen diez valores o menos.

5. Haga clic en **Guardar**.

Volverá a la pestaña **Ámbito**.

6. Seleccione la directiva que se asignará a cada valor del ámbito seleccionado.

7. Haga clic en **Guardar**.

Se guardará la configuración de la directiva de seguridad.

1.8.3.3. Eliminación de una directiva de seguridad

Puede eliminar una directiva de seguridad personalizada que no se use actualmente. La directiva predeterminada de OpenText Core Application Security se puede editar, pero no se puede eliminar.

Siga los siguientes pasos para eliminar una directiva de seguridad personalizada:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Administración de directivas**.

Aparecerá la pestaña **Ámbito** de la página Administración de directivas.

3. Seleccione la pestaña **Directivas**.



Administración de directivas			
Asignación de directivas		Directivas	+ AGREGAR DIRECTIVA
NOMBRE DE DIRECTIVA	CLASIFICACIÓN POR ESTRELLAS	REQUISITOS DE CONFORMIDAD	
Business Criticality High	Al menos 4 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Business Criticality Low	Al menos 2 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Business Criticality Medium	Al menos 3 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Directiva predeterminada del sistema	Al menos 3 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Static Test	Al menos 3 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR
Test Policy	Al menos 2 estrellas	Todas las categorías de vulnerabilidad	EDITAR ELIMINAR

4. Haga clic en **Eliminar** en la fila de la directiva que desee eliminar.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí**.

La directiva se eliminará.

1.8.4. Registro único (SSO)

El registro único (SSO) elimina la necesidad de mantener credenciales separadas para OpenText Core Application Security y permite que los administradores gestionen fácilmente el acceso de los usuarios y el aprovisionamiento. OpenText Core Application Security admite la integración de SSO con proveedores de identidad existentes mediante el estándar SAML 2.0 para identidad federada.

OpenText Core Application Security admite las siguientes vinculaciones de SAML 2.0:

- Vinculaciones POST y Redirect de solicitudes de autenticación de SAML de OpenText Core Application Security al proveedor de identidad.
- Vinculación POST de respuestas de aserción de SAML del proveedor de identidad a OpenText Core Application Security.

Los líderes en seguridad pueden configurar SSO para el inquilino. La configuración de SSO incluye las siguientes tareas:

- Configurar SSO en OpenText Core Application Security. Para obtener instrucciones, consulte [Configurar SSO en OpenText Core Application Security](#).
- Adición de los metadatos del proveedor de identidad a OpenText Core Application Security. Para obtener instrucciones, consulte [Adición de los metadatos del proveedor de identidades](#).
- Configuración del cifrado en OpenText Core Application Security. Para obtener instrucciones, consulte [Configuración del cifrado](#).
- Descarga de los metadatos de OpenText Core Application Security. Para obtener instrucciones, consulte [Descarga de los metadatos de OpenText Core Application Security](#).
- Configuración SSO en su proveedor de identidad. Para obtener instrucciones, consulte [Configuración SSO en el proveedor de identidad](#).

1.8.4.1. Configurar SSO en OpenText Core Application Security

Ajuste la configuración de SSO de OpenText Core Application Security y asigne los nombres de atributo de OpenText Core Application Security a los nombres de atributo del proveedor de identidad.

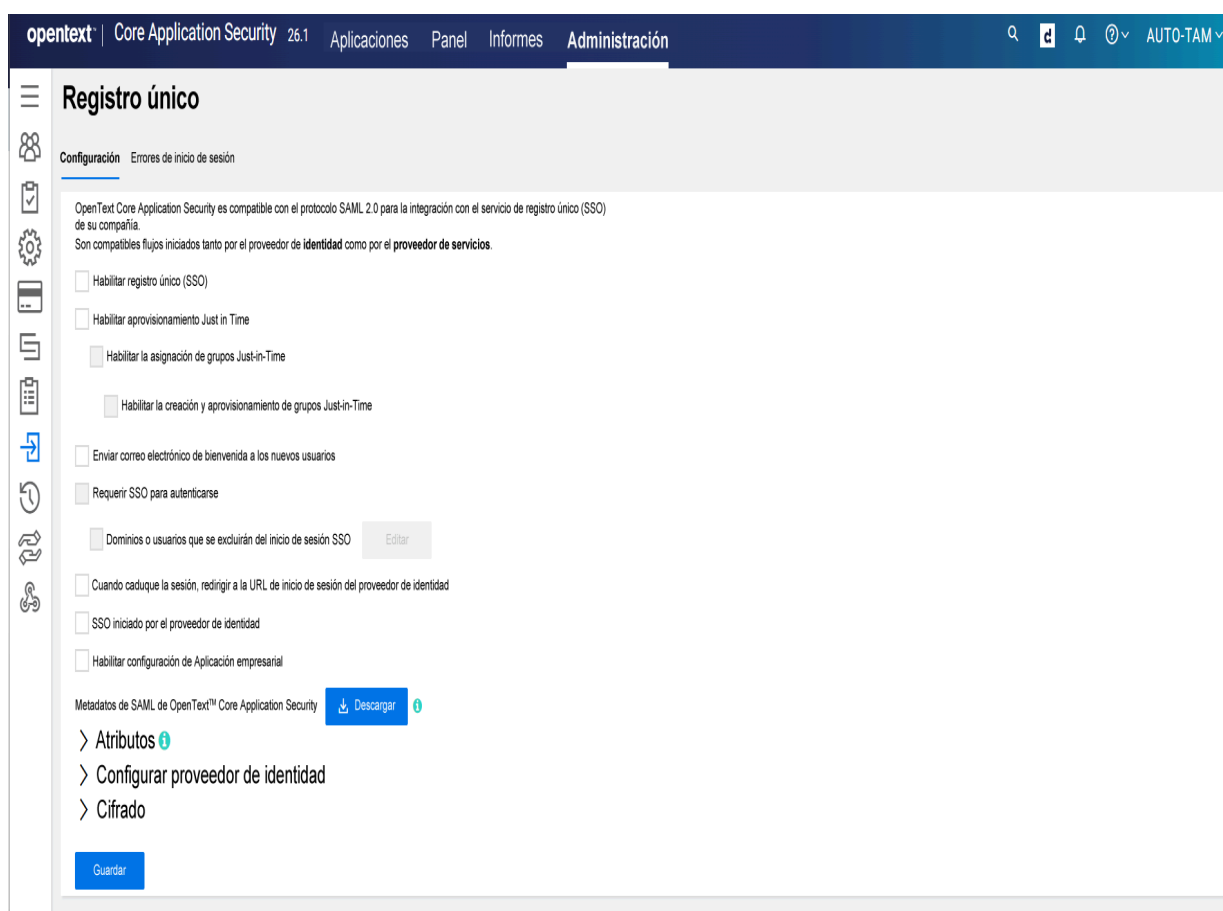
Para ajustar la configuración de SSO de OpenText Core Application Security:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Registro único**.

Aparece la página Registro único.



3. Seleccione las casillas de verificación que desee:

Campo	Descripción	
Habilitar registro único (SSO)	Esta opción habilita el SSO.	
Habilitar aprovisionamiento Just in Time	Esta opción permite la creación o la actualización automática de cuentas de usuario de OpenText Core Application Security para usuarios que se autentican mediante su proveedor de identidad.	
Habilitar la asignación de grupos Just in Time	Habilitar aprovisionamiento Just in Time debe estar seleccionado. Esta opción permite la actualización automática de las asignaciones de grupos de usuarios de OpenText Core Application Security a través de su proveedor de identidad.	

Campo	Descripción	
Habilitar la creación y el aprovisionamiento de grupos Just-in-Time	Habilitar aprovisionamiento Just in Time y Habilitar asignación de grupos Just in Time. Esta opción permite la creación automática de grupos de usuarios de OpenText Core Application Security a través de su proveedor de identidad.	
Enviar correo electrónico de bienvenida a los nuevos usuarios	Los nuevos usuarios que se creen a través del portal recibirán un correo electrónico de bienvenida. No obstante, este mensaje incluye instrucciones de configuración de contraseña que no se aplican a los usuarios que se autentican mediante SSO. Si no se selecciona esta opción, los correos electrónicos de bienvenida no se enviarán a los nuevos usuarios.	

Campo	Descripción	
Requerir SSO para autenticarse	Esta opción requiere que todos los usuarios usen SSO. Si no se selecciona esta opción, puede que los usuarios inicien sesión en OpenText Core Application Security mediante autenticación SSO o con el nombre de usuario y la contraseña en la página de inicio de sesión estándar.	

Campo	Descripción	
	 Note Si se habilita esta opción, no se podrán usar ciertos clientes e integraciones especializadas que emplean la API web de OpenText Core Application Security debido a que dicha API web tiene compatibilidad limitada con los tokens de autenticación de SAML. Por ejemplo, el cliente iOS requiere credenciales que no sean de SSO para	

Campo	Descripción	
	conectarse a OpenText Core Application Security. El enfoque recomendado en este caso consiste en generar una contraseña segura y aleatoria (32 caracteres como mínimo) que se pueda usar como "token de acceso personal" para la autenticación que no es de SSO. ◦ Dominios o usuarios que se excluirán del inicio de sesión SSO: Esta opción le permite agregar la lista de dominios o usuarios que se	

Campo	Descripción	
	excluirán del inicio de sesión SSO. Haga clic Editar para especificar los nombres de dominio o los Id. de correo electrónico que se excluirán del inicio de sesión SSO. Una vez agregados los nombres de dominio o los Id. de correo electrónico, haga clic en Guardar para guardar los cambios.  Note Esta opción está deshabilitada cuando Requerir SSO para autenticars e no está seleccionado	

Campo	Descripción	
Cuando caduque la sesión, redirigir a la URL de inicio de sesión del proveedor de identidad	Esta opción tiene usuarios redirigidos a su página de inicio de sesión del proveedor de identidad después de que la sesión caduque o cuando los usuarios cierran sesión. Esta función requiere que las cookies estén habilitadas en el navegador y que un usuario haya iniciado sesión en los últimos 30 días.	

Campo	Descripción	
SSO iniciado por el proveedor de identidad	Se admiten flujos de autenticación SAML iniciados por el proveedor de servicios y por el proveedor de identidad. ◦ (Recomendado) Si esta opción no está seleccionada, se utiliza el flujo del proveedor de servicios. Los usuarios iniciarán sesión en OpenText Core Application Security mediante la URL de inicio de sesión de SSO proporcionada en esta página. A continuación, OpenText Core Application Security enviará una solicitud iniciada por el proveedor de servicios al proveedor de identidad para autenticar el usuario. ◦ Si se selecciona esta opción, se usará el flujo iniciado por el	

Campo	Descripción	
	proveedor de identidad. Los usuarios iniciarán sesión conectándose directamente al proveedor de identidad y se los redirigirá a OpenText Core Application Security cuando la autenticación se realice correctamente.	

Campo	Descripción	
Habilitar configuración de Aplicación empresarial	Si su organización tiene varios inquilinos, esta opción permite la autenticación a través de un único proveedor de identidad.	

Campo	Descripción	
	 Note Si selecciona esta opción y tiene una configuración de SSO existente, deberá descargar los metadatos OpenText Core Application Security actualizados, importarlos al proveedor de identidad y volver a importar los metadatos del proveedor de identidad a OpenText Core Application Security. Como alternativa,	

Campo	Descripción	
	puede agregar ? t= <sso_login_url_guid> tanto al Nombre del proveedor de identidad en la configuración de SSO OpenText Core Application Security como al nombre del proveedor de servicios en la configuración del proveedor de identidad, donde <sso_login_url_guid> es un identificador único encontrado en la URL de inicio de	

Campo	Descripción	
	sesión de SSO.	

4. En la sección **Atributos**, asigne los nombres de atributo esperados por OpenText Core Application Security a los que se configuraron en el proveedor de identidad. Cada nombre de atributo que se defina aquí deberá coincidir con el valor exacto de **Nombre** del atributo usado por el proveedor de identidad, y se suele definir como una URL de esquema completa. Algunos proveedores de identidad también envían un valor **Nombre descriptivo** más corto para el atributo, que también se puede usar en la asignación de atributos. Para obtener las descripciones de los atributos, consulte [Configuración del proveedor de identidades](#).

Atributos

Atributo	Nombre
Nombre de usuario	
Nombre	
Apellido	
Correo electrónico	
Número de teléfono móvil	
Grupos	
Rol	

☐ Habilitar asignación personalizada de líder en seguridad

Asignación personalizada

5. Seleccione **Habilitar asignación personalizada de líder en seguridad** para asignar un valor personalizado (en lugar de un valor "Líder en seguridad" predeterminado) al rol Líder en seguridad en una aserción SAML. Escriba ese valor en el campo **Asignación personalizada**. Tenga en cuenta que esto anula la

validez del valor "Líder en seguridad" predeterminado empleado para la asignación.

6. Haga clic en **Guardar**.

Se guarda su configuración de SSO.

1.8.4.2. Adición de los metadatos del proveedor de identidades

Para agregar los metadatos del proveedor de identidad, impórtelos en OpenText Core Application Security o configúrelos manualmente.

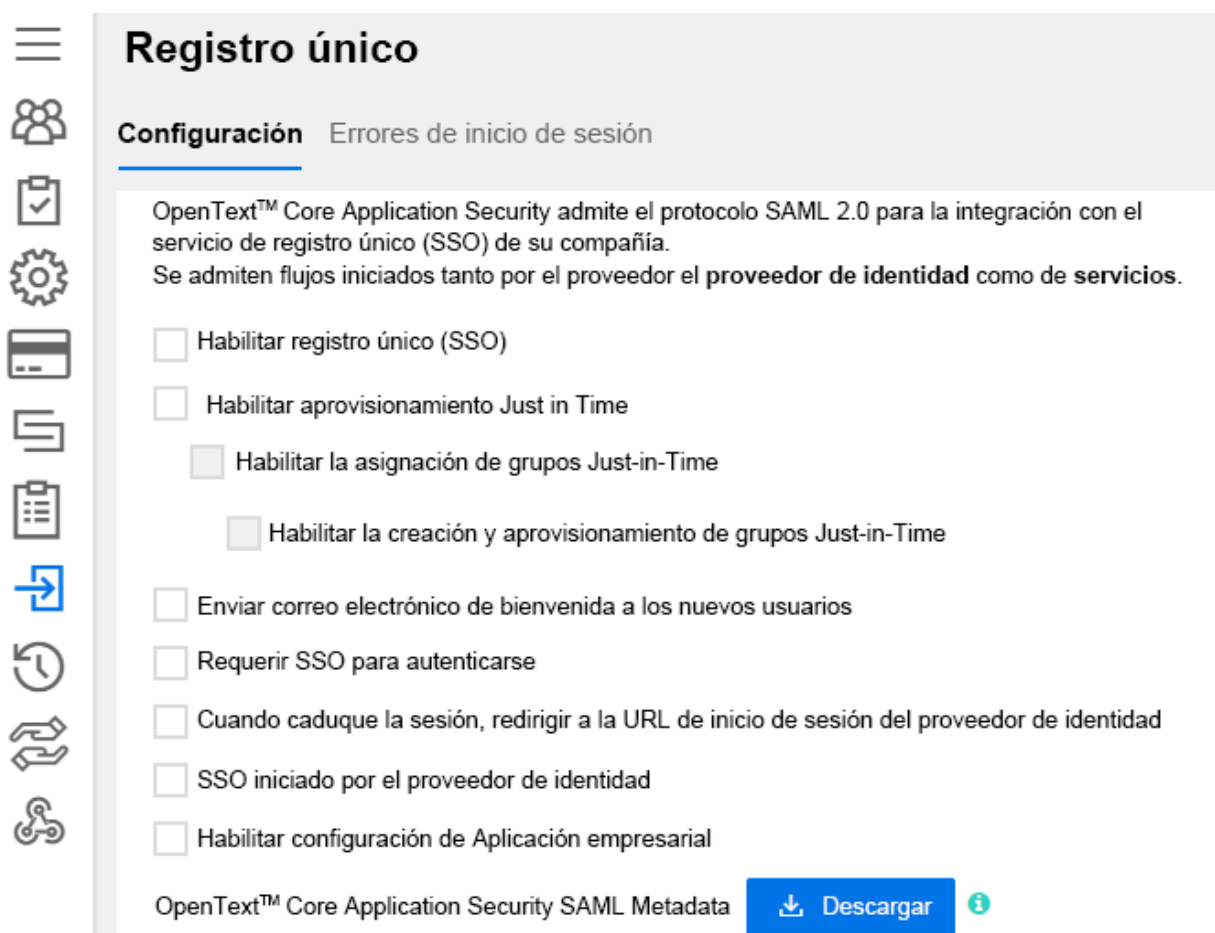
Para agregar los metadatos del proveedor de identidad:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Registro único**.

Aparece la página Registro único.



Registro único

Configuración Errores de inicio de sesión

OpenText™ Core Application Security admite el protocolo SAML 2.0 para la integración con el servicio de registro único (SSO) de su compañía.
Se admiten flujos iniciados tanto por el proveedor el **proveedor de identidad** como de **servicios**.

- ☐ Habilitar registro único (SSO)
- ☐ Habilitar aprovisionamiento Just in Time
 - ☐ Habilitar la asignación de grupos Just-in-Time
 - ☐ Habilitar la creación y aprovisionamiento de grupos Just-in-Time
- ☐ Enviar correo electrónico de bienvenida a los nuevos usuarios
- ☐ Requerir SSO para autenticarse
- ☐ Cuando caduque la sesión, redirigir a la URL de inicio de sesión del proveedor de identidad
- ☐ SSO iniciado por el proveedor de identidad
- ☐ Habilitar configuración de Aplicación empresarial

OpenText™ Core Application Security SAML Metadata [Descargar](#) ⓘ

3. En la sección **Configurar proveedor de identidad**, seleccione el método de adición de los metadatos del proveedor de identidad:

Configurar proveedor de identidad

☒ Importar metadatos de proveedor de identidad

...

 IMPORTAR

☐ Editar manualmente

 ELIMINAR INFORMACIÓN DE PROVEEDOR DE IDENTIDAD

Nombre del proveedor de identidad

URL de inicio de sesión del proveedor de identidad

Vinculación de solicitud de autenticación

☐ Limitar a los valores compatibles con el proveedor de identidad

Algoritmo de firmado de petición SAML

☒ SHA-1 ☐ SHA-256

Certificado del proveedor de identidad

URL de inicio de sesión de SSO 

GUARDAR

- **Importar metadatos de proveedor de identidad**
- **Editar manualmente**

4. Siga las instrucciones correspondientes al método seleccionado.



Note

Una vez se haya configurado SSO, los usuarios tendrán que utilizar el vínculo del cuadro **URL de inicio de sesión SSO** para iniciar sesión en OpenText Core Application Security.

- Importar los metadatos del proveedor de identidad:
 1. Haga clic en el botón Examinar.
 2. Busque el archivo .xml y selecciónelo.
 3. Haga clic en **Importar**.
- Configurar manualmente los metadatos del proveedor de identidad:
 1. Rellene los campos con la información de su proveedor de identidad:
 - **Nombre del proveedor de identidad**
 - **URL de inicio de sesión del proveedor de identidad**
 - **Vinculación de solicitud de autenticación** (seleccione **Limitar a los valores compatibles con el proveedor de identidad** para usar las vinculaciones compatibles con el proveedor de identidad)
 - **Algoritmo de firma de la solicitud SAML**
 - **Certificado del proveedor de identidad**
 5. Haga clic en **Guardar**.

Los metadatos del proveedor de identidad se agregan a OpenText Core Application Security.

1.8.4.3. Configuración del cifrado

Configuración del cifrado para OpenText Core Application Security SSO.

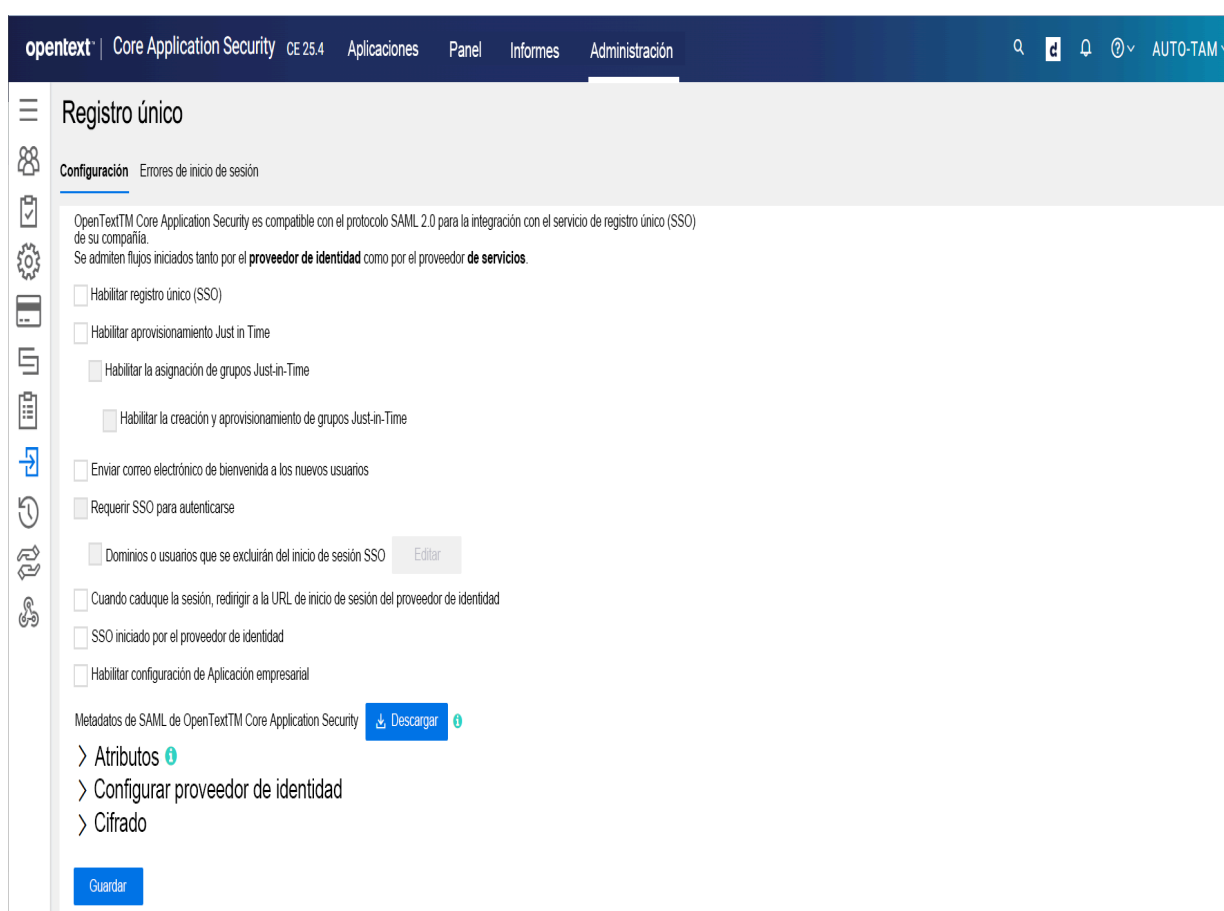
Para configurar el cifrado:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Registro único**.

Aparece la página Registro único.



3. En la sección **Cifrado**, seleccione la casilla de verificación **Habilitar cifrado** para agregar un nuevo certificado de cifrado.

▼ Cifrado

☒ **Habilitar cifrado** ⓘ

Si la casilla anterior está activada, descargue los metadatos SAML y vuelva a cargarlos en su IDP.

Actualmente no dispone de ningún certificado agregado. Añada un nuevo certificado.

[+ Agregar](#)

4. Para agregar un nuevo certificado, haga clic en **Agregar**. El certificado se crea con los siguientes detalles:

- Nombre del certificado
- Fecha de inicio del certificado
- Fecha de finalización del certificado



Note

- Cuando se configura el cifrado por primera vez, se muestra un certificado predeterminado de 1 año. Puede eliminar ese certificado y generar uno nuevo si es necesario.
- Si el cifrado está habilitado e intenta guardar la configuración SAML sin haber creado ningún certificado, se mostrará un mensaje de error.
- Cuando hay varios inquilinos dentro de Core Application Security que comparten el mismo proveedor de identidad, cada inquilino puede crear diferentes certificados de cifrado. Sin embargo, solo uno de estos certificados de cifrado se carga en el proveedor de identidad (IDP).
- Si el cifrado está habilitado para un inquilino, también afectará a todos los demás inquilinos que comparten el mismo proveedor de identidad (IDP). Por lo tanto, el cifrado también debe estar habilitado para todos esos inquilinos. Sin embargo, puede cargar el certificado de cualquier inquilino al IDP y el descifrado funcionará automáticamente para todos los demás inquilinos en Core Application Security.

✓ Cifrado

☒ Habilitar cifrado ⓘ

Si la casilla anterior está activada, descargue los metadatos SAML y vuelva a cargarlos en su IDP.

Nombre del certificado	Fecha de inicio del certificado	Fecha de finalización del certificado	Acción	
Certificado1	2025/06/25	2026/06/25	Descargar	Eliminar

1. Puede descargar un certificado válido como archivo .crt. Para descargar el certificado, haga clic en **Descargar**. No podrá descargar los

certificados caducados o que estén a punto de caducar. En tal escenario, también puede agregar un nuevo certificado.

☐ **Habilitar cifrado** ⓘ

Si la casilla anterior está activada, descargue los metadatos SAML y vuelva a cargarlos en su IDP.

Nombre del certificado	Fecha de inicio del certificado	Fecha de finalización del certificado	Acción	
Ficticio	2025/06/25	2025/06/24	Caducado	Eliminar

Su certificado ha caducado o está a punto de caducar. Añada un nuevo certificado.

[+ Agregar](#)

2. Para eliminar un certificado, haga clic en **Eliminar**.

5. Haga clic en **Guardar**.

Los detalles de cifrado se agregan a OpenText Core Application Security.



Note

Después de crear un certificado de cifrado SAML, este pasa a formar parte de los metadatos SAML. Además del certificado de firma, puede acceder al certificado de cifrado cuando descarga los metadatos SAML de Core Application Security.

1.8.4.4. Descarga de los metadatos de OpenText Core Application Security

Descargue el archivo de metadatos de OpenText Core Application Security a fin de facilitar la configuración del proveedor de identidad para que responda a las solicitudes de autenticación de OpenText Core Application Security. El archivo de metadatos incluye las URL de servicio de consumidor de aserción, el certificado de OpenText Core Application Security y el id. de entidad (también conocido como el nombre del proveedor de servicios).

Para descargar el archivo de metadatos de OpenText Core Application Security:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

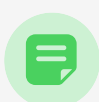
2. Haga clic en **Registro único**.

Aparece la página Registro único.



3. Haga clic en **Descargar**.

El archivo de metadatos se guarda en la carpeta local especificada en la configuración del navegador.



Note

Los metadatos también están disponibles como una URL para admitir la configuración en proveedores de identidad compatibles con la recuperación de metadatos automática. El acceso a los metadatos se realiza mediante la ruta absoluta "/SAML" del sitio del portal (por ejemplo, "https://ams.fortify.com/SAML"). La URL de metadatos no requiere autenticación, por lo que el proveedor de identidad puede acceder a ella sin proporcionar las credenciales de OpenText Core Application Security.

1.8.4.5. Configuración SSO en el proveedor de identidad

OpenText Core Application Security admite cualquier proveedor de identidad que cumpla las especificaciones de SAML 2.0 para flujos de autenticación basados en navegador. Siga estas instrucciones para configurar un proveedor de identidad para su uso con OpenText Core Application Security.

La información necesaria sobre el proveedor de servicios de OpenText Core Application Security se puede obtener de los metadatos de SAML, y muchos proveedores de identidad admiten la importación de metadatos para no tener que ajustar la configuración de forma manual.

Para configurar SSO en el proveedor de identidad:

1. Acepte las solicitudes de autenticación de OpenText Core Application Security.

El proveedor de identidad debe aceptar las solicitudes de autenticación enviadas desde el nombre del proveedor de servicios de OpenText Core Application Security. El nombre del proveedor de servicios es "https://<tenant_host>/SAML", donde <tenant_host> es su centro de datos (por ejemplo, "https://ams.fortify.com/SAML"). Podrá obtener el nombre del proveedor de servicios en los metadatos de SAML de OpenText Core Application Security.

OpenText Core Application Security firma todas las solicitudes de autenticación, por lo que quizá desee validar las firmas con el certificado de SAML proporcionado en los metadatos de SAML de OpenText Core Application Security.



Note

Antes de la versión 5.2, OpenText Core Application Security usaba un nombre de proveedor de servicios que no era compatible con algunos proveedores de identidad. Si configura la autenticación SSO en una versión anterior a la 5.2, puede conservar el nombre del proveedor de servicios "urn:fortify:FodServiceProvider" por motivos de compatibilidad con versiones anteriores con la configuración del proveedor de identidad existente. No obstante, se recomienda migrar el nuevo nombre del proveedor de servicios cuanto antes.

2. Firme todas las aserciones de SAML.

Todas las aserciones de SAML enviadas a OpenText Core Application Security deben firmarse mediante el certificado del proveedor de identidad especificado en la configuración de SSO de OpenText Core Application Security. OpenText Core Application Security acepta firmas de la respuesta de SAML completa o de la aserción que contiene la respuesta.



Note

OpenText Core Application Security no admite aserciones cifradas.

3. Asegúrese de que el reloj del sistema del proveedor de identidad se ha configurado correctamente, preferiblemente desde un servicio de origen de hora central como NIST.

La mayoría de las aserciones de SAML contienen un periodo de tiempo válido especificado por el proveedor de identidad. OpenText Core Application Security comprueba el periodo de tiempo con su reloj del sistema al recibir la aserción. OpenText Core Application Security permite una diferencia máxima de 3 minutos para tener en cuenta las diferencias en la configuración de los relojes. Si la aserción se recibe más de 3 minutos después de la hora de caducidad especificada en esta, se rechazará.

4. Configure la URL a la que el proveedor de identidad enviará la respuesta de aserción de SAML tras la autenticación de un usuario.

La URL se conoce como la URL de servicio de consumidor de aserción. Puede que se indique con otro término, como "URL de respuesta", según el proveedor de identidad. Puede obtener esta URL en los metadatos de SAML de OpenText Core Application Security.

5. Defina los atributos de reclamación de identidad que se incluirán en la aserción de SAML. OpenText Core Application Security usa los atributos de reclamación de la aserción de SAML para obtener información sobre el usuario autenticado.

Cada aserción debe contener un atributo de **nombre de usuario** que identifique al usuario en OpenText Core Application Security. Dicho valor debe ser exclusivo en OpenText Core Application Security, por lo que debería usar un identificador que fuera exclusivo de su organización, como una dirección de correo electrónico.



Note

Algunos sistemas usan el valor **Id. del nombre** en el elemento Asunto de la aserción de SAML para aprobar el identificador de usuario. OpenText Core Application Security no admite el uso del **Id. del nombre**, por lo que también deberá asignar un atributo para **Nombre de usuario**.

Los siguientes atributos se utilizan para el aprovisionamiento Just-In-Time (JIT). Los atributos son obligatorios para crear un nuevo usuario de OpenText Core Application Security. Cuando se actualiza un usuario de OpenText Core Application Security existente, todos los atributos son opcionales, y los valores existentes se conservan para los atributos no especificados.

Atributo	Necesario	Descripción
Correo electrónico	Sí	La dirección de correo electrónico del usuario. El valor puede ser igual que el valor Nombre de usuario, pero no es necesario. Puede asignar tanto Nombre de usuario como Correo electrónico al mismo atributo en la configuración de SSO de OpenText Core Application Security.
Nombre de pila	Sí	El nombre de pila del usuario.
Apellido	Sí	El apellido del usuario.
Número de teléfono móvil	No	El número de teléfono móvil del usuario.

Atributo	Necesario	Descripción
Rol	No	Rol de usuario. El valor debe ser una cadena de texto sin formato que coincida con el nombre de un rol en OpenText Core Application Security (no distingue mayúsculas de minúsculas). Si no se proporciona ningún valor, el rol Desarrollador se establece para un nuevo usuario. Si el valor no coincide con un nombre de rol, se devuelve un error.

Atributo	Necesario	Descripción
Grupo	No	Grupo de usuarios. El valor debe ser una cadena de texto sin formato (máximo 50 caracteres y no distingue entre mayúsculas y minúsculas). Si el valor no coincide con un grupo de usuarios existente en OpenText Core Application Security, el grupo de usuarios se creará si la opción SSO del portal Habilitar la creación y aprovisionamiento de grupos Just-in-Time está seleccionado.

Atributo	Necesario	Descripción
		 Note Si un usuario inicia sesión con SSO y el atributo Grupos está vacío en la aserción de SAML, se retirarán todas las asignaciones de grupos de usuarios existentes.

Atributo	Necesario	Descripción
provision_user	Sí	Especifica si un usuario se ha creado automáticamente en OpenText Core Application Security si no se encuentra. Si el valor se establece como TRUE, se crea un nuevo usuario. Si el valor se establece como FALSE o no se proporciona, el usuario no se crea y se produce un error en la solicitud de inicio de sesión si el usuario no existe en OpenText Core Application Security.  Note Si no se proporcion a ningún valor y el aprovisionamiento JIT se habilita en el portal, el valor predeterminado de provision_user será TRUE.

Atributo	Necesario	Descripción
update_user	No	Especifica si la información de un usuario existente de OpenText Core Application Security se actualiza automáticamente a partir de los valores de atributo de la aserción de SAML. Si el valor se establece como TRUE, la información del usuario se actualiza automáticamente. Si el valor se establece como FALSE, la información del usuario no se actualiza. Si no se proporciona ningún valor, se usa el valor del atributo provision_user . Puede especificar ambos para controlar la creación y la actualización por separado. Por ejemplo, puede que desee crear usuarios en el portal de forma manual, pero que su información esté actualizada a partir de los valores de aserción.

Atributo	Necesario	Descripción
mtt	No	Si se selecciona la opción SSO Habilitar configuración de Aplicación empresarial del portal, este atributo es necesario. Identificador único que se encuentra en la URL de inicio de sesión de SSO, entre comillas. Por ejemplo, dada la URL <code>https://ams.fortify.com/SSO/Login/c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc</code>, el identificador es <code>c7f4cde3-891b-49ea-b7ae-f03de4f8a8dc</code>.



Important

También debe configurar OpenText Core Application Security para reconocer los atributos utilizados por el proveedor de identidad. Consulte [Configuración de los ajustes de SSO](#).

1.8.4.6. Solución de errores de inicio de sesión

La solución de un error de solicitud de autenticación SSO puede resultar una tarea difícil debido a que los valores reales aprobados en la aserción de SAML se ocultan al usuario. Para facilitar la solución de problemas, el portal ofrece un registro de las aserciones de SAML con errores. Las aserciones con errores se eliminan tras 30 días.

Para ver un registro de las aserciones de SAML con errores:

1. Seleccione la vista **Administración**.

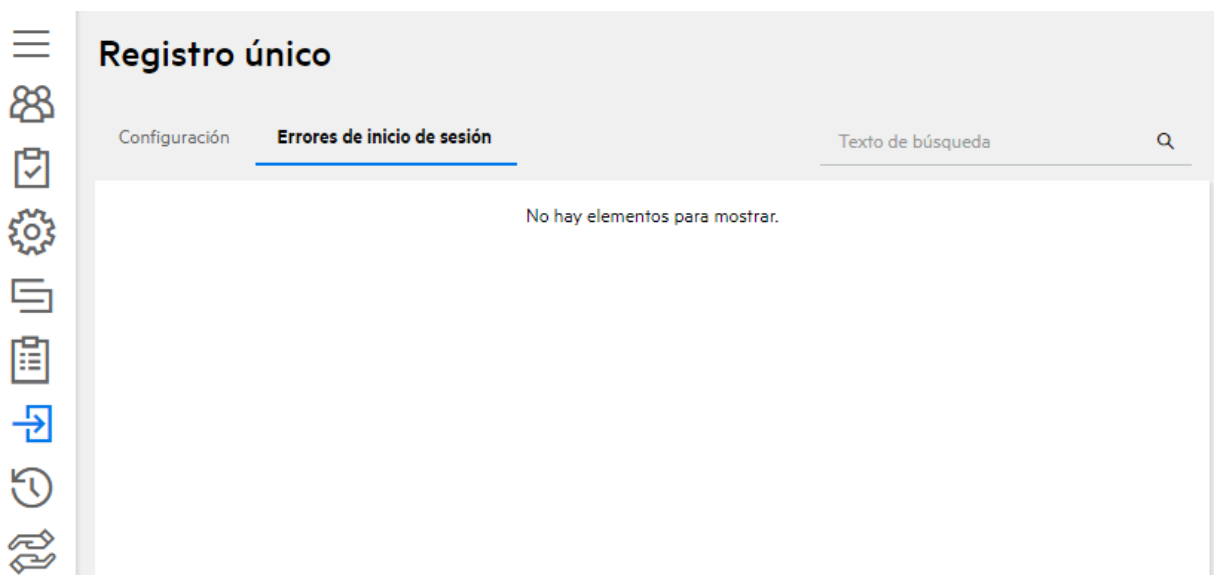
Aparecerá la página Administración de usuarios.

2. Haga clic en **Registro único**.

Aparece la página Registro único.

3. Seleccione la pestaña **Errores de inicio de sesión**.

Aparece el registro de aserciones de SAML fallidas.



La cuadrícula contiene las siguientes columnas:

- Hora de recepción: la hora a la que se recibió la aserción de SAML.
- Dirección IP: la dirección IP del cliente que solicitó la autenticación.
- Nombre de usuario: el nombre de usuario especificado en la aserción, si se encuentra alguno.

- Razón: una breve descripción del motivo por el cual se rechazó la aserción de SAML.

4. Haga clic en el vínculo **Aserción sin procesar** de cualquier inicio de sesión con errores para abrir una vista XML de la aserción de SAML descodificada.

La página mostrará la información de la aserción, incluidos la hora a la que el proveedor de identidad envió la aserción, los atributos y los valores que se proporcionaron, el periodo válido y el público, así como el certificado usado para firmar la aserción.

1.8.5. Administración de proveedores

Si desea compartir sus resultados de evaluación con un proveedor con el que hace negocios su empresa, o con otra división de la empresa, puede hacerlo a través del portal, siempre y cuando cada entidad tenga su propio inquilino con OpenText Core Application Security. Las relaciones entre inquilinos debe iniciarlas un inquilino y confirmarlas el otro; nadie puede establecer una conexión con su inquilino sin su permiso.

Además, cada vínculo va en una única dirección. Es decir, si desea compartir los informes, debe iniciar un vínculo a otro inquilino. Si ese inquilino desea compartir sus informes con usted, también debe iniciar un vínculo. El vínculo Informe de proveedor solo está visible una vez que la relación de uso compartido se crea correctamente y se comparten informes.

Solo comparte los resultados de su evaluación; su código no se comparte.

En este contexto, "Proveedores" significa los inquilinos de los que puede recibir informes y "Clientes" los inquilinos a los que puede enviar informes.

Esta sección aborda los siguientes temas:

- [Inicio de una relación con otro inquilino](#)
- [Aceptación de una relación iniciada por otro inquilino](#)
- [Publicación de un informe de administración de proveedores](#)
- [Visualización de informes publicados](#)

1.8.5.1. Inicio de una relación con otro inquilino

Para establecer que su inquilino sea un "Proveedor" (es decir, alguien que puede enviar informes a otros inquilinos):

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.



Nombre de usuario	Nombre de pila	Apellido	Correo electrónico	Número de teléfono	Nombre de rol	Estado	Fecha de creación	Fecha de último inicio de sesión	Creado mediante
saislead	Sai	Fu	sai@gogame.com		Líder en seguridad	Activo	22/10/2024	23/10/2024	

2. Haga clic en **Proveedores**.
3. Seleccione la pestaña **Clientes**.



Note

"Mis proveedores" se refiere a los inquilinos de los que puede recibir informes y "Clientes" a los inquilinos a los que puede enviar informes.

4. Haga clic en **Solicitud para ser un proveedor**.

Use el cuadro opcional **Notas** para agregar información sobre la relación entre el proveedor y el cliente.

Request to be a Vendor

Before you can send an analysis report to a customer, you must request to be a vendor of that customer. To initiate this request click "Generate." This will create a Link ID which you will send to the receiving customer.

Notes

Used to add supplementary identification information to the company relationship (only viewable by you)

GENERATE

5. Haga clic en **Generar** para mostrar el número del **Id. de vínculo**.

Request to be a Vendor

The vendor request has been initiated. To activate the vendor-customer relationship:

- Securely send the Link ID below to the customer you wish to be a vendor of so that you can send reports to that customer.
- The customer you send the Link ID to will use this ID to verify the vendor request.
- Once verified by the receiving customer, you will need to approve the relationship to make it active.

To copy the Link ID, select the ID, right click and select copy or click the 'Copy To Clipboard' button.

⚠ This Link ID is not recoverable after this dialog is closed.

Link ID

bdb1e28b-2bb7-4b7c-b2e7-73b934657c3f

CLOSE

6. Copie el número del **Id. de vínculo**.

7. Envíe el vínculo, a través de correo electrónico u otro medio de transferencia seguro, al contacto apropiado de la empresa o a otro inquilino al que le gustaría estar conectado.
8. Haga clic en **Cerrar**.

1.8.5.2. Aceptación de una relación iniciada por otro inquilino

La aceptación de una relación iniciada por otro inquilino se realiza en dos pasos.

- [Confirmación de una relación](#)
- [Establecimiento de su inquilino como cliente](#)

Confirmación de una relación

Para confirmar una relación con otro inquilino que le ha enviado una solicitud, siga estos pasos:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.



Administración de usuarios									
Usuarios Roles Grupos									
Texto de búsqueda									
1 encontrado									
seleccionar todo									
Nombre de usuario	Nombre de pila	Apellido	Correo electrónico	Número de teléfono	Nombre de rol	Estado	Fecha de creación	Fecha de último inicio de sesión	Creado mediante
☐	saislead	Sai	Fu	sai@gogame.com	Lider en seguridad	Activo	22/10/2024	23/10/2024	
Editar Asignar aplicaciones Ver aplicaciones Eliminar									

2. Haga clic en **Proveedores**.

Se abre la página Administración de proveedores, que muestra las pestañas Mis proveedores y Clientes. En este contexto, "Proveedores" significa los inquilinos de los que puede recibir informes y "Clientes" los inquilinos a los que puede enviar informes.

Establecimiento de su inquilino como cliente

Para establecer el inquilino como "cliente" (es decir, aquel que puede recibir informes de otros inquilinos), siga estos pasos:

1. Haga clic en **Mis proveedores**.
2. Haga clic en **Verificar vínculo de proveedor**.

Verify Vendor Link

✕

To accept the link request, enter the Link ID below that was given to you from the vendor.

Link ID

Notes

Used to add supplementary identification information to the company relationship (only viewable by you)

SUBMIT

3. Pegue el **Id. de vínculo** que ha recibido del otro inquilino.
4. (Opcional) Agregue notas adicionales sobre la relación de la compañía (por ejemplo, subsidiaria o división de Australia). Estas notas solo están visibles para usted.
5. Haga clic en **Enviar**.

1.8.5.3. Publicación de un informe de administración de proveedores

Una vez que haya establecido una relación con otro inquilino en OpenText Core Application Security, puede “publicar” sus informes para que ese inquilino pueda revisarlos.

Para compartir un informe con un proveedor aprobado:

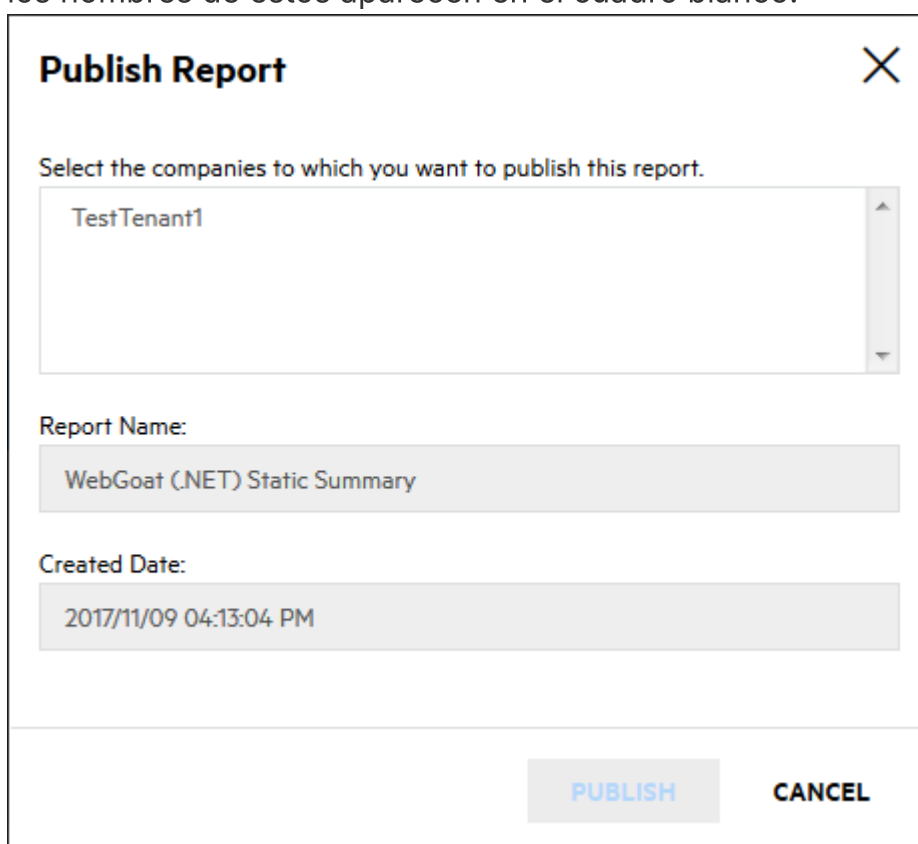
1. Seleccione la página Informes.

Aparece una nueva pantalla con una lista de todos los informes generados para su inquilino.

2. Haga clic en el nombre del informe que desea compartir. La página se actualiza y muestra los **Detalles del informe** debajo de la lista de informes.

3. Haga clic en .

Aparece la ventana **Publicar informe**. Si existe una relación con otros inquilinos, los nombres de estos aparecen en el cuadro blanco.



Publish Report

Select the companies to which you want to publish this report.

- TestTenant1

Report Name:

WebGoat (.NET) Static Summary

Created Date:

2017/11/09 04:13:04 PM

PUBLISH CANCEL

4. Seleccione el nombre del inquilino al que desea enviar el informe y haga clic en Publicar.

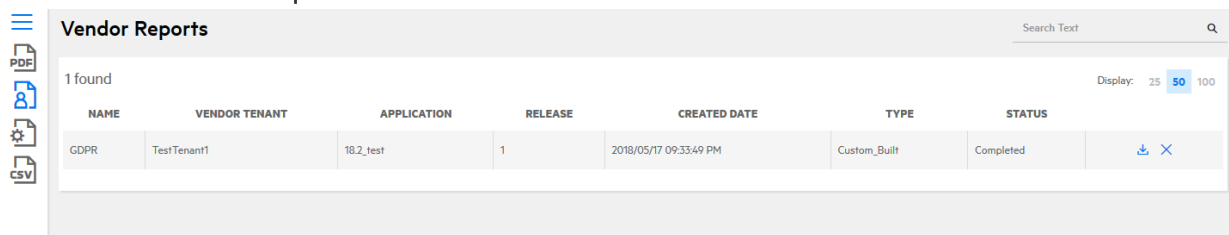
Aparece una nota informando de que el informe se ha puesto en cola para su publicación y que se enviará al inquilino.

1.8.5.4. Visualización de informes publicados

Una vez que otro inquilino publique un informe para usted (es decir, “comparta” un informe con su inquilino), podrá ver el informe siguiendo estos pasos:

1. Seleccione la página Informes.
2. Haga clic en Informe de proveedor.

Aparece una Lista de informes, que muestra los informes que han compartido con usted otros inquilinos.



NAME	VENDOR TENANT	APPLICATION	RELEASE	CREATED DATE	TYPE	STATUS	
GDPR	TestTenant1	18.2_test	1	2018/05/17 09:33:49 PM	Custom_Built	Completed	Download Delete

3. Resalte un informe de la lista y haga clic en **Descargar informe** en la columna **Acción**.

Aparece una nota que le informa de que el informe está disponible en formato PDF en su carpeta Descargas del sistema.



Note

Nota: Si **Informe de proveedor** no aparece en la lista de tipos de informe, esto significa que ningún otro inquilino ha compartido aún informes. Asegúrese de que tanto usted como el otro inquilino hayan completado todos los pasos necesarios para crear correctamente una relación de uso compartido y de que un informe específico se haya “publicado” para usted.

1.9. API de OpenText Core Application Security

OpenText Core Application Security proporciona una interfaz de programación de aplicaciones (API) RESTful que permite a los usuarios realizar diversas tareas y acceder a los datos de aplicaciones y versiones. La versión más reciente de la API es la 3. El centro de datos del inquilino determina la URL raíz de API

Centro de datos	URL raíz de API
AMS (América)	https://api.ams.fortify.com
EMEA (Europa, Oriente Medio y África)	https://api.emea.fortify.com
APAC	https://api.apac.fortify.com
SGP	https://api.sgp.fortify.com
FedRAMP	https://api.fed.fortifygov.com
Prueba	https://api.trial.fortify.com



Note

La API de OpenText Core Application Security no es compatible con el uso compartido de recursos entre orígenes (CORS).

Esta sección contiene los siguientes temas:

- [Visualización de la documentación de la API a través del Explorador de API](#)
- [Pruebas de extremos de API mediante el Explorador de API](#)
- [Autenticación de API](#)
- [Ámbitos de API](#)
- [Límites de frecuencia de API](#)
- [Tokens de acceso personal](#)

1.9.1. Visualización de la documentación de la API a través del Explorador de API

La documentación de la API de OpenText Core Application Security se proporciona en forma de Explorador de API. El Explorador de API se basa en el marco de Swagger (OpenAPI) y está disponible directamente en el portal. De este modo, la API puede ser autodocumentada e interactiva; los usuarios pueden ver instantáneamente la API actualizada, realizar llamadas de prueba y usar la descripción JSON de la API para generar código auxiliar y SDK en distintos lenguajes de programación mediante herramientas de código abierto como Swagger Editor y Swagger Codegen.

Para ver el Explorador de API:

1. Haga clic en el nombre de su cuenta en la barra de herramientas y seleccione **Explorador de API**.

Se abrirá la página Explorador de API en una nueva ventana, en la que se mostrará una lista de recursos.

Autenticar	access_token	Obtener JSON
Explorador de API OpenText™ Core Application Security Web		
Gestión de claves de API	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Supervisión de aplicaciones	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Aplicaciones	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Atributos	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Plantilla de auditoría	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Análisis de Dast automatizada	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Análisis dinámicos	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Registros de eventos	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Redes de Fortify On Demand Connect	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Elementos de búsqueda	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Análisis móviles	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Código de autorización multifactorial	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Notificaciones	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Componentes de código abierto	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Análisis de código abierto	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Tokens de acceso personal	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Versiones	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones
Informes	Mostrar/Ocultar	Enumerar operaciones Expandir operaciones

2. Explore los recursos con mayor detalle:

- Haga clic en **Obtener JSON** en la parte superior de la página Explorador de API. El navegador muestra la descripción JSON de la API.

```
{
  "swagger": "2.0",
  "info": {
    "version": "v3",
    "title": "Fortify on Demand Web API Explorer",
    "host": "16.103.234.237",
    "schemes": [
      "http"
    ],
    "paths": {
      "/api/v3/applications/{applicationId}": {
        "get": {
          "tags": [
            "Applications"
          ],
          "summary": "Retrieves an individual application by id",
          "operationId": "ApplicationsV3_GetApplication",
          "consumes": [
            "application/json",
            "text/xml"
          ],
          "parameters": [
            {
              "name": "applicationId",
              "in": "path",
              "description": "The application id",
              "required": true,
              "type": "integer",
              "format": "int32"
            }
          ],
          "responses": {
            "200": {
              "description": "Ok",
              "schema": {
                "$ref": "#/definitions/Application"
              },
              "401": {
              "description": "Unauthorized",
              "404": {
              "description": "Not Found",
              "500": {
              "description": "Internal Server Error"
            }
          }
        }
      }
    }
  }
}
```

Puede pegar o importar el archivo JSON en una herramienta de generación de código compatible con Swagger, como [Swagger Editor](#) o [Swagger Codegen](#) y generar los SDK o el código auxiliar de cliente.

- Haga clic en **Mostrar/Ocultar** para mostrar u ocultar los extremos.
- Haga clic en **Enumerar operaciones** para ver los extremos de un recurso.
- Haga clic en **Expandir operaciones** para ver las descripciones de los extremos de un recurso.
- Haga clic en un extremo para ver su descripción.

1.9.2. Pruebas de extremos de API mediante el Explorador de API

Puede probar los extremos de API de la versión 3 en el Explorador de API.



Important

Los métodos POST, PUT y DELETE del Explorador de API modifican los datos del inquilino en el portal.

1. Haga clic en **Autenticar** en la parte superior de la página Explorador de API.

Authenticate

Get JSON

Se abrirá una ventana modal donde podrá introducir sus credenciales de autenticación.

Real data will be accessed and modified using the "Try it out!" button for each endpoint.

Exercise extra caution with Post, Put, and Delete endpoints as these will affect production data!

Help with Authentication

Grant Type
password

Scope
api-tenant

Username

Password

Tenant

If your tenant requires two-factor authentication enter the Security Code

Close Submit

2. Seleccione el método de autenticación en la lista **Tipo de concesión**:
 - **password**: las credenciales de la cuenta de usuario del portal
 - **client_credentials**: las claves de API generadas en el portal
3. En el campo **Ámbito**, escriba los ámbitos que se concederán a un token de acceso. Separe los valores de ámbito mediante espacios. Para obtener la lista de ámbitos, consulte [Ámbitos de API](#).
4. Introduzca las credenciales de autenticación:

Método de autenticación	Procedimiento
client_credentials	1. En el campo Id. de cliente, escriba la clave de API. Para obtener información sobre la creación de claves de API, consulte Creación de una clave de API. 2. En el campo Secreto de cliente, escriba el secreto de API.

Método de autenticación	Procedimiento
contraseña	 Note Puede obtener el nombre de usuario y el código del inquilino en la configuración de la cuenta. 1. En el campo Nombre de usuario, escriba el nombre de usuario de la cuenta. 2. En el campo Contraseña, escriba la contraseña de la cuenta o su token de acceso personal.  Note Si se utiliza un token de acceso personal y los ámbitos especificados no constituyen un subconjunto de los ámbitos permitidos del token de acceso personal, se producirá un fallo en la autenticación. 3. En el campo Inquilino, escriba el código de inquilino. 4. (Obligatorio si se habilita la autenticación en dos pasos) En

Método de autenticación	Procedimiento
	el campo Código de seguridad , escriba el código de seguridad que recibió como parte de la autenticación en dos pasos.

5. Haga clic en **Enviar**.

Se genera un token de acceso para la sesión.

6. Expanda un extremo y complete los parámetros en los campos indicados.

GET /api/v3/applications/{applicationId}
Retrieves an individual application by id

Response Class (Status 200)
Ok

Model Model Schema

```

{
  "applicationId": 0,
  "applicationName": "string",
  "applicationDescription": "string",
  "applicationCreatedDate": "2016-05-20T16:01:36.708Z",
  "businessCriticalityTypeId": 0,
  "businessCriticalityType": "string",
  "emailList": "string",
  "applicationTypeId": 0,
  "applicationType": "string",
  "attributes": f

```

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
applicationId	(required)	The application id	path	integer

Response Messages

HTTP Status Code	Reason	Response Model	Headers
401	Unauthorized		
404	NotFound		
500	InternalServerError		

Try it out!

7. Haga clic en **Probar**.

La respuesta se muestra más abajo.

Try it out! [Hide Response](#)

Curl

```
curl -X GET --header 'Accept: application/json' --header 'Authorization: Bearer gAAAAH21jER2935DMsX8qvA2q6qyhpPh8c0VeDfNo_9Keqnlwz'
< [REDACTED] >
```

Request URL

```
http://16.103.234.237/api/v3/applications/4191
```

Response Body

```
{
  "applicationId": 4191,
  "applicationName": "Test Application",
  "applicationDescription": null,
  "applicationCreateDate": "2016-01-26T10:23:22.717",
  "businessCriticalityTypeId": 3,
  "businessCriticalityType": "Low",
  "emailList": null,
  "applicationTypeId": 1,
  "applicationType": "Web_Thick_Client",
  "attributes": null
}
```

Response Code

```
200
```

Response Headers

```
{
  "pragma": "no-cache",
  "date": "Thu, 19 May 2016 14:14:34 GMT",
  "server": "Microsoft-IIS/8.5",
  "x-powered-by": "ASP.NET",
  "content-type": "application/json; charset=utf-8",
  "expires": "-1",
  "cache-control": "no-cache",
  "content-length": "296",
  "x-ua-compatible": "IE=Edge"
}
```


1.9.3. Autenticación de API

La autenticación de solicitudes de API OpenText Core Application Security se realiza a través de un token Bearer. Obtenga un token Bearer enviando una solicitud al extremo del token.

Para autenticar llamadas API OpenText Core Application Security:

1. Realice una solicitud POST al extremo del token

`<datacenter_root_URL>/oauth/token` con los siguientes parámetros de cuerpo:



Note

Para obtener una lista de las URL raíz de API del centro de datos, consulte [Interfaz de programación de aplicaciones \(API\)](#).

Parámetro del cuerpo	Descripción
scope	Ámbitos concedidos a un token de acceso (en minúsculas). Separe los valores de ámbito mediante espacios. Para obtener la lista de ámbitos, consulte Ámbitos de API .
grant_type	Tipo de concesión (en minúsculas): - password : credenciales de usuario (credenciales de contraseña del propietario de recursos) - client_credentials : el secreto y la clave de API
username	Nombre de usuario de la cuenta como <code><tenant_code>\<username></code> . El código de inquilino y el nombre de usuario se muestran en la configuración de la cuenta. Escriba el nombre de usuario entre comillas para representar los caracteres especiales.

Parámetro del cuerpo	Descripción
password	Contraseña de la cuenta o token de acceso personal. Escriba la contraseña entre comillas para representar los caracteres especiales.  Note El uso de tokens de acceso personales está restringido para los usuarios de SSO.  Note Si se utiliza un token de acceso personal como una contraseña y los ámbitos especificados no constituyen un subconjunto de los ámbitos permitidos del token de acceso personal, se producirá un fallo en la autenticación. Para obtener más información sobre los tokens de acceso personal, consulte Creación de tokens de acceso personal.
client_id	Clave de API
client_secret	Secreto de API

Se devuelve un token en una respuesta de JSON con el nombre "access_token".

2. Use este token como un token Bearer (Portador) en el encabezado Authorization (Autorización):

```
Authorization: Bearer {token}
```

El siguiente ejemplo es una solicitud para obtener un token Bearer utilizando las credenciales de usuario:

```
curl --request POST 'https://api.ams.fortify.com/oauth/token' \
--form 'scope="api-tenant"' \ --form 'grant_type="password"' \ -
--form 'username="myTenantCode\\myUsername"' \ --form
'password="myPassword"'
```

El siguiente ejemplo es una solicitud para obtener un token Bearer utilizando la clave y el secreto de API.

```
curl --request POST 'https://api.ams.fortify.com/oauth/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \ --
data-urlencode 'scope=api-tenant' \ --data-urlencode
'grant_type=client_credentials' \ --data-urlencode
'client_id=myApiKey' \ --data-urlencode
'client_secret=myApiSecret'
```

1.9.4. Ámbitos de API

Los ámbitos limitan el acceso que se concede a los tokens de acceso. No conceden permisos adicionales más allá de los que ya posee el usuario. Puede ver los detalles de un extremo en el Explorador de API para consultar qué ámbitos admite.

En la siguiente tabla se enumeran los ámbitos disponibles:

Ámbito	Descripción
api-tenant	Conceder acceso a todos los extremos
start-scans	Configurar e iniciar análisis estáticos, dinámicos y móviles, e importar análisis estáticos y dinámicos
manage-apps	Administrar aplicaciones
view-apps	Ver aplicaciones
manage-issues	Administrar problemas
view-issues	Ver problemas
manage-reports	Administrar informes
view-reports	Ver informes
manage-users	Administrar usuarios
view-users	Ver usuarios
manage-notifications	Administrar notificaciones
view-tenant-data	Ver datos a nivel de inquilino

1.9.5. Límites de frecuencia de API

OpenText Core Application Security implementa límites de frecuencia de API por extremo y por usuario o clave.

Los siguientes extremos no tienen límite:

- PUT/api/v3/releases/{releaseld}/dynamic-scans/import-scan
- POST /api/v3/releases/{releaseld}/mobile-scans/start-scan
- PUT /api/v3/releases/{releaseld}/mobile-scans/import-scan
- POST /api/v3/releases/{releaseld}/static-scans/start-scan
- PUT /api/v3/releases/{releaseld}/static-scans/import-scan

En la siguiente tabla, se enumeran los límites de frecuencia de los extremos limitados.

Extremo	Solicitudes máximas	Segundos
POST /api/v3/applications	6	30
PUT /api/v3/applications/{applicationId:int}	1	30
GET /api/v3/eventlogs/download	1	300
POST /api/v3/releases	6	30
PUT /api/v3/releases/{releaseId:int}	1	30
POST /api/v3/releases/{releaseId:int}/dynamic-scans/start-scan	1	30
GET /api/v3/releases/{releaseId:int}/fpr	1	30
 Note El límite de frecuencia es por tipo de análisis.		
GET /api/v3/releases/{releaseId:int}/vulnerabilities/{vulnId}/all-data	1	1

Extremo	Solicitudes máximas	Segundos
POST /api/v3/releases/{releaseId:int}/vulnerabilities/bug-link	1	5
POST /api/v3/releases/{releaseId:int}/vulnerabilities/bulk-edit	1	5
Otros extremos	10	1

Límites de frecuencia de seguimiento

Cuando se llama a un extremo de API, el encabezado HTTP de respuesta proporciona el límite de frecuencia y la rapidez con la que se alcanza dicho límite:

- X-Rate-Limit-Limit: la cantidad máxima de solicitudes.
- X-Rate-Limit-Remaining: la cantidad de solicitudes restantes.
- X-Rate-Limit-Reset: el número de segundos para restablecer el límite de frecuencia.

Cuando se alcanza el límite de frecuencia de un extremo de API, la API devuelve el código de estado de respuesta HTTP 429 "Too Many Requests" junto con un mensaje de respuesta como el siguiente:

```
{ "errors": [ { "errorCode": null, "message": "Rate limit of 1 request(s) every 15 second(s) has been exceeded" } ] }
```

Mejores procedimientos para evitar alcanzar el límite de frecuencia

Para evitar alcanzar el límite de frecuencia al llamar a la API, siga estos mejores procedimientos para reducir y regular la cantidad de solicitudes de API:

- Guarde en la memoria caché los datos usados con frecuencia.

Para los extremos de API que se usan con frecuencia, guarde en la memoria caché las respuestas de API y cargue las respuestas de la memoria caché al

solicitar los datos.

- Elimine las llamadas de API innecesarias.

Examine las solicitudes que obtengan datos que no se usen y las solicitudes que envían datos a OpenText Core Application Security sin cambios.

- Regule la frecuencia de solicitudes.

Si suele alcanzar el límite de frecuencia, considere incluir un proceso que regule la frecuencia de las solicitudes de modo que no se superen los límites de frecuencia establecidos. Puede regular la frecuencia de solicitudes de forma estática configurando una frecuencia de solicitudes fija, o bien puede hacerlo de manera dinámica realizando un seguimiento de las solicitudes y regulándolas al acercarse al límite de frecuencia.

1.9.6. Tokens de acceso personal

Los tokens de acceso personal son claves exclusivas vinculadas al usuario que las generó. Funcionan como contraseñas alternativas que se usan para autenticarse en la API. Incluyen los permisos del usuario y se pueden restringir mediante ámbitos. El uso de tokens de acceso personal ignora la autenticación en dos fases y los requisitos de SSO configurados en el portal.



Note

Los tokens de acceso personal no se pueden usar para iniciar sesión en el portal.

Los tokens de acceso personales proporcionan un método flexible y seguro de autenticación para las integraciones con OpenText Core Application Security. Los usuarios pueden tener varios tokens con distintos ámbitos para satisfacer necesidades concretas, especificar fechas de caducidad de tokens y deshabilitar los tokens en cualquier momento.

OpenText Core Application Security envía notificaciones en el portal y por correo electrónico 14 días antes de que caduque un token de acceso personal. Los tokens de acceso personal caducados no se pueden utilizar a menos que se genere un nuevo secreto.

Esta sección aborda los siguientes temas:

- [Creación de un token de acceso personal](#)
- [Edición o eliminación de los tokens de acceso personal](#)

1.9.6.1. Creación de un token de acceso personal

Para crear un token de acceso personal:

1. Haga clic en el nombre de cuenta y seleccione **Tokens de acceso personal**.

Aparecerá la página Tokens de acceso personal.



Tokens de acceso personales						+ AGREGAR TOKEN DE ACCESO PERSONAL
NOMBRE	AUTORIZADO	FECHA DE CADUCIDAD DEL SECRETO	ÁMBITOS PERMITIDOS	FECHA DE ÚLTIMO INICIO DE SESIÓN	DIRECCIÓN IP DE ÚLTIMO INICIO DE SESIÓN	
newtoken2	SI	2019/02/15	start-scans, manage-apps, view-apps			NUEVO SECRETO EDITAR ELIMINAR
token1	SI	2019/03/02	start-scans, manage-apps, view-apps	2019/02/01	16.168.194.235	NUEVO SECRETO EDITAR ELIMINAR
new1	SI	2019/03/02	start-scans, manage-apps, view-apps			NUEVO SECRETO EDITAR ELIMINAR
token2	SI	2019/03/04	start-scans, manage-apps, view-apps	2019/02/01	16.168.194.235	NUEVO SECRETO EDITAR ELIMINAR

2. Haga clic en **+Agregar token de acceso personal**.

Se abrirá la ventana Agregar/editar token de acceso personal.

Agregar/editar token de acceso personal

Nombre

Autorizar el uso de la API

☐
☒ Sí

Fecha de caducidad del secreto

Días de caducidad del secreto (máx. 40)

Ámbitos permitidos

☐ api-tenant
 ☐ start-scans
 ☐ manage-apps
 ☐ view-apps
 ☐ manage-issues
 ☐ view-issues
 ☐ manage-reports
 ☐ view-reports
 ☐ manage-users

- Complete los campos. Los campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
Nombre	Escriba un nombre para el token.
Autorizar el uso de la API	El token está habilitado de forma predeterminada. Mueva el control deslizante a No para deshabilitar el token.
Fecha de caducidad del secreto, Días de caducidad del secreto	Use el calendario para seleccionar una fecha de caducidad o escriba el número de días tras los cuales caducará el secreto. El token caducará a las 00:00 PT (Hora del Pacífico) de la fecha que configure. La fecha de caducidad no puede exceder la validez máxima establecida en el portal.
Ámbitos permitidos	Seleccione los ámbitos permitidos para el token. Para obtener más información sobre los ámbitos, consulte Ámbitos de API .

4. Haga clic en **Guardar**.

Se abrirá la ventana Clave secreta.

5. Copie el secreto con codificación Base64. El secreto se muestra una sola vez.

6. Haga clic en **Cerrar**.

El token nuevo aparecerá en la lista de tokens de acceso personal.

1.9.6.2. Edición o eliminación de los tokens de acceso personal

Para editar o eliminar un token de acceso personal:

1. Haga clic en el nombre de cuenta y seleccione **Tokens de acceso personal**.

Aparecerá la página Tokens de acceso personal.



Tokens de acceso personales						+ AGREGAR TOKEN DE ACCESO PERSONAL
NOMBRE	AUTORIZADO	FECHA DE CADUCIDAD DEL SECRETO	ÁMBITOS PERMITIDOS	FECHA DE ÚLTIMO INICIO DE SESIÓN	DIRECCIÓN IP DE ÚLTIMO INICIO DE SESIÓN	
newtoken2	SI	2019/02/15 ⓘ	start-scans, manage-apps, view-apps			NUEVO SECRETO EDITAR ELIMINAR
token1	SI	2019/03/02 ⓘ	start-scans, manage-apps, view-apps	2019/02/01	16.168.194.235	NUEVO SECRETO EDITAR ELIMINAR
new1	SI	2019/03/02	start-scans, manage-apps, view-apps			NUEVO SECRETO EDITAR ELIMINAR
token2	SI	2019/03/04	start-scans, manage-apps, view-apps	2019/02/01	16.168.194.235	NUEVO SECRETO EDITAR ELIMINAR

2. Puede realizar las siguientes tareas:

Tarea	Procedimiento
Generar un nuevo secreto	- Haga clic en Nuevo secreto. Se abrirá la ventana Nuevo secreto. - Use el calendario para seleccionar una fecha de caducidad o escriba el número de días tras los cuales caducará el secreto. El token caducará a las 00:00 PT (Hora del Pacífico) de la fecha que configure. La fecha de caducidad no puede exceder la validez máxima establecida en el portal. - Haga clic en Crear. Esto anulará el secreto actual.
Editar el token	- Haga clic en Editar. Se abrirá la ventana Agregar/editar token de acceso personal. - Edite los campos según sea necesario. La fecha de caducidad del secreto actual no se puede editar.
Eliminar el token	- Haga clic en Eliminar. Aparecerá un mensaje de confirmación. - Haga clic en Sí.

1.10. Integraciones y herramientas

OpenText Core Application Security ofrece diferentes integraciones y herramientas para ayudar a su organización a integrar pruebas de seguridad de las aplicaciones en sus procesos de DevOps.

Esta sección contiene los siguientes temas:

- [Herramientas de CI/CD](#)
- [Herramientas de IDE](#)
- [Herramientas de preparación y seguimiento del análisis](#)
- [Herramientas de visualización y descarga](#)
- [Integraciones de portales](#)
- [Cursos de formación](#)

1.10.1. Herramientas de CI/CD

Las siguientes herramientas de integración continua y entrega continua (CI/CD) permiten integrar pruebas estáticas y dinámicas en la automatización de compilación existente.

Herramienta de CI/CD	Descripción	Más información
OpenText Core Application Security Uploader	Utilidad independiente para cargar código de un servidor de compilación en OpenText Core Application Security para análisis estáticos	GitHub
Fortify Azure DevOps Extension	Extensión Azure DevOps para: • Cargar código en OpenText Core Application Security y enviar análisis dinámicos como tareas de compilación y versión • Enviar análisis dinámicos como tareas de compilación y versión	• Visual Studio Marketplace • Documentación
Fortify on Demand Jenkins Plugin	Complemento de Jenkins para cargar código en OpenText Core Application Security y enviar análisis estáticos como tareas de compilación	• Jenkins • Documentación
Fortify CLI	Utilidad de línea de comandos para interactuar con varios productos Fortify	Repositorio de GitHub

Herramienta de CI/CD	Descripción	Más información
Fortify Bitbucket Pipelines	Recopilación de canalizaciones de Bitbucket para: Subir código a OpenText Core Application Security y enviar escaneos estáticos	Bitbucket Documentación
Fortify GitHub Actions	Recopilación de acciones de GitHub para: Subir código a OpenText Core Application Security y enviar escaneos estáticos	GitHub Marketplace Documentación
Fortify GitLab CI Templates	Recopilación de plantillas de GitLab para: Subir código a OpenText Core Application Security y enviar escaneos estáticos	GitLab

Herramienta de CI/CD	Descripción	Más información
Fortify CI Tools	Contenedor de Docker que simplifica la integración de las pruebas de seguridad de las aplicaciones estáticas de Fortify para las canalizaciones de DevSecOps que usan ejecutores configurables para ejecutar flujos de trabajo de CI/CD	Docker Hub

1.10.2. Herramientas de IDE

Las siguientes herramientas de entorno de desarrollo integrado (IDE) permiten a los desarrolladores cargar código de los IDE en OpenText Core Application Security para pruebas estáticas:



Note

La documentación para cada herramienta de IDE ahora está disponible como una guía independiente.

Herramienta de IDE	Descripción	Más información
Fortify on Demand Plugin for Eclipse	Complemento de Eclipse para cargar código en OpenText Core Application Security para el análisis estático y la apertura de resultados de análisis para su solución	Fortify on Demand Plugin for Eclipse
Complemento de Core Application Security para IntelliJ IDEA	Complemento de IntelliJ IDEA para cargar código en OpenText Core Application Security para el análisis estático y la apertura de resultados de análisis para su solución	Complemento de Core Application Security para IntelliJ IDEA
Fortify on Demand Extension for Visual Studio	Extensión de Visual Studio para cargar código en OpenText Core Application Security para el análisis estático y la apertura de resultados de análisis para su solución	Fortify on Demand Extension for Visual Studio
Extensión de corrección de Core Application Security para Visual Studio Code	Extensión de Visual Studio Code para ver y auditar problemas directamente desde una versión de aplicación en OpenText Core Application Security	Extensión de corrección de Core Application Security para Visual Studio Code

Herramienta de IDE	Descripción	Más información
Extensiones de Fortify para el análisis de Visual Studio Code	Extensión de Visual Studio para cargar código para análisis estáticos	Documentación de la extensión de código de Fortify Visual Studio
Fortify Security Assistant Plugin for Eclipse	Complemento de Eclipse que proporciona alertas sobre posibles problemas de seguridad en archivos Java mientras escribe código¹ Incluye analizadores de flujo de datos semánticos y entre clases para detectar lo siguiente: • Posibles usos peligrosos de funciones y API. • Problemas causados por datos dañados que conciernen funciones vulnerables y API en el nivel entre clases.	Documentación de Fortify Security Assistant para Eclipse

Herramienta de IDE	Descripción	Más información
Fortify Security Assistant Plugin for IntelliJ	Complemento de IntelliJ IDEA que proporciona alertas sobre posibles problemas de seguridad en archivos Java mientras escribe código¹ Incluye analizadores estructurales y de configuración para detectar: • Posibles usos peligrosos de funciones y API. • Configuraciones de aplicaciones no seguras en archivos de propiedad y XML	Documentación de Fortify Security Assistant para IntelliJ

Herramienta de IDE	Descripción	Más información
Fortify Security Assistant Extension for Visual Studio	Extensión de Visual Studio que proporciona alertas a posibles problemas de seguridad en archivos C# (.cs) , Razor (.cshtml), WebForms (.aspx) y .config, .xml e .ini mientras escribe código¹ Incluye analizadores estructurales y de configuración para detectar: • Posibles usos peligrosos de funciones y API. • Configuración de aplicaciones no seguras.	Documentación de extensión de Fortify Security Assistant para Visual Studio

¹Fortify Security Assistant requiere de un archivo de licencia válido en busca de problemas, así como para instalar o actualizar contenido de seguridad de Fortify. La licencia es válida para todas las versiones de Fortify Security Assistant.

1.10.3. Herramientas de preparación y seguimiento del análisis

Las siguientes herramientas se utilizan para preparar el código fuente de la aplicación para el análisis estático.

Herramienta de análisis estáticos	Descripción	Más información
OpenText SAST	Versión de solo traducción OpenText SAST para traducir el código de C/C++ y Scala, y empaquetarlo para el análisis  Note OpenText SAST requiere un archivo de licencia válido para traducir el código fuente.	Documentación de herramientas y pruebas de seguridad de aplicaciones estáticas de OpenText
Extractor de ABAP de Fortify	Solicitud de transporte SAP para descargar archivos de código fuente en el servidor de presentación	Preparación de los archivos de aplicación de ABAP (SAP)
Fortify ScanCentral SAST client	Cliente independiente Fortify ScanCentral SAST para empaquetar código fuente	Fortify ScanCentral SAST
Fortify Audit Workbench	Herramienta para ver y auditar archivos FPR	Documentación de herramientas y pruebas de seguridad de aplicaciones estáticas de OpenText

Las siguientes herramientas se utilizan para preparar aplicaciones web para el análisis dinámico.

Herramienta de análisis dinámico	Descripción	Más información
Grabador de macros de flujo de trabajo	Utilidad independiente para crear macros de flujo de trabajo	Documentación de pruebas de seguridad de aplicaciones dinámicas de OpenText
Grabador de macros de inicio de sesión	Utilidad independiente para crear macros de inicio de sesión	Documentación de pruebas de seguridad de aplicaciones dinámicas de OpenText

Las herramientas de seguimiento incluyen las siguientes:

Herramienta	Descripción	Más información
Software Security Sync Utility	Utilidad independiente para la sincronización automatizada y programada de la aplicación, las versiones y los análisis de OpenText Core Application Security con el Software Security Center (SSC) de Fortify	GitHub
Seguimiento de errores de OpenText Core Application Security	Utilidad independiente para enviar problemas de OpenText Core Application Security a los seguimientos de errores.	GitHub

1.10.4. Herramientas de visualización y descarga

Puede ver y descargar las herramientas disponibles para usar con OpenText Core Application Security.

Para ver las herramientas disponibles:

1. Haga clic en el nombre de la cuenta y seleccione **Herramientas** en la lista.
Aparecerá la página Herramientas.
2. Haga clic en los enlaces para los instaladores, las licencias y las instrucciones de uso.



Note

El uso de la mayoría de las herramientas no necesita licencia. Póngase en contacto con el soporte técnico para solicitar una licencia si cumple con las siguientes condiciones:

- OpenText SAST: desea analizar código C, C++ y Scala
- Fortify Audit Workbench: desea visualizar archivos FPR
- Asistente de seguridad Fortify: tiene una suscripción estática activa

1.10.5. Integraciones de portales

OpenText Core Application Security ofrece varias integraciones que se gestionan a través del portal.

Esta sección contiene los siguientes temas:

- [Integración con el seguimiento de errores](#)
- [Integración de análisis externo](#)
- [Integración con Secure Code Warrior](#)
- [Integración con Slack para las notificaciones](#)
- [Integración de control de código fuente](#)
- [Seguimiento de integraciones configuradas](#)
- [Webhooks](#)

1.10.5.1. Integración con el seguimiento de errores

Para los inquilinos que desean vincular los resultados de vulnerabilidad con sus herramientas de seguimiento de errores, OpenText Core Application Security ofrece integración con seguimiento de errores para las versiones más recientes de las siguientes herramientas:

- Gestión de calidad de aplicaciones de OpenText (anteriormente ALM)
- Gestión de entrega de software Octane de OpenText (anteriormente ALM Octane)
- Jira
- Bugzilla
- Azure DevOps/Azure DevOps Server

Los usuarios pueden enviar problemas como errores a una herramienta de seguimiento de errores compatible y administrar los errores directamente desde el portal. En el caso de seguimientos de errores no admitidos, los usuarios pueden agregar manualmente vínculos del seguimiento de errores a los problemas.

Esta sección contiene los siguientes temas:

- [Configuración de la integración con el seguimiento de errores](#)
- [Envío de problemas al seguimiento de errores](#)
- [Vinculación manual de un problema](#)

1.10.5.1.1. Configuración de la integración con el seguimiento de errores

La integración con el seguimiento de errores se configura en el nivel de la aplicación. Debe establecer una conexión entre OpenText Core Application Security y el servidor de seguimiento de errores (no puede seleccionarse una VPN para establecer la conexión). El servidor requerirá una cuenta de usuario dedicada para agregar y cerrar errores.

Para configurar la integración con el seguimiento de errores para una aplicación:

1. Seleccione la vista **Aplicaciones**.

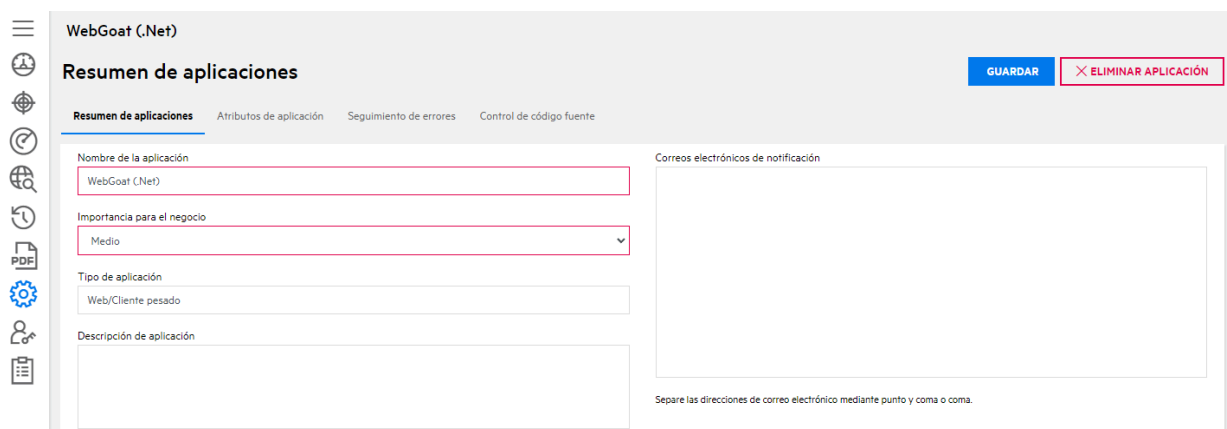
Aparecerá la página Sus aplicaciones.

2. Haga clic en la aplicación para la que desea configurar la integración con el seguimiento de errores.

Aparecerá la página Información general de la aplicación.

3. Haga clic en **Configuración**.

Aparecerá la página Configuración.



WebGoat (.Net)

Resumen de aplicaciones GUARDAR ELIMINAR APLICACIÓN

Resumen de aplicaciones | Atributos de aplicación | Seguimiento de errores | Control de código fuente

Nombre de la aplicación: WebGoat (.Net)

Importancia para el negocio: Medio

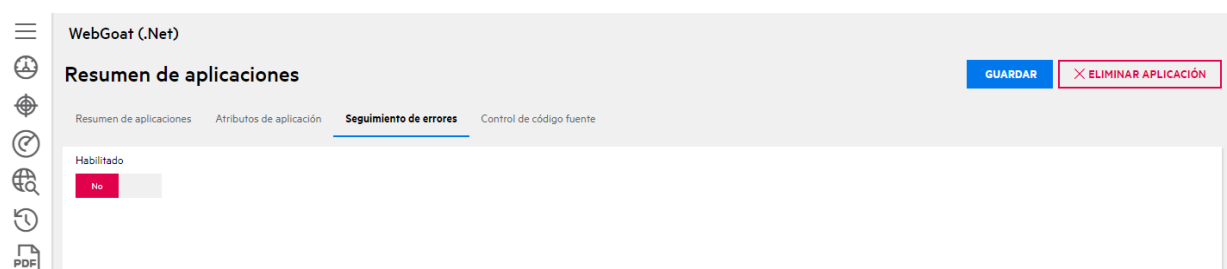
Tipo de aplicación: Web/Cliente pesado

Descripción de aplicación:

Correos electrónicos de notificación:

Separe las direcciones de correo electrónico mediante punto y coma o coma.

4. Seleccione la pestaña **Seguimiento de errores**.



WebGoat (.Net)

Resumen de aplicaciones GUARDAR ELIMINAR APLICACIÓN

Resumen de aplicaciones | Atributos de aplicación | **Seguimiento de errores** | Control de código fuente

Habilitado: No

5. Mueva el control deslizante **Habilitar integración con el seguimiento de errores** de **No** a **Sí** para habilitar la integración con el seguimiento de errores.
6. Seleccione el seguimiento de errores en la lista **Seguimiento de errores**.

Si seleccionó un seguimiento de errores admitido, abajo aparecerán más campos. Los nombres de los campos dependen del seguimiento de errores seleccionado.

The screenshot shows the 'WebGoat (.NET)' application configuration interface. The 'Resumen de aplicaciones' (Application Summary) tab is active, with sub-tabs for 'Resumen de aplicaciones', 'Atributos de aplicación', 'Seguimiento de errores' (selected), and 'Control de código fuente'. The 'Seguimiento de errores' section includes a 'Habilitado' (Enabled) toggle set to 'Sí' (Yes). Below this, a note states: 'Fortify on Demand Para la integración con el seguimiento de errores, se debe poder acceder a partir de las redes y los intervalos IP siguientes: 74.221.229.249/32'. The 'Seguimiento de errores' (Error Tracking) dropdown menu is set to 'Atlassian JIRA'. The 'URL de Atlassian JIRA' field contains 'http://fodqa-jira:8080/'. The 'Nombre de usuario' (Username) field contains 'TAMUser', and the 'Contraseña' (Password) field is empty. The 'Id. de cuenta de solicitante' (Requester account ID) field is empty. The 'AUTENTICAR' (Authenticate) button is visible. The 'Dominio' (Domain) dropdown is set to 'No', and the 'Componente' (Component) dropdown is set to 'No'. The 'Cerrar automáticamente los problemas al solucionarlos' (Automatically close problems when solved) checkbox is checked. The 'Sincronizar el estado del desarrollador con el estado del seguimiento de errores' (Synchronize developer state with error tracking state) checkbox is checked. A note at the bottom states: 'Nota: Los nuevos comentarios del seguimiento de errores se incluyen en la sincronización.'

7. En el campo **URL** , escriba la URL del sitio del seguimiento de errores.
8. En los campos **Nombre de usuario** y **Contraseña**, escriba las credenciales de inicio de sesión que se usarán para iniciar sesión en el sitio del seguimiento de errores.

Si tiene una instancia JIRA en la nube en la que el campo Informador sea necesario, en el campo **Id. de cuenta de solicitador**, introduzca el id. de usuario asociado con el **Nombre de usuario** proporcionado.



Important

Atlassian no admite la autenticación básica con contraseña y la autenticación basada en cookies para API de REST.

Microsoft finalizó el soporte para la autenticación básica con contraseña para las API REST.

9. Haga clic en **Autenticar**.

Si la autenticación se realizó correctamente, aparecerá el mensaje "Autenticado". También se rellenará la lista de categorías del sitio del seguimiento de errores.



Tip

Si tiene problemas al autenticarse para el seguimiento de errores, consulte los siguientes consejos de solución de problemas:

- Compruebe que la instancia del seguimiento de errores sea accesible públicamente. Por ejemplo, puede probar la accesibilidad de una instancia de Jira con el comando `curl -D -u <Jira_userid>:<Jira_password> http://<host>.atlassian.net/rest`
- Habilite la API de seguimiento de errores, si corresponde.
- Compruebe que la cuenta que se usó para iniciar sesión en el seguimiento de errores tenga permiso para acceder a la API de seguimiento de errores.
- Agregue las direcciones IP de OpenText Core Application Security a la lista de direcciones permitidas en los firewalls, los IPS, los IDS y los WAF. Las direcciones IP aparecen en la pestaña Seguimiento de errores.

10. Seleccione la categoría predeterminada a la que se enviarán los problemas de la aplicación. Los campos son específicos del seguimiento de errores seleccionado.

ValueEdge/ALM Octane: **Proyecto y Espacio de trabajo**

ALM.Net: **Dominio y Proyecto**

Jira: **Proyecto y Componente**

Bugzilla: **Producto y Componente**

Azure DevOps/Azure DevOps Server: **Proyecto**

11. Mueva el control deslizante **Habilitar administración del estado de los errores** a **Sí** para habilitar la administración del estado de los errores. Cuando se habilita la administración del estado de los errores, OpenText Core Application Security asignará automáticamente los errores a los estados enumerados en la siguiente tabla una vez que los problemas vinculados se hayan marcado como **Solución validada** o **Suprimido**. Un error vinculado a varios problemas no se cerrará a

menos que todos los problemas tengan el estado **Solución validada** o **Suprimido**.

Seguimiento de errores	Estado cerrado
ALM Octane	Solucionado (phase.defect.fixed)
ALM	Solucionado
Jira	Listo
Azure DevOps/Azure DevOps Server	Resuelto
ALM.Net	Solucionado (phase.defect.fixed)
Bugzilla	Estado: Resuelto. Resolución: Solucionado



Note

OpenText Core Application Security no vuelve a abrir los errores vinculados a problemas reabiertos.

- (Disponible para Azure DevOps y JIRA) Cuando la administración del estado de los errores esté habilitada, mueva el control deslizante de **Sincronizar el estado del desarrollador con el estado del seguimiento de errores** a **Sí** para sincronizar los valores del OpenText Core Application Security **Estado del desarrollador** con los valores de estado del seguimiento de errores. Asigne los valores de estado del seguimiento de errores a los valores del **Estado de desarrollador**.



Note

El campo **Estado del desarrollador** de un problema enviado ya no se puede editar en OpenText Core Application Security, ya que el **Estado del desarrollador** se sincroniza automáticamente con el valor de estado del seguimiento de errores. Se incluyen nuevos comentarios del seguimiento de errores en la sincronización.

13. (Disponible para Azure DevOps) Especifique valores predeterminados para los campos personalizados al enviar errores. Si corresponde, se completan los valores predeterminados de Azure DevOps. Los campos personalizados necesarios se marcan en rojo.

Para restablecer los valores de campo a los valores predeterminados de Azure DevOps, borre los campos.

Campos personalizados

Campo2

Campo4

Definición

14. Haga clic en **Guardar**.

Se guardará la configuración del seguimiento de errores.

1.10.5.1.2. Envío de problemas al seguimiento de errores

En cuanto se configura la integración con el seguimiento de errores para una aplicación, un usuario con los permisos Acceso a las aplicaciones y Editar problemas puede enviar los problemas de OpenText Core Application Security al seguimiento de errores. El portal evita que los problemas se envíen varias veces.

Para enviar problemas al seguimiento de errores:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación con problemas que desee enviar al seguimiento de errores.

Aparecerá la página Información general de la aplicación.

3. Vaya a la página Problemas de la aplicación o Problemas de versión:

- Para desplazarse a la página Problemas de la aplicación:

1. Haga clic en **Problemas**.

Aparecerá la página Problemas de la aplicación.

The screenshot shows the 'Problemas de la aplicación' page. On the left, there is a sidebar with a list of vulnerabilities, including 'Cross-Site Sc...', 'blogEntry.jsp...', 'Dangerous FL...', 'Insecure Tran...', 'Open Redirect', 'Password Ma...', and 'Path Manipul...'. The main content area displays a detailed view of a 'Cross-Site Scripting: Reflected' vulnerability. The vulnerability details include a summary, explanation, and remediation steps. The 'Auditar' section on the right shows the state of the vulnerability, including the state of the developer, the state of the auditor, the severity, and the comment.

- Para desplazarse a la página Problemas de versión:

1. Haga clic en el nombre de una versión.
2. Haga clic en **Problemas**.

Aparecerá la página Problemas de versión.

The screenshot shows the 'Problemas de versión' (Version Problems) page in the OpenText Core Application Security interface. The page is divided into three main sections:

- Left Panel:** A list of vulnerabilities grouped by version. The selected vulnerability is 'Cross-Site Scripting: Reflected' (Critic). Below it, a list of versions is shown, with 'blogEntry.jsp : 29' selected.
- Center Panel:** A detailed view of the selected vulnerability. It includes a 'Resumen' (Summary) section, an 'Explicación' (Explanation) section, and a 'Historial' (History) section. The explanation describes the vulnerability and its impact, mentioning that the method `_jspService()` in `blogEntry.jsp` sends unvalidated data to a web browser on line 29.
- Right Panel:** An 'Auditar' (Audit) panel showing the state of the vulnerability. It includes fields for 'Estado' (State), 'Fecha de introducción' (Date of introduction), 'Fecha de la última vez que se encontró' (Date of the last time it was found), 'Usuario asignado' (Assigned user), 'Estado del desarrollador' (Developer state), 'Estado del auditor' (Auditor state), 'Gravedad' (Severity), and 'Comentario' (Comment).

4. Seleccione uno o más problemas que desee enviar en el panel de navegación. Para enviar problemas por lotes, marque las casillas junto a los problemas que desee editar.



Note

Si se encuentra en la página Problemas de la aplicación y activa la casilla junto a un problema encontrado en varias versiones, se activarán todas las instancias del problema.

5. En el panel de auditoría, haga clic en **Enviar error**.

Se abrirá la ventana Enviar error a <bug_tracker>. Los campos se rellenarán con los valores predeterminados, incluidos los resúmenes de problemas. Puede editar los valores predeterminados.

Enviar un error a Azure DevOps

Proyecto

WebGoat

Asunto

Vulnerabilidad de seguridad de FoD: 236323

Descripción

Seuencias de comandos entre sitios: problemas Reflected-1

Detalles del problema:
acctxferconfirm.asp: 0 - 236323 - 236323

Gravedad

1-Crítico

Campos personalizados (obligatorio)

Campo2

Campo4

Definición

ENVIAR

CANCELAR

Problemas seleccionados 1

ID DEL PROBLEMA	UBICACIÓN PRINCIPAL
236323	/acctxferconfirm.asp

6. OpenText Core Application Security admite campos personalizados en ALM, Jira y Azure DevOps. Si el seguimiento de errores contiene campos personalizados, dichos campos aparecerán en la sección **Valores personalizados (necesario)**. Complete los campos.

7. Haga clic en **Enviar**.

Se le redirigirá a la página Problemas. Si está pendiente el envío de errores, en el panel de auditoría se muestra un estado **Error pendiente**. Cuando finaliza el envío de los problemas, en el panel de auditoría se muestra un botón **Ver error** que se vincula con la URL de seguimiento de errores del problema.



Note

Cuando se copia una versión, se actualizan los problemas en el seguimiento de errores. Los enlaces a los problemas recién copiados se agregan a las descripciones de los problemas en el seguimiento de errores.

1.10.5.1.3. Vinculación manual de un problema

Puede agregar manualmente un vínculo del seguimiento de errores al problema desde el portal. De este modo, los inquilinos que usan otros seguimientos de errores pueden rastrear los errores externos asociados con problemas de OpenText Core Application Security.

Para vincular un problema de OpenText Core Application Security a un seguimiento de errores no admitido:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación con problemas que desee enviar al seguimiento de errores.

Aparecerá la página Información general de la aplicación.

3. Vaya a la página Problemas de la aplicación o Problemas de versión:

- Para desplazarse a la página Problemas de la aplicación:

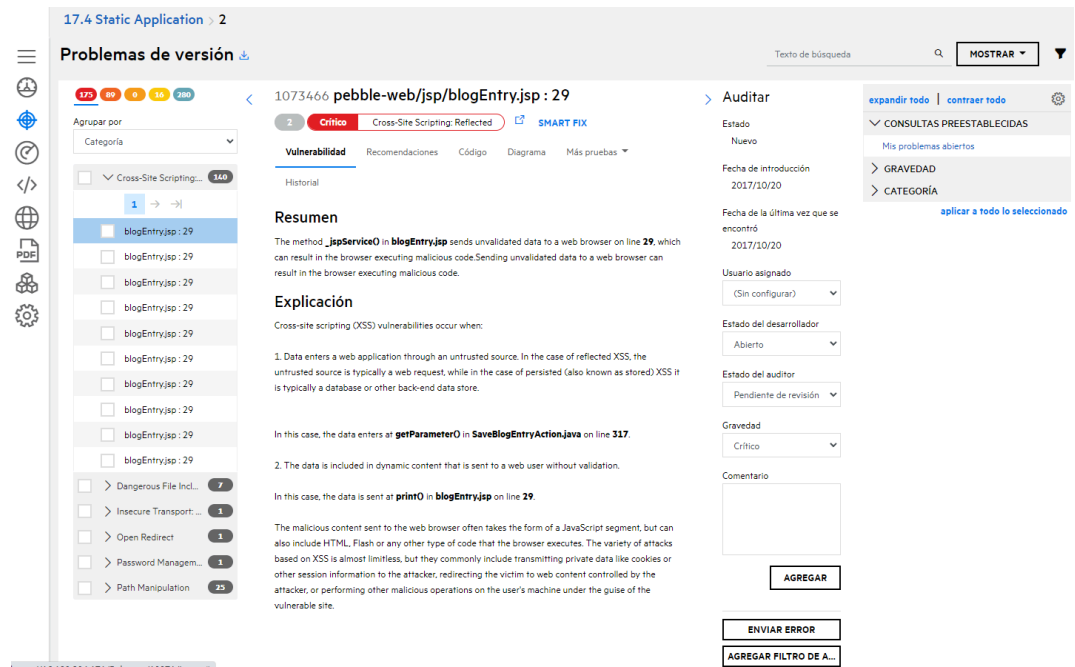
1. Haga clic en **Problemas**.

Aparecerá la página Problemas de la aplicación.

The screenshot shows the 'Problemas de la aplicación' (Application Problems) page. On the left, there is a sidebar with a list of vulnerabilities grouped by category. The main area displays a detailed view of a specific vulnerability: 'Cross-Site Scripting: Reflected' (Código: 1073124). The vulnerability is marked as 'Crítico' (Critical) and 'Nuevo' (New). The 'Resumen' (Summary) section states: 'The method `_jspService()` in `blogEntry.jsp` sends unvalidated data to a web browser on line 53, which can result in the browser executing malicious code. Sending unvalidated data to a web browser can result in the browser executing malicious code.' The 'Explicación' (Explanation) section describes the conditions for Cross-site scripting (XSS) vulnerabilities and provides a detailed description of the issue. The right sidebar contains filters for 'Estado' (Estado: Nuevo), 'Fecha de introducción' (2017/10/20), 'Fecha de la última vez que se encontró' (2017/10/20), 'Usuario asignado' (Sin configurar), 'Estado del desarrollador' (Abierto), 'Estado del auditor' (Pendiente de rev), 'Gravedad' (Crítico), and 'Comentario'. There are also buttons for 'AGREGAR', 'ENVIAR ERROR', and 'AGREGAR FILTRO ...'.

- Para desplazarse a la página Problemas de versión:
 1. Haga clic en el nombre de una versión.
 2. Haga clic en **Problemas**.

Aparecerá la página Problemas de versión.



4. Seleccione uno o más problemas que desee enviar en el panel de navegación. Para enviar problemas por lotes, marque las casillas junto a los problemas que desee editar.
5. Haga clic en **Enviar error**.
Se abrirá la ventana modal Enviar error.

Enviar error

Campos de seguimiento de error

URL del error

Asunto sugerido

Vulnerabilidad de seguridad de HPE FoD: 388656

Descripción sugerida

- 388656 - http://16.103.234.171/Redirect/Issues/388656

Problemas

NOMBRE DEL PROBLEMA	UBICACIÓN PRINCIPAL
null	10.29.92:

GUARDAR

CANCELAR

6. En el campo **URL del error**, escriba el vínculo de seguimiento de errores que desea agregar al problema.

7. Haga clic en **Guardar**.

Cuando finaliza el envío de los problemas, en el panel de auditoría se muestra un botón **Ver error** que se vincula con la URL de seguimiento de errores del problema.

1.10.5.2. Integración de análisis externo

Puede importar resultados de análisis de orígenes externos en OpenText Core Application Security para administrar los resultados de los análisis de varios orígenes en una única vista. OpenText Core Application Security admite la importación de los siguientes tipos de análisis:

- Resultados de OpenText SAST locales y de análisis OpenText DAST
- Resultados de análisis de código abierto que cumplen con el estándar CycloneDX 1.4

Esta sección contiene los siguientes temas:

- [Importación de un análisis en las instalaciones](#)
- [Importación de una lista de materiales de software](#)
- [Eliminación de un análisis importado](#)

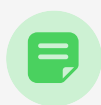
1.10.5.2.1. Importación de un análisis en las instalaciones

Puede importar localmente los resultados de los análisis OpenText SAST y OpenText DAST en OpenText Core Application Security. Al importar un archivo FPR o SARIF:

- Las horas de inicio y compleción del análisis usan la fecha de análisis del archivo FPR o SARIF.
- Se aplican plantillas de auditoría de aplicaciones y globales.
- El Id. de instancia proporcionado por OpenText SAST u OpenText DAST se utiliza para hacer un seguimiento de los problemas en los FPR o SARIF importados. OpenText Core Application Security no comprueba si hay FPR o SARIF duplicados.

Por ejemplo, si importa un archivo FPR o SARIF en una versión vacía, todos los problemas importados tendrán el estado **Nuevo**. Si vuelve a importar los mismos archivos FPR o SARIF, todos los problemas cambiarán de **Nuevo** a **Existente**. Si entonces importa un archivo FPR o SARIF diferente, el estado de los problemas cambiará de la siguiente manera:

- Los problemas que están presentes en la versión y en el archivo FPR o SARIF más reciente tendrán el estado **Existente**.
- Los problemas que solo aparecen en el archivo FPR o SARIF más reciente tendrán el estado **Nuevo**.
- Los problemas que aparecen en la versión y no en el archivo FPR o SARIF más reciente tendrán el estado **Solucionado**.
- Los problemas suprimidos en el FPR o SARIF que no se encuentren en la versión se importan y se suprimen. Se ignorará el estado de supresión de los problemas en el FPR o SARIF que estén presentes en la versión.



Note

No se aceptan FPR o SARIF con una fecha de análisis anterior al análisis completado más reciente del mismo tipo.

Para importar un FPR estático, un FPR dinámico o un SARIF estático:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

- Haga clic en la versión para la que desee importar un archivo FPR o SARIF.

Aparecerá la página Información general de versión.

- Haga clic en **Análisis**.

Aparecerá la página **Análisis de versión**.

- Haga clic en **Importar análisis>Dinámico | Estático**.

Se abrirá la ventana Importar análisis.



Seleccione el formato de archivo como FPR o SARIF.



Note

La compatibilidad de archivos SARIF solo está disponible para tipos de análisis estático. Core Application Security solo es compatible con la versión 2.1.0 de SARIF.

- Haga clic en ..., desplácese hasta el archivo FPR o SARIF y selecciónelo.
- Haga clic en **Siguiente**.

Después de completar la importación, los resultados se podrán ver en la página Problemas. El análisis aparece en la página Análisis de versión con un estado "Completado" y un tipo de evaluación "WebInspect (importado)" para OpenText SAST o el tipo de evaluación "SCA (importado)" para OpenText SAST.

1.10.5.2.2. Importación de una lista de materiales de software

Los usuarios con el permiso **Administrar aplicaciones** pueden importar resultados de análisis de código abierto, conocidos como listas de materiales de software (SBOM), de terceros. Para su importación, las SBOM deben cumplir con los siguientes requisitos:

- La SBOM es un archivo JSON que cumple con el estándar CycloneDX 1.4.
- La SBOM contiene una sola entrada de `tools` en el objeto `metadata`.
- La versión de la SBOM es superior a la versión de la SBOM importada más recientemente.

Para importar una lista de materiales de software:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

3. Haga clic en la versión para la que desee importar un análisis de código abierto.

Aparecerá la página Información general de versión.

4. Haga clic en **Análisis**.

Aparecerá la página Análisis de versión.

5. Seleccione **Importar análisis > Código abierto**.

Se abrirá la ventana Importar análisis de código abierto.

1.10.5.2.3. Eliminación de un análisis importado

Los usuarios con el permiso de Administrar aplicaciones pueden eliminar los archivos de resultados de análisis importados. No se puede eliminar un análisis si se ha importado uno posterior del mismo tipo.

Para eliminar un análisis importado:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación para la cual desea eliminar el análisis importado más reciente.

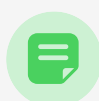
Aparecerá la página Versiones de la aplicación.

3. Haga clic en **Análisis**.

Aparecerá la página Análisis de la aplicación, donde se muestran los análisis ejecutados en la aplicación.



VERSIÓN	TIPO DE ANÁLISIS	TIPO DE EVALUACIÓN	TIPO DE DERECHO	ESTADO	INICIADO	COMPLETADO	N.º PROBLEMAS	
1	Móvil	Mobile Assessment	Análisis único	✓	2018/05/30	2018/05/30	0 1 1 69 85	...
1	Estático	Mobile Basic	N/D	✗	2017/11/02	2017/11/02		...



Note

Se puede filtrar la lista de análisis para que solo se muestren los análisis ejecutados en una versión; para ello, haga clic en el nombre de la versión en la página Versiones de la aplicación.

4. Haga clic en **Cancelar análisis importado** en la columna de acción del análisis importado.

Aparecerá un mensaje de confirmación.

5. Haga clic en **Sí** para confirmar la cancelación del análisis.

El análisis se elimina, junto con todos los problemas asociados a él.

1.10.5.3. Integración con Secure Code Warrior

OpenText Core Application Security se ha asociado con Secure Code Warrior para proporcionar formación interactiva gratuita a los clientes de OpenText Core Application Security para las categorías de vulnerabilidad admitidas. Cuando revisan un problema, los usuarios pueden iniciar un módulo de formación desde el vínculo **Iniciar formación** en la pestaña **Recomendaciones** del panel Detalles del problema.

Los módulos consisten en desafíos cortos y prácticos en los que los usuarios analizan el diseño y el código del software en busca de vulnerabilidades y luego las corrigen o mitigan. Hay módulos de prueba disponibles para todas las categorías de vulnerabilidad admitidas por Secure Code Warrior. Los módulos están organizados de forma jerárquica por categoría, subcategoría e idioma.

OpenText Core Application Security no comparte información del usuario o de la organización con Secure Code Warrior. Puede comprarse formación adicional de Secure Code Warrior. Para obtener más información, consulte <https://www.securecodewarrior.com/>.

1.10.5.3.1. Inicio de la formación de Secure Code Warrior

Para iniciar la formación de Secure Code Warrior para un problema:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en **Sus versiones**.

Aparecerá la página Sus versiones.

3. Seleccione una versión de la lista.

4. Haga clic en **Problemas**.

Aparecerá la página Problemas de versión.

5. En el panel de navegación, seleccione un problema de una categoría en la que esté disponible la formación de Secure Code Warrior.

6. Seleccione la pestaña **Recomendaciones**.

930712 <https://zero.webappsecurity.com:443/>

Crítico Insecure Transport: Weak SSL Cipher

Vulnerabilidad **Recomendaciones** Código Diagrama Más pruebas Historial

Recomendación

Deshabilite la compatibilidad con cifrados débiles en el servidor. En general, se definen como cifrados débiles:

- Todos los cifrados con clave de longitud inferior a 128 bits
- Los conjuntos de cifrado de clase de exportación
- Los cifrados NULL
- Los cifrados compatibles con modos no autenticados
- Los cifrados evaluados a niveles de seguridad inferiores a 112 bits
- Todos los cifrados RC4
- Todos los cifrados de bloques de 64 bits

Los siguientes cifrados admitidos por el servidor son débiles y deben deshabilitarse:

- En Apache, modifique las líneas siguientes en httpd.conf o ssl.conf:
 - SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:!RC4:!RC2:!DES:!3DES:+HIGH:+MEDIUM
- En IIS, consulte los artículos de Microsoft Knowledge Base:
 - Id. de artículo: 187498
 - Id. de artículo: 245030 y
 - Security Guidance for IIS
 - Id. de artículo: 2868725
- En otros servidores, consulte la documentación específica del proveedor.

Los siguientes cifrados admitidos por el servidor deben proporcionar la protección adecuada y pueden mantenerse habilitados:

Consejos

Todos los cifrados débiles se han obtenido estableciendo una conexión SSL con el host de destino y especificando el cifrado que se deseaba probar en el mensaje Client Hello de la etapa de sincronización SSL.

7. En la sección **Formación interactiva**, puede llevar a cabo las siguientes tareas:

- Para iniciar un módulo de formación, haga clic en **Iniciar formación**.
- Para ver un vídeo sobre la categoría del problema, haga clic en **Ver vídeo**.
- Para obtener más información sobre la categoría del problema, haga clic en los vínculos de recursos educativos externos.

NOVEDAD Formación interactiva ?

INICIAR FORMACIÓN

Ver vídeo

1. OWASP Top Ten 2017 A3: Exposición de datos sensibles
2. OWASP Top Ten Proactive Controls 2018 C8: Proteger datos en todas partes
3. OWASP Top Ten 2021 A02: Fallas criptográficas



Note

Si el problema no pertenece a una categoría de vulnerabilidad admitida, se le redirigirá a la página principal de Secure Code Warrior.

1.10.5.4. Integración con Slack para las notificaciones

OpenText Core Application Security ofrece la integración con Slack para la publicación de notificaciones en Slack. Los líderes en seguridad pueden configurar uno o más webhooks para el inquilino. Cuando se hayan configurado los webhooks, los líderes en seguridad pueden habilitar la publicación de notificaciones en Slack al crear las suscripciones de notificaciones.

Esta sección contiene los siguientes temas:

- [Configuración de la integración con Slack](#)
- [Eliminación de la integración con Slack](#)

1.10.5.4.1. Configuración de la integración con Slack

Puede configurar la integración con Slack mediante la configuración de uno o más webhooks para el inquilino.

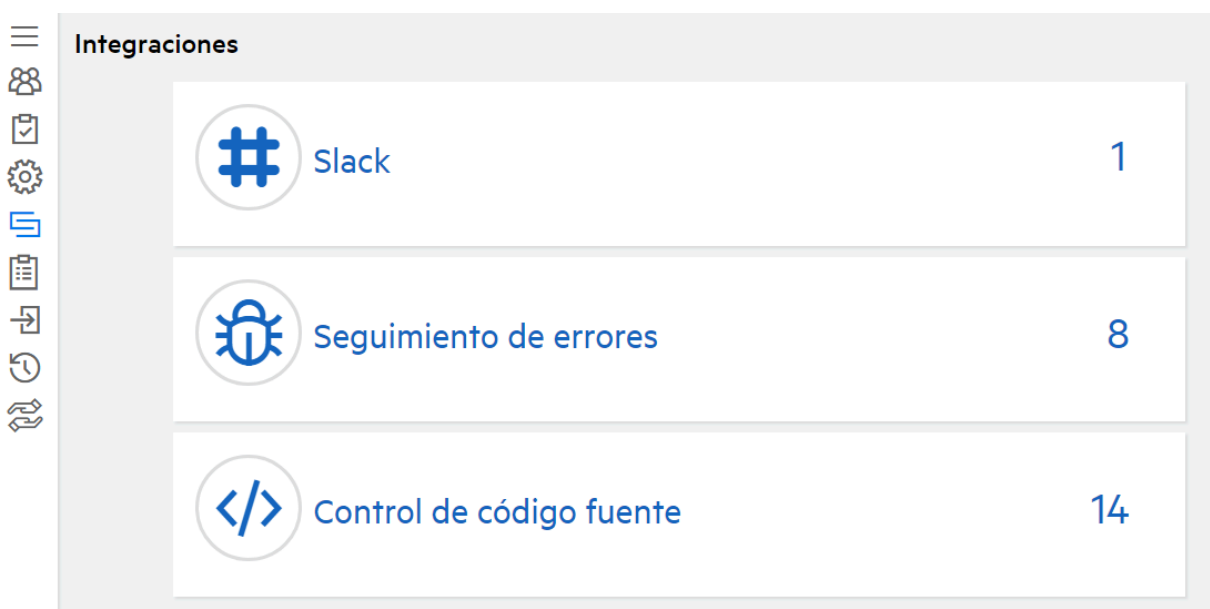
Para configurar un webhook:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Haga clic en **Integraciones**.

Aparecerá la página **Integraciones**.



3. Expanda la sección **Slack**.



4. Haga clic en **Agregar integración**.

- Si actualmente no ha iniciado sesión en un espacio de trabajo, se le redirigirá a la página de inicio de sesión del espacio de trabajo de Slack.
- Si ya ha iniciado sesión en uno o más espacios de trabajo, se le redirigirá a la página de autorización.



Note

Debe disponer de permiso para administrar aplicaciones e integraciones para el espacio de trabajo.

5. Si no ha iniciado sesión en el espacio de trabajo al que desea conectarse, complete el proceso de inicio de sesión. De lo contrario, vaya al siguiente paso.
6. Si aún no lo ha hecho, seleccione el espacio de trabajo en la lista de la parte superior derecha de la página de autorización.



En foddoc, a Fortify on Demand le gustaría:

Confirmar tu identidad en foddoc

Publicar en

Seleccionar canal

Cancelar

Autorizar

7. Seleccione el canal o el mensaje directo del usuario en el que se publicarán las notificaciones. Los valores disponibles son los canales y las cuentas de usuario a las que tiene acceso.
8. Haga clic en **Autorizar** para autorizar el acceso de OpenText Core Application Security a su cuenta de Slack.

Se le redirigirá a OpenText Core Application Security. Aparecerá un mensaje indicando que la integración con Slack se ha realizado correctamente. Ahora

puede habilitar la publicación de notificaciones en el canal. Para obtener información sobre cómo habilitar la publicación de notificaciones en Slack, consulte [Creación de una suscripción individual](#) y [Creación de una suscripción global](#).

.

1.10.5.4.2. Eliminación de la integración con Slack

Puede eliminar una integración con Slack de OpenText Core Application Security de las siguientes maneras:

- Los propietarios y usuarios de espacios de trabajo de Slack que tengan permiso para administrar aplicaciones pueden quitar autorizaciones específicas o la aplicación OpenText Core Application Security del espacio de trabajo de Slack. Esto provocará errores de las publicaciones en Slack.
- Los líderes en seguridad pueden eliminar los webhooks en OpenText Core Application Security.

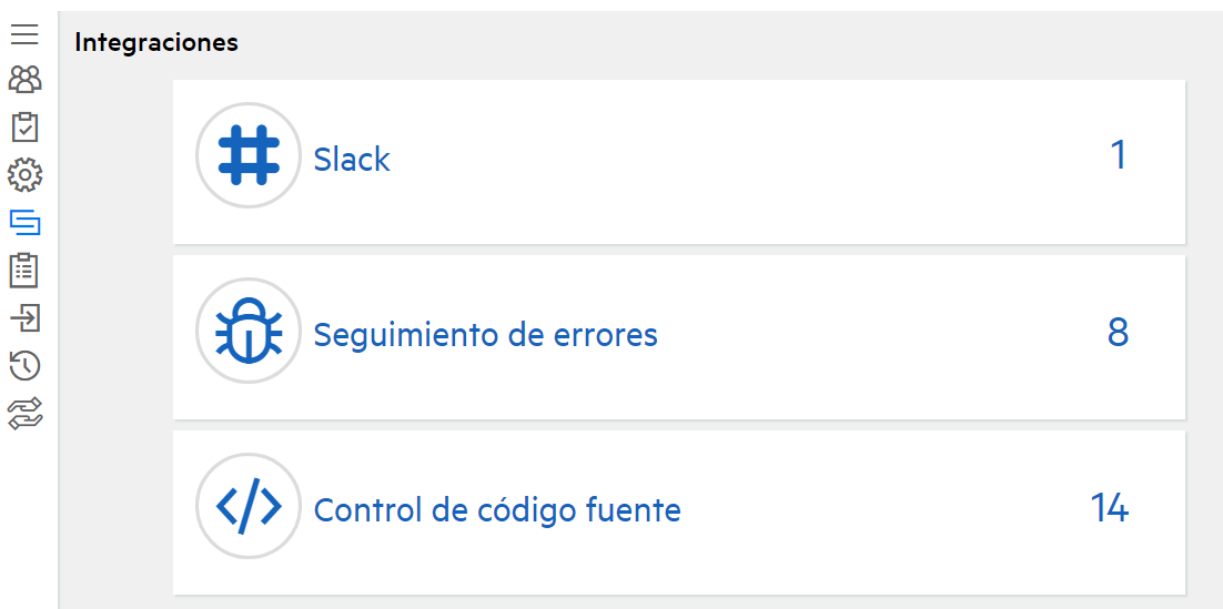
Para eliminar una integración con Slack:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Haga clic en **Integraciones**.

Aparecerá la página **Integraciones**.



3. Expanda la sección **Slack**.



4. Realice las siguientes tareas en función de sus preferencias y permisos de usuario:

- Para quitar autorizaciones en Slack:

1. Haga clic en  en la fila de un webhook.

Se le redirigirá a la página de OpenText Core Application Security en el directorio de aplicaciones de su espacio de trabajo.



Note

También puede acceder a la página desde el espacio de trabajo de Slack.

2. Quite las autorizaciones específicas o la aplicación para eliminar todas las autorizaciones. Para obtener más información acerca de cómo quitar aplicaciones de Slack, consulte la sección acerca de [cómo quitar aplicaciones e integraciones personalizadas del espacio de trabajo](#) en la documentación de Slack.

- Para quitar un webhook en OpenText Core Application Security:

1. Haga clic en  en la fila de un webhook.

El webhook se eliminará.

1.10.5.5. Integración de control de código fuente



Important

La integración del control de código fuente a través del portal es una integración heredada. Está previsto que esta función quede obsoleta. Los usuarios existentes deben migrar las integraciones de control de código fuente a las canalizaciones en las plataformas de control de versiones aplicables lo antes posible. Fortify ofrece plantillas de canalizaciones para varias plataformas de control de versiones, incluidas Bitbucket, GitHub y GitLab. Para obtener más información, consulte [Herramientas de CI/CD](#).

OpenText Core Application Security ofrece la integración de control de código fuente a través del portal para GitHub y Bitbucket. Esto permite que OpenText Core Application Security obtenga código fuente a partir de repositorios de esas plataformas para realizar evaluaciones estáticas.

Se admiten los siguientes lenguajes: Java, JavaScript, .NET, PHP y Python. Los requisitos de preparación del código para cargarlo en OpenText Core Application Security siguen siendo los mismos que los descritos en [Preparación de archivos en evaluaciones estáticas](#). Para .NET y Java, se recomienda que compile previamente los archivos y los cargue en una versión para garantizar la aceptación de la carga.

La integración de control de código fuente se configura a nivel de aplicación. Una vez configurada, los usuarios pueden seleccionar una rama o una versión para cargar al iniciar una evaluación estática.

Esta sección contiene los siguientes temas:

- [Configuración de la integración de control de código fuente con Bitbucket](#)
- [Configuración de la integración de control de código fuente con GitHub](#)

1.10.5.5.1. Configuración de la integración de control de código fuente con Bitbucket



Important

La integración del control de código fuente a través del portal es una integración heredada. Está previsto que esta función quede obsoleta. Los usuarios existentes deben migrar las integraciones de control de código fuente a las canalizaciones en las plataformas de control de versiones aplicables lo antes posible. Fortify ofrece plantillas de canalizaciones para varias plataformas de control de versiones, incluidas Bitbucket, GitHub y GitLab. Para obtener más información, consulte [Herramientas de CI/CD](#).

La integración con Bitbucket requiere la adición de un usuario de OAuth en Bitbucket.

Siga los siguientes pasos para configurar la integración de control de código fuente con Bitbucket:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación que desee editar.

3. Haga clic en **Configuración**.

Aparecerá la página Resumen de aplicaciones.

4. Seleccione la pestaña **Control de código fuente**.

5. Seleccione **Bitbucket** de la lista **Plataforma de administración del código fuente**.

6. En los campos **Clave de cliente** y **Secreto del cliente**, escriba la clave y el secreto del usuario de OAuth que se generan en Bitbucket.

Para generar la clave y el secreto, agregue un usuario de OAuth en Bitbucket. Al configurar el usuario, asegúrese de realizar las siguientes acciones:

- Establezca la URL de devolución de llamada como `https://<dominio_de_fod>/Redirect/OAuth/` , donde `<dominio_de_fod>` representa el dominio y el esquema de OpenText Core Application Security.
 - EE. UU.: `ams.fortify.com`
 - EMEA: `emea.fortify.com`
 - APAC: `apac.fortify.com`
 - FedRAMP: `fed.fortify.com`
- Asigne el permiso de lectura a la cuenta, la pertenencia a espacios de trabajo, los proyectos y los repositorios.

Para obtener más información sobre la adición de un usuario de OAuth en Bitbucket, consulte la sección [Integrate another application through OAuth](#) de la documentación de Bitbucket.



Tip

Asegúrese de que la casilla de verificación **Este es un consumidor privado** esté seleccionada en la configuración del consumidor de OAuth de su espacio de trabajo.

7. Haga clic en **Autenticar**.

Si la autenticación se realizó de forma correcta, se lo redirige al sitio de Bitbucket.

8. Otorgue autorización a la aplicación OpenText Core Application Security para acceder a su cuenta.

Se rellenan los campos **Equipo** y **Repositorio**. El campo **Equipo** indica la cuenta de usuario y todos los equipos a cuyos repositorios tiene acceso.

9. En la lista **Equipo**, seleccione el equipo propietario del repositorio que se vinculará con la aplicación.

10. En la lista **Repositorio**, seleccione el repositorio.

11. Haga clic en **Guardar**.

Se guardarán los ajustes de integración de control de código fuente.

1.10.5.5.2. Configuración de la integración de control de código fuente con GitHub



Important

La integración del control de código fuente a través del portal es una integración heredada. Está previsto que esta función quede obsoleta. Los usuarios existentes deben migrar las integraciones de control de código fuente a las canalizaciones en las plataformas de control de versiones aplicables lo antes posible. Fortify ofrece plantillas de canalizaciones para varias plataformas de control de versiones, incluidas Bitbucket, GitHub y GitLab. Para obtener más información, consulte [Herramientas de CI/CD](#).

La integración con GitHub utiliza la aplicación de catálogo de GitHub de OpenText Core Application Security, que es exclusiva de cada centro de datos. La integración de control de código fuente con GitHub Enterprise no está disponible.

Para configurar la integración de control de código fuente con GitHub:

1. Seleccione la vista **Aplicaciones**.

Aparecerá la página Sus aplicaciones.

2. Haga clic en el nombre de la aplicación que desee editar.

3. Haga clic en **Configuración**.

Aparecerá la página Resumen de aplicaciones.

4. Seleccione la pestaña **Control de código fuente**.

5. Seleccione **GitHub** de la lista **Plataforma de administración del código fuente**.

6. Haga clic en **Autenticar**.

Si la autenticación es correcta, se lo redirige al sitio de GitHub.

7. Otorgue autorización a la aplicación OpenText Core Application Security para acceder a su cuenta.

Se rellenan los campos **Organización** y **Repositorio**. El campo **Organización** indica la cuenta de usuario y todas las organizaciones a cuyos repositorios tiene acceso.

8. En la lista **Organización**, seleccione la organización a la que pertenece el repositorio que se vinculará con la aplicación.
9. En la lista **Repositorio**, seleccione el repositorio.
10. Haga clic en **Guardar**.

Se guardarán los ajustes de integración de control de código fuente.

1.10.5.6. Seguimiento de integraciones configuradas

Los líderes en seguridad pueden llevar el seguimiento de integraciones configuradas por los usuarios con herramientas externas en todas las aplicaciones de OpenText Core Application Security. Actualmente, las integraciones disponibles para el seguimiento son: seguimiento de errores, control de código fuente y Slack.

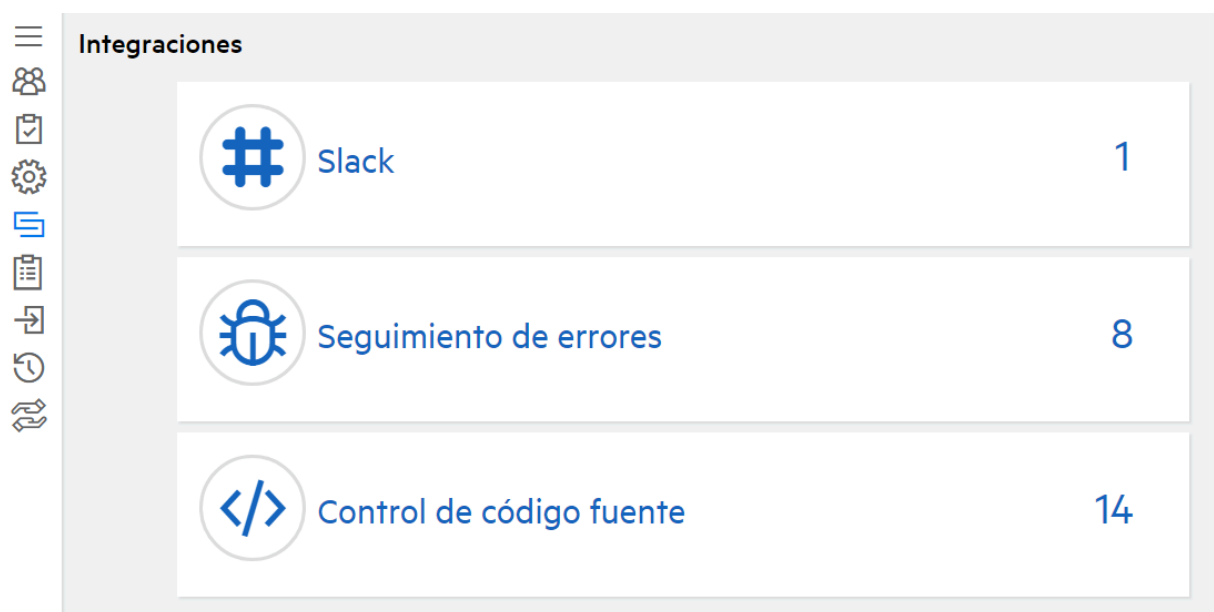
Para llevar el seguimiento de integraciones configuradas por los usuarios en el inquilino:

1. Seleccione la vista **Administración**.

Aparecerá la página **Administración de usuarios**.

2. Haga clic en **Integraciones**.

Aparecerá la página **Integraciones**.



3. Expanda las secciones que desee ver.


Slack
1

AGREGAR INTEGRACIÓN

Nombre de usuario	Nombre del equipo	Canal de webhook
HuangTam	foddoc	#random


Seguimiento de errores
8

APLICACIÓN	SEGUIMIENTO DE ERRORES	NOMBRE DE USUARIO	URL
KA Dynamic App101316	ALM.Net	TAMuser	http://16.103.234.248:8080/qcbin
Application KA	Microsoft TFS / VSTS	TAMtest	http://fodqa-tfs:8080/tfs/TAM
Dynamic Beta	Microsoft TFS / VSTS	TAMTest	http://fodqa-tfs:8080/tfs/TAM
Test 02-07-17_2	ALM Octane	kristine.cas.arellano@hpe.com	https://mqast001pngx.saas.hpe.com
HFD-1611 Test	Atlassian JIRA	TAMuser	http://16.103.235.2:8080/
17.4 Static Application	Atlassian JIRA	TAMuser	http://16.103.235.2:8080/
Mobile App 17.4	Atlassian JIRA	TAMuser	http://16.103.235.2:8080/
Mobile Test App 03	Atlassian JIRA	TAMuser	http://16.103.235.2:8080/


Control de código fuente
14

APLICACIÓN	PLATAFORMA DE ADMINISTRACIÓN
Dynamic Test App 01	GitHub
KA Dynamic App101316	GitHub
KA Test 072716	GitHub
Dynamic Scan 1-18	GitHub
KA Test 10-26-15	GitHub
0131 App	GitHub
Application KA	Bitbucket
Test 02-07-17_2	GitHub
Test 02-07-17	Bitbucket
Dynamic Beta	GitHub
Test 02-06-17	GitHub
17.4 Static Application	GitHub
Test Issue Filters	GitHub
Mobile 02-07-18	GitHub

4. Puede realizar las siguientes acciones:

- Slack: haga clic en los vínculos en la fila de un webhook para quitar autorizaciones específicas o para eliminar el webhook. Para obtener más

información, consulte [Eliminación de la integración con Slack](#).

- Seguimiento de errores: haga clic en el vínculo de una fila de la aplicación para que le redirija a la configuración de seguimiento de errores de la aplicación. Para obtener más información, consulte [Configuración de la integración con el seguimiento de errores](#).
- Control de código fuente: haga clic en el vínculo de una fila de la aplicación para que le redirija a la configuración de control de código fuente de la aplicación. Para obtener más información, consulte [Integración de control de código fuente](#)

1.10.5.7. Webhooks

Los webhooks proporcionan una forma de entregar notificaciones a un servidor web externo cuando se producen eventos de análisis. Los usuarios con el permiso **Configurar webhooks** pueden configurar webhooks para que se desencadenen cuando se produce un evento suscrito. Los siguientes eventos están disponibles: inicio de análisis, pausa de análisis, reanudación de análisis, cancelación de análisis y finalización de análisis. Cuando se produce un evento al cual se ha suscrito un webhook, OpenText Core Application Security envía una carga de HTTP POST a la URL configurada del webhook. Los webhooks se pueden usar en lugar de hacer sondeos en canalizaciones CI/CD que incorporan análisis.

Esta sección contiene los siguientes temas:

- [Configuración de un webhook](#)
- [Solicitudes y respuestas de webhook](#)
- [Visualizar entregas de webhook](#)

1.10.5.7.1. Configuración de un webhook

Los usuarios con el permiso **Configurar webhooks** pueden configurar webhooks para el inquilino. Se debe asignar un webhook a una versión como mínimo.

Para configurar un webhook:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Webhooks**

Aparecerá la página Webhooks.

DIRECCIÓN	ID	DESCRIPCIÓN	ESTADO	
https://7e9ea9dc.ngrok.io/payload	20ef6006-0b73-4c9c-9a79-0f4306305685		Activo	EDITAR ASIGNAR VERSIONES ELIMINAR
https://16.103.234.171/Admin/Webhooks	5da568f3-fa37-4d0b-9dce-caeb421ef67d		Activo	EDITAR ASIGNAR VERSIONES ELIMINAR

3. Haga clic en **Agregar webhooks**.

Aparece la ventana Agregar/editar webhooks.

Agregar/Editar webhook

URL de carga

Descripción

Secreto

Supervisar todas las versiones de la aplicación

Activo

Qué eventos desea que desencadenen el webhook

Análisis iniciado

Análisis en pausa

Análisis reanudado

Análisis cancelado

Análisis completado

PROBAR WEBHOOK GUARDAR CANCELAR

4. Rellene los campos según sea necesario. Los siguientes campos son obligatorios a menos que se indique lo contrario.

Campo	Descripción
URL de carga	Escriba la URL del servidor que recibirá las solicitudes POST de webhook. Por ejemplo, <code>https://7e9ea9dc.ngrok.io/payload</code> .
Descripción	(Opcional) Escriba una frase que describa el webhook.

Campo	Descripción
Secreto	(Opcional) Escriba un secreto que se pueda usar para validar que las solicitudes de webhook enviadas a la URL de carga se hagan desde OpenText Core Application Security. El algoritmo HMAC-SHA256 se utiliza en combinación con el secreto para calcular un hash del cuerpo de carga. El resultado es el HMAC y se incluye en el encabezado de una solicitud como <code>X-FOD-Signature</code>. Tip  Para validar la solicitud de webhook, calcule el HMAC troceando el cuerpo de carga sin procesar utilizando el algoritmo HMAC-SHA256 en combinación con el secreto y luego codificando de manera hexadecimal el hash. Compruebe si el resultado coincide con el valor de <code>X-FOD-Signature</code>.

Campo	Descripción
Supervisar todas las versiones de la aplicación	◦ Establezca Sí para supervisar todas las versiones de la aplicación. ◦ Establezca No para supervisar versiones individuales (opción predeterminada). Puede especificar versiones para supervisar después de haber configurado el webhook.
Activo	◦ Establezca Sí para habilitar la entrega de las solicitudes de webhook (opción predeterminada). ◦ Establezca No para deshabilitar la entrega de las solicitudes de webhook.

5. Seleccione qué eventos de análisis desencadenarán el webhook.

6. Haga clic en **Probar webhook** para hacer ping en la URL de carga.

Aparece un mensaje que indica que «Se ha enviado el evento de ping correctamente» si el webhook se ha configurado correctamente.

7. Haga clic en **Guardar**.

El nuevo webhook aparecerá en la lista de webhooks.



Note

Puede buscar webhooks por dirección, descripción e id. completo. La coincidencia parcial de cadena es compatible con la dirección y la descripción.

8. Si eligió supervisar versiones individuales, haga clic en **Editar** en la fila del webhook.

Aparece la ventana Asignar versiones.

Asignar versiones



Seleccionado

Disponible

Buscar



101 encontrados

|< < 3 4 **5**

Mostrar: **25** 50 100

APLICACIÓN

VERSIÓN

☐	アプリケーション名84	r2

GUARDAR

CANCELAR

9. Seleccione las versiones que supervisará el webhook y haga clic en **Guardar**.

El webhook ahora está asignado a las versiones seleccionadas.

1.10.5.7.2. Solicitudes y respuestas de webhook

OpenText Core Application Security envía información sobre los eventos de webhook como solicitudes de HTTP POST con la carga de JSON como el cuerpo de la solicitud.



Note

La verificación de SSL está habilitada de forma predeterminada. Si la URL de la carga es HTTPS, OpenText Core Application Security verificará los certificados SSL cuando se envían solicitudes de webhook.

Ejemplo de solicitud

El siguiente ejemplo muestra una solicitud con una firma hash en el encabezado como `X-FOD-Signature` y la carga de JSON.

Encabezado:

```
connection: close expect: 100-continue content-length: 324 host:
webhook.site content-type: application/json; charset=utf-8 x-
fod-signature:
4F837B0AE04303E975BBBCF9FFBBC09E0016013835757BD611C20F7930711980F
x-fod-deliveryid: f8d97b5e-4cae-414b-aa84-8de766f8116f
```

Carga:

```
{ "deliveryId": "f8d97b5e-4cae-414b-aa84-8de766f8116f",
"eventName": "scan_started", "payload": { "scanId": 31278,
"tenantId": 1126, "applicationId": 14155, "applicationName":
"Zero", "releaseId": 16149, "releaseName": "v1", "scanType":
"dynamic" }, "webhookId": "a798dc91-3242-4dc6-8188-
2fd3e4aae86e", "triggeredAt": "2021-07-02T16:08:28.5496187Z" }
```

Ejemplo de respuesta:

El siguiente ejemplo muestra la respuesta recibida por OpenText Core Application Security.

```
Transfer-Encoding = chunked Vary = Accept-Encoding X-Request-Id
= e9cbce0c-108f-46e9-b2cc-89f6f0104dca X-Token-Id = 89be42d3-
a8dd-4414-9e31-6b09a5590ee5 Cache-Control = no-cache, private
Date = Fri, 02 Jul 2021 16:08:29 GMT Set-Cookie =
laravel_session=CRuQJLoiFx9ay1UV88ufH83vC0jq1PL0JN0wY59v;
expires=Fri, 02-Jul-2021 18:08:29 GMT; Max-Age=7200; path=/;
httponly Server = nginx/1.14.2
```

1.10.5.7.3. Visualizar entregas de webhook

Los usuarios con el permiso **Configurar webhooks** pueden ver los detalles de las entregas de webhook, incluyendo la solicitud de HTTP (incluyendo la carga) y la respuesta.

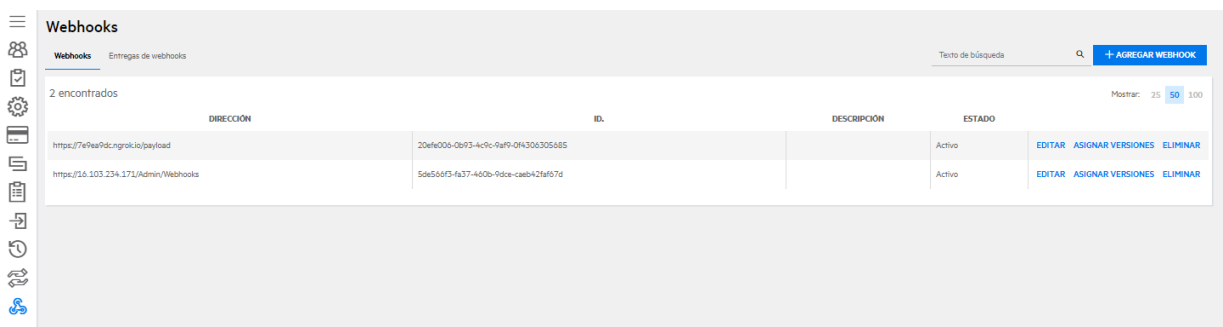
Para ver la lista de entregas de webhook:

1. Seleccione la vista **Administración**.

Aparecerá la página Administración de usuarios.

2. Haga clic en **Webhooks**

Aparecerá la página Webhooks.

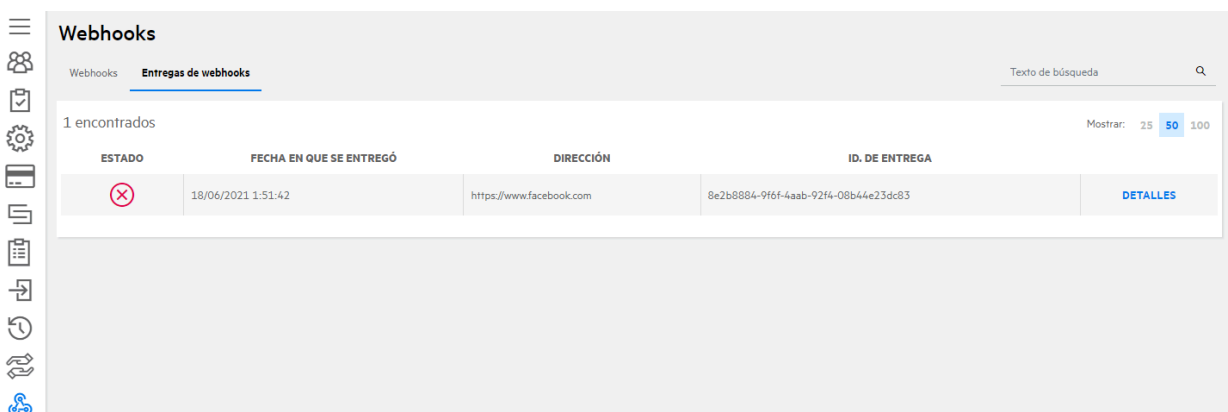


The screenshot shows the 'Webhooks' management interface. It features a sidebar with navigation icons and a main content area. The main area has a search bar and a '+ AGREGAR WEBHOOK' button. Below this, it indicates '2 encontrados' (2 found). The table has columns for 'DIRECCIÓN', 'ID.', 'DESCRIPCIÓN', and 'ESTADO'. Two webhooks are listed, both with 'Activo' status. Each row has links for 'EDITAR', 'ASIGNAR VERSIONES', and 'ELIMINAR'.

DIRECCIÓN	ID.	DESCRIPCIÓN	ESTADO
https://7e9ea9dc.ngrok.io/payload	20ef6006-0b73-4c9c-9a79-0f4306305685		Activo
https://16.103.234.171/Admin/Webhooks	5da568f3-fa37-4d0b-9dce-caeb421ef67d		Activo

3. Seleccione la pestaña **Entregas de webhook**.

Aparece una lista de entregas de webhook.



The screenshot shows the 'Webhooks' management interface with the 'Entregas de webhook' tab selected. It indicates '1 encontrados' (1 found). The table has columns for 'ESTADO', 'FECHA EN QUE SE ENTREGÓ', 'DIRECCIÓN', and 'ID. DE ENTREGA'. One delivery is listed with a status of 'Error' (indicated by a red X icon), a date of '18/06/2021 1:51:42', a direction of 'https://www.facebook.com', and an ID of '8e2b8884-9f6f-4aab-92f4-08b44e23dc83'. A 'DETALLES' link is present for this entry.

ESTADO	FECHA EN QUE SE ENTREGÓ	DIRECCIÓN	ID. DE ENTREGA
	18/06/2021 1:51:42	https://www.facebook.com	8e2b8884-9f6f-4aab-92f4-08b44e23dc83



Note

Puede buscar entregas de webhook por dirección (coincidencia parcial de cadena compatible) y un id. completo.

4. Haga clic en **Detalles** en la fila de una entrega de webhook.

Aparece la ventana Entrega de webhook que contiene la solicitud HTTP y la respuesta.

Solicitud:

Webhook Delivery

8909f981-4cee-4af7-a8cd-418a12ee9aee

https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4

6/30/2021, 11:37:47 PM

Request

Response

Headers

X-FOD-DeliveryId = 8909f981-4cee-4af7-a8cd-418a12ee9aee
X-FOD-Signature = 6B5D3EF8315ADFE4728ADCC40ACCE437CB5F215CF8D386B3622B5C6A3EC53A4D

Content

```
{
  "deliveryId": "8909f981-4cee-4af7-a8cd-418a12ee9aee",
  "eventName": "scan_completed",
  "payload": {
    "scanId": "31246",
    "tenantId": "1126",
    "applicationId": "12237",
    "applicationName": "WebGoat",
    "releaseId": "12672",
    "releaseName": "8.0",
    "scanType": "static",
    "notes": "Scan Job Id 12549 : FPR IMPORT SUCCESSFUL AND AUTOMATICALLY RELEASED",
    "webhookId": "f16b45d0-9631-4af6-9db7-7132d60a1b21",
    "triggeredAt": "2021-07-01T03:37:47.3105424Z"
  }
}
```

Respuesta:

Webhook Delivery

✓

3c727595-35c6-4775-a91b-96006f34a168

https://hooks.slack.com/services/TALM3FNGL/B026W8DLTU4

7/1/2021, 2:31:11 AM

Request

Response

Headers

x-frame-options = SAMEORIGIN

x-xss-protection = 0

vary = Accept-Encoding

referrer-policy = no-referrer

x-slack-backend = r

strict-transport-security = max-age=31536000; includeSubDomains; preload

Date = Thu, 01 Jul 2021 06:31:50 GMT

Content

This PDF was generated on February 12, 2026

Page 768 of 784

1.10.6. Cursos de formación

OpenText Core Application Security se asoció con Security Innovations para ofrecer cursos de formación en materia de desarrollo seguro. Revise su contrato para verificar si se incluyen. Si le interesa agregar cursos, póngase en contacto con su representante de ventas.

Esta característica requiere que se habilite el uso de ventanas emergentes y cookies para el portal.

1.10.6.1. Visualización de los cursos de formación

Para ver los cursos de formación asignados:

1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá la página Formación. La pestaña Cursos muestra una lista de los cursos asignados con la siguiente información: nombre del curso, currículo principal, id. de módulo, estado de finalización del curso, fecha del último intento, fecha de aprobación y vínculo del curso.

2. Realice una de las siguientes acciones:

- Haga clic en el vínculo **Iniciar curso** de la fila de un curso para iniciarlo.



Note

Al iniciar un curso, se restablecerá el estado de finalización, pero no la fecha de aprobación. Cuando finalice, cierre la ventana del curso para garantizar que los resultados se registran correctamente.

- Haga clic en el vínculo **Reanudar curso** de la fila de un curso para continuar desde donde lo dejó.
- Haga clic en el vínculo **Examinar curso** de la fila de un curso para ver el contenido sin que eso afecte al estado de finalización ni a la fecha de aprobación.

Aparecerá un mensaje de confirmación.

3. Haga clic en **Sí**.

El curso aparecerá en una nueva ventana.

1.10.6.2. Asignación de cursos de formación

Puede asignarse a usted mismo los cursos de formación disponibles para el inquilino. Además, los usuarios con los permisos **Administrar usuarios** pueden asignar cursos de formación a todos los usuarios activos del inquilino. Los cursos se agrupan en diferentes tipos de currículum y se asignan como un currículum.

Para asignar cursos de formación a otro usuario o a usted mismo:

1. Haga clic en el icono  en la barra de herramientas del portal.

Aparecerá la página Formación.

2. Seleccione la pestaña **Asignación**.

Formación						
Informe		Tareas				
						Texto de búsqueda
20 encontrados						Mostrar: 25 50 100
NOMBRE DE USUARIO	NOMBRE	APELLIDO	CORREO ELECTRÓNICO	ROL	CURRÍCULO DEL CURSO	
bigdaddy	Big	Dad	bd@gmail.com	Líder en aplicaciones		
careena	Careena	R	pacabig@microfocus.com	Líder en seguridad		
carla_seclead	carla	kamil	carla.kam.dacaynos@microfocus.com	Líder en seguridad		
chu_seclead	Oleksii	Chudnovskiy	oleksii.chudnovskiy@microfocus.com	Líder en seguridad		
enzo_testUAT	Lorenzo	Ponon	enzo.ponon@outlook.com	Ejecutivo		
hamtan_sec	Hamid	Navbary	hamid.navbary@microfocus.com	Líder en seguridad		
jarib_uat	Jarib Micah	Cruz	jaribmicah.cruz@microfocus.com	Líder en seguridad		
jdevila_Application_lead	Jose	Devila	jdevila777@gmail.com	Líder en aplicaciones		
leola_test	lelele	Apao	alexander.apao@microfocus.com	Líder en seguridad		

Si su rol tiene el permiso **Administrar usuarios**, aparecerá la lista de usuarios activos y sus currículos asignados en el inquilino. De lo contrario, solo verá su cuenta de usuario y los currículos que tenga asignados.

3. Haga clic en  junto a un usuario.

Aparecerá la ventana modal Currículo del curso.

4. Active las casillas junto a los currículos que desea asignar al usuario.

Haga clic en **Guardar**.

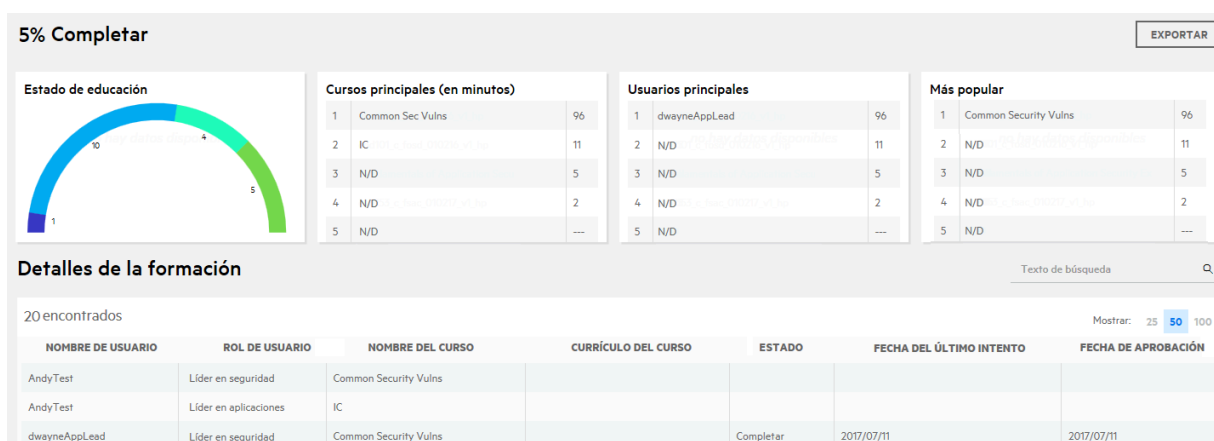
La pestaña **Asignación** mostrará los cambios guardados.

1.10.6.3. Visualización del informe de formación

Los usuarios con el permiso **Administrar usuarios** pueden hacer un seguimiento del progreso de los usuarios en los cursos de formación asignados en el inquilino accediendo al informe de progreso de formación. El informe proporciona un resumen a nivel de inquilino de la actividad de los usuarios y una lista de los estados de finalización de los cursos de cada usuario.

Para ver el informe de formación:

- Haga clic en el icono  en la barra de herramientas del portal.
- Aparecerá la página Formación.
- Seleccione la pestaña **Informe**.



En la pestaña se muestra la siguiente información:

- El porcentaje de cursos asignados que se han completado.
- Gráficos que resumen el progreso y las tendencias de los usuarios:
 - Estado de educación:** el número de cursos completados, en curso o no iniciados.
 - Cursos principales:** los cursos más activos en cuanto a la cantidad de minutos dedicados.
 - Usuarios principales:** los usuarios más activos en cuanto a la cantidad de cursos realizados.
 - Más popular:** los cursos que más se han realizado.
- La cuadrícula **Detalles de la formación**, la cual muestra en cada fila al usuario de inquilino, el curso asignado, el estado de progreso del curso, la

fecha del último acceso al curso y la fecha de la última finalización del curso.

3. Haga clic en **Exportar** para exportar la cuadrícula **Detalles de la formación** como un archivo CSV. Los resultados de búsqueda se aplican a la exportación.

1.11. Directivas y soporte técnico

Consulte las directivas de OpenText Core Application Security para obtener información acerca de la administración y mantenimiento del portal. Si tiene más preguntas, póngase en contacto con el soporte técnico.

Esta sección contiene los siguientes temas:

- [Programación de mantenimiento y actualizaciones de software](#)
- [Directiva de retención de datos](#)
- [Obtención de soporte técnico](#)



1.11.1. Programación de mantenimiento y actualizaciones de software

OpenText Core Application Security proporciona la siguiente información relacionada con la programación de mantenimiento y las actualizaciones de software.

Programación de mantenimiento

Para ayudar a los clientes a planificar el mantenimiento programado, OpenText Core Application Security reserva períodos de tiempo predefinidos que se usarán según sea necesario: un intervalo semanal de dos (2) horas (jueves, de 00:00 a 02:00) y un (1) intervalo mensual de cuarenta y ocho (48) horas (de las 00:00 del sábado a las 00:00 del domingo). Estos intervalos de mantenimiento se usarán según sea necesario y, en la gran mayoría de los casos, no afectarán a la capacidad de los usuarios para acceder a la funcionalidad de OpenText Core Application Security ni para sacar partido de esta.

El intervalo de mantenimiento de cada centro de datos se establece con las siguientes zonas horarias:

Centro de datos	Zona horaria de mantenimiento
AMS (América)	Hora oriental de Estados Unidos
EMEA (Europa, Oriente Medio y África)	Hora del meridiano de Greenwich
APAC	Hora de Australia oriental

Para obtener detalles adicionales sobre el mantenimiento programado en otros entornos, comuníquese con el soporte técnico.

Actualizaciones de software

OpenText Core Application Security determina si se desarrollan, publican y aplican actualizaciones de software en la plataforma y los componentes de apoyo de OpenText Core Application Security, así como el momento en que se realizarán estas acciones. Las versiones principales se suelen publicar de forma trimestral, mientras que las versiones secundarias y las revisiones se publican según sea necesario. A menos que OpenText Core Application Security anticipe una interrupción del servicio debido a una actualización de software, puede que OpenText Core Application

Security implemente una actualización de SaaS en cualquier momento sin avisar al cliente. OpenText Core Application Security pretende emplear el intervalo de mantenimiento programado mensual con el fin aplicar actualizaciones de software principales.

Las actualizaciones de contenido de seguridad para ampliar y mejorar la capacidad de OpenText Core Application Security para identificar las vulnerabilidades son un componente clave del servicio de OpenText Core Application Security. El equipo de Fortify Software Security Research (SSR) desarrolla las actualizaciones de contenido de seguridad, las cuales se suelen publicar al final de cada trimestre natural. OpenText Core Application Security normalmente implementa contenido de seguridad actualizado algunas semanas después de la publicación. Las actualizaciones de contenido de seguridad se pueden implementar fuera de las actualizaciones trimestrales como respuesta a nuevas e importantes amenazas o vulnerabilidades de día cero. OpenText recomienda a los usuarios mantenerse actualizados con la última información de seguridad siguiendo el [blog de ciberseguridad](#).

1.11.2. Directiva de retención de datos

OpenText Core Application Security ha implementado la siguiente directiva de retención de datos para los clientes a partir de la versión v18.4. OpenText recomienda a los clientes que revisen y descarguen los archivos que deseen conservar y que estén fuera de los intervalos de retención de datos.

Recursos	Tipo de archivo	Período de retención
Exportaciones de datos (páginas Problemas de la aplicación y Problemas de versión)	.csv	7 días
Código fuente	.zip	15 días
Archivos binarios de aplicaciones móviles	.ipa, .apk	30 días
Notificaciones	-	3 meses
Exportaciones de datos (página Informes global)	.csv	3 meses
Registro de eventos	.csv	13 meses
Informes generados por los usuarios	.pdf, .html	2 años
Archivos de resultados de análisis de Fortify	.fpr	2 años
Lista de materiales de software (SBOM)	.json	2 años
Árboles del sitio	.csv	2 años

Recursos	Tipo de archivo	Período de retención
Datos de aplicaciones	-	Controlado por el cliente*
Datos de versiones	-	Controlado por el cliente*
Datos de problemas	-	Controlado por el cliente*
Datos de usuarios	-	Controlado por el cliente*

*El cliente es responsable de crear y eliminar los datos especificados siempre que el cliente mantenga un estado activo con OpenText Core Application Security. El cliente puede eliminar una aplicación, una versión o un usuario en cualquier momento. También se eliminan los datos de problemas asociados con una aplicación o una versión. Tras la terminación del servicio de OpenText Core Application Security, el período de recuperación de los datos de terminación es de 30 días.

Para obtener más información, comuníquese con el soporte técnico.

1.11.3. Obtención de soporte técnico

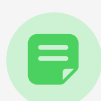
OpenText Core Application Security ofrece soporte técnico a través de recursos de autoservicio y mediante el Centro de ayuda de , el cual está disponible de manera ininterrumpida y cuenta con un equipo de soporte dedicado. Los recursos de autoservicio incluyen demostraciones de vídeo, una base de conocimiento y documentación de producto. Si tiene algún problema sin resolver, inicie un chat activo con el soporte técnico o envíe un vale de soporte técnico en el Centro de ayuda envíe una solicitud al [correo electrónico de asistencia específico de FEDRamp](#). Puede llamar al soporte técnico al 800.893.8141 o al 650.800.3233 si no tiene acceso a Internet.

Esta sección contiene los siguientes temas:

- [Acceso a los recursos de soporte técnico](#)
- [Envío de un vale del Centro de ayuda](#)
- [Seguimiento de los vales del Centro de ayuda](#)

1.11.3.1. Acceso a los recursos de soporte técnico

Los recursos de soporte técnico están disponibles a través del portal. El portal contiene vínculos directos a vídeos instructivos, a la guía del usuario en formato HTML, al chat activo y al centro de ayuda. El Centro de ayuda es el sistema de vales de soporte técnico de OpenText Core Application Security. También hospeda la base de conocimientos y la guía del usuario en formato PDF. .



Note

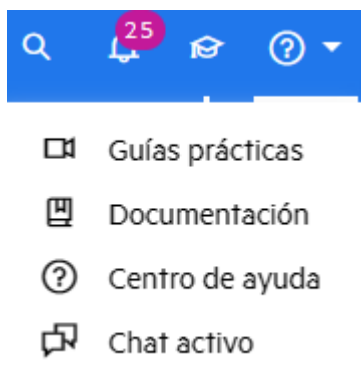
Puede iniciar sesión directamente en el Centro de ayuda a través de la URL correspondiente mediante las credenciales de OpenText Core Application Security:

- AMS: <https://helpcenter.ams.fortify.com>
- EMEA: <https://helpcenter.emea.fortify.com>
- APAC: <https://helpcenter.apac.fortify.com>
- SGP: <https://fodsgp.zendesk.com/>

Para acceder a los recursos de soporte técnico:

1. Haga clic en el menú de ayuda y seleccione uno de los siguientes elementos:

- **Guías prácticas:** abre [guías de vídeos de instrucciones](#), parte de las ofertas de formación digital de Fortify.
- **Documentación:** abre la guía del usuario.
- **Centro de ayuda:** abre el Centro de ayuda
- **Chat activo:** abre la ventana del Chat activo, donde puede conversar con el soporte técnico en cualquier momento.



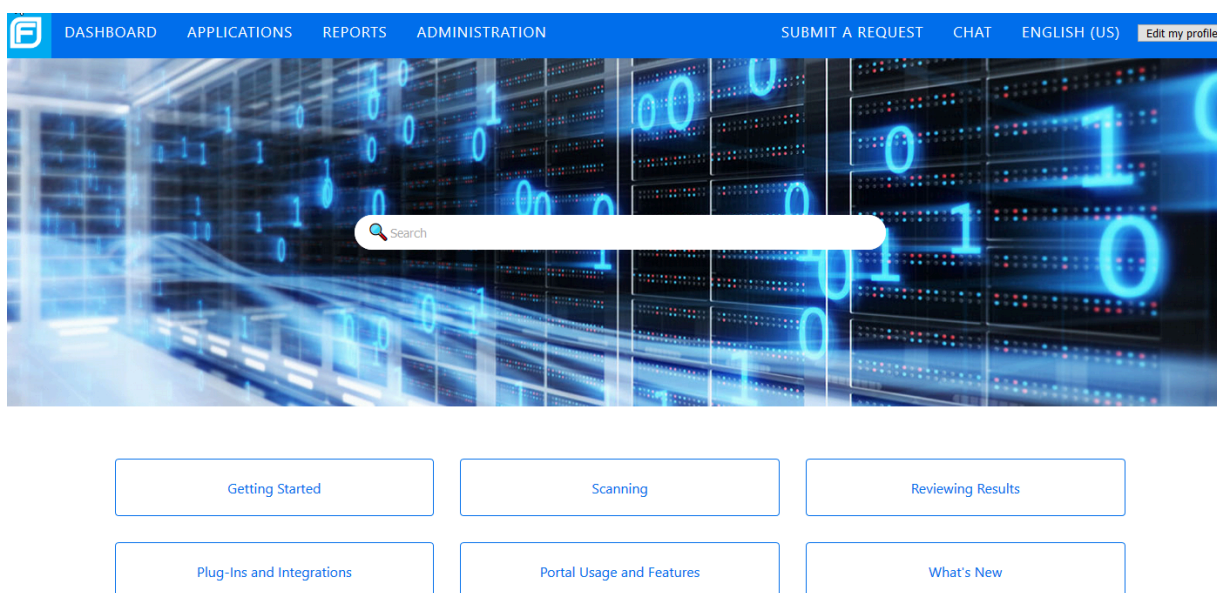
1.11.3.2. Envío de un vale del Centro de ayuda

Envíe un vale de soporte técnico del Centro de ayuda.

Para enviar un vale del Centro de ayuda:

1. Haga clic en el menú de ayuda y seleccione **Centro de ayuda**.

El Centro de ayuda se abrirá en una ventana nueva.



2. Haga clic en **Enviar un vale**.

Aparecerá el formulario **Enviar solicitud**.

3. Seleccione el tipo de vale de la lista desplegable:

- **Crear un vale:** obtenga ayuda con una pregunta general sobre el producto o un problema específico del inquilino.
- **Envío de defecto de FoD:** informe de un problema o un error
- **Envío de mejora de FoD:** solicite una mejora.

4. Complete los campos que se muestran para el tipo de vale seleccionado. Proporcione la mayor cantidad de detalles posible.

5. Haga clic en **Enviar**.

Un mensaje en la parte superior de la página indica que se envió el vale del Centro de ayuda.

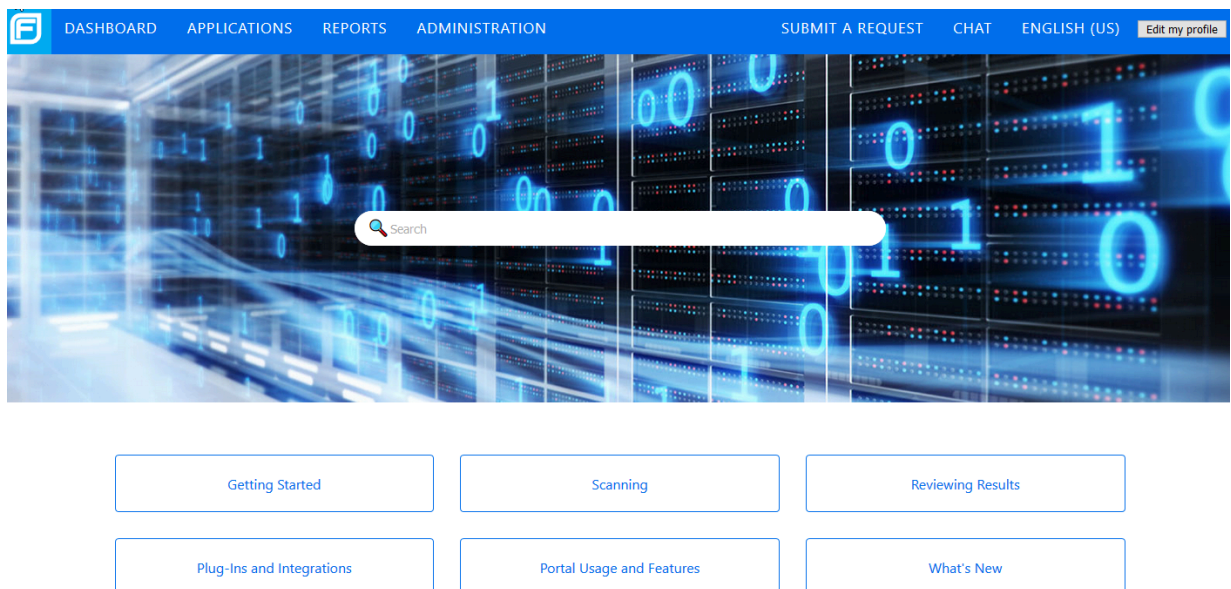
1.11.3.3. Seguimiento de los vales del Centro de ayuda

Puede supervisar los vales de soporte técnico enviados para el inquilino del Centro de ayuda. Solo podrá ver los vales que haya enviado, a los que haya sido asignado y en los que haya sido copiado (si está en una lista de notificaciones de la aplicación, se lo agregará automáticamente a vales vinculados con la aplicación).

Siga los siguientes pasos para realizar el seguimiento de los vales del Centro de ayuda:

1. Haga clic en el menú de ayuda y seleccione **Centro de ayuda**.

Se le redirigirá al Centro de ayuda.



2. Haga clic en **Ver vales**.

Aparecerán los vales. Los vales tienen uno de los siguientes estados:

- **Abierto:** su solicitud se ha recibido y asignado a un soporte técnico que está trabajando en el problema para resolverlo.
- **Esperando su respuesta:** el soporte técnico asignado tiene una pregunta de seguimiento para usted. Los vales que se establecen en el estado Pendiente suelen permanecer en este estado hasta que responde y proporciona la información que el soporte técnico necesita para continuar resolver el problema.
- **Resuelto:** el soporte técnico ha resuelto el problema. Los vales resueltos se cierran automáticamente a los siete días de haberse definido en este

estado. Puede volver a abrir un vale hasta que se cierra.

- **Cerrado:** el vale está completado y no se puede reabrir. Si necesita ayuda adicional para el vale original, cree una solicitud de seguimiento.

3. Para limitar el número de vales que se ven, filtre la lista con los filtros de **Estado:**

- **Cualquiera:** muestra todos los vales.
- **Abierto:** muestra los vales en los que el equipo de soporte técnico aún está trabajando.
- **Esperando su respuesta:** muestra los vales que requieren una acción por parte de su organización.
- **Resuelto:** muestra los vales que se resolvieron.



© Copyright 2026 Open Text

For more info, visit <https://docs.microfocus.com>
