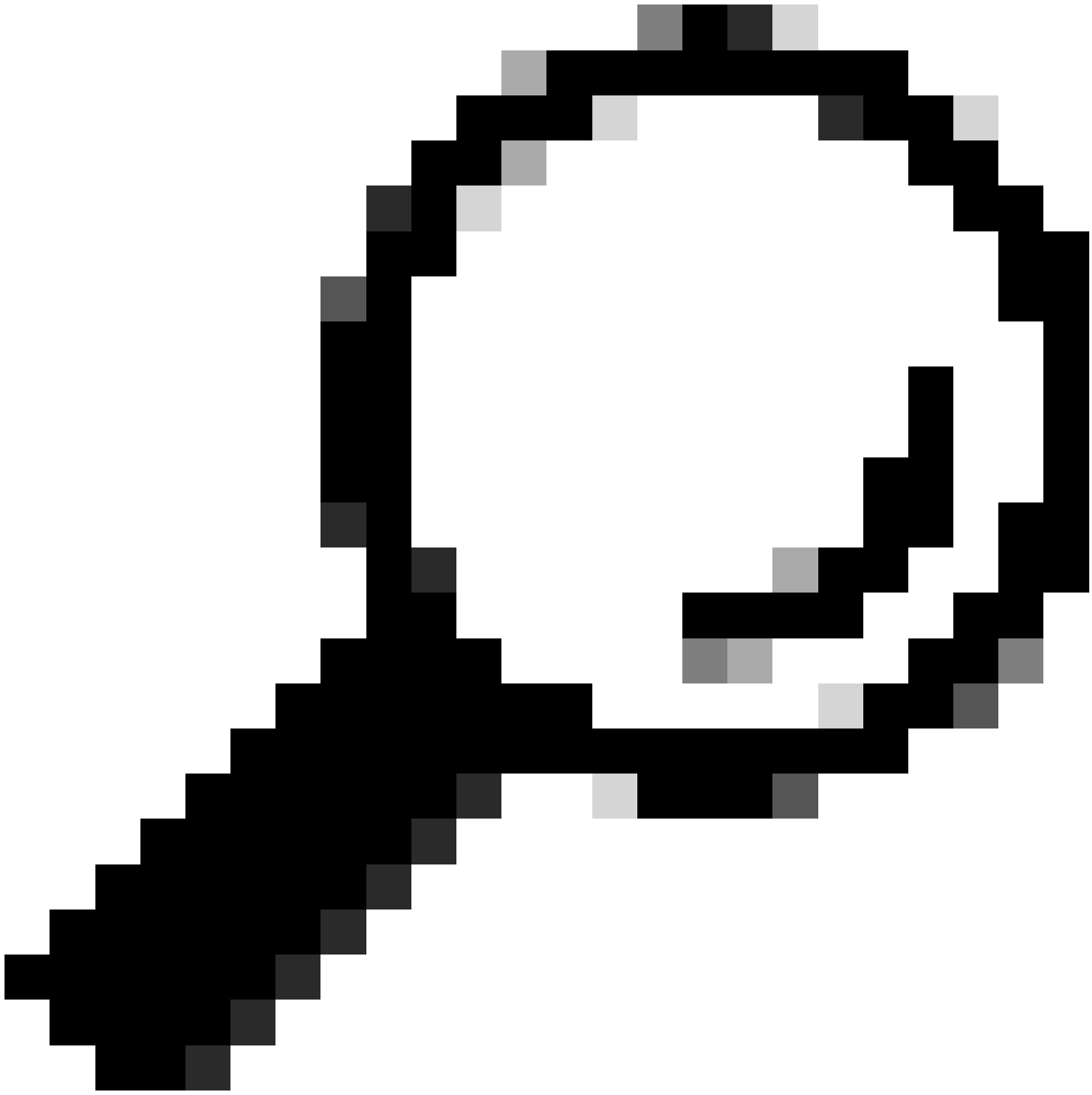
# Secure Network Analytics Descripción de la Guía de conexiones externas

## Contenido



## Introducción

Utilice esta guía para revisar las conexiones externas que se requieren para que determinadas funciones de Secure Network Analytics funcionen rápidamente.  Estas conexiones externas pueden ser dominios o extremos.  Los dominios son nombres utilizados para identificar recursos en Internet, generalmente sitios web o servicios; y los terminales son dispositivos o nodos reales que se comunican a través de una red. Dado que el objetivo de esta guía son los servicios web, estos se mostrarán como URL.  En la tabla se enumeran las direcciones URL de las conexiones externas en orden alfabético.



Consejo: En la tabla se enumeran las direcciones URL de las conexiones externas en orden alfabético.

## Conexiones externas

| URL de conexión externa | Propósito |
| --- | --- |
| https://analytics.int.obsrvbl.com | Utilizado por Secure Network Analytics para el intercambio de datos de telemetría con |

| | |
|---|---|
| | los servicios Secure Cloud Analytics. |
| https://api.apj.sse.itd.cisco.com | Cisco lo requiere para el tránsito de datos a Amazon Web Services (AWS) para la región de Asia Pacífico, Japón y China (APJC). Se utiliza al reenviar alertas a Cisco XDR y también para las métricas de servicio al cliente. |
| https://api.eu.sse.itd.cisco.com | Requerido por Cisco para el tránsito de datos a Amazon Web Services (AWS) para la región de Europa (UE). Se utiliza al reenviar alertas a Cisco XDR y también para las métricas de servicio al cliente. |
| https://api-sse.cisco.com | Requerido por Cisco para el tránsito de datos a Amazon Web Services (AWS) para la región de |

| | |
|---|---|
| | Estados Unidos (US). Se utiliza al reenviar alertas a Cisco XDR y también para las métricas de éxito/servicio al cliente. |
| https://apix.cisco.com | Utilizado por Secure Network Analytics para la función de descargas directas de software. |
| https://dex.sse.itd.cisco.com | Necesario para el envío y la recopilación de métricas de éxito del cliente |
| https://est.sco.cisco.com | Necesario para el envío y la recopilación de métricas de éxito del cliente |
| https://eventing-ingest.sse.itd.cisco.com | Necesario para el envío y la recopilación de métricas de éxito del cliente |
| https://feodotracker.abuse.ch/downloads/ipblocklist.txt | Requerido por la fuente de amenazas, que se utiliza para las alertas y observaciones |

| | |
|---|---|
| | de Secure Network Analytics, cuando el análisis está habilitado. |
| https://id.cisco.com | Utilizado por Secure Network Analytics para la función de descargas directas de software. |
| https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz | Requerido por la fuente de amenazas, que se utiliza para las alertas y observaciones de Secure Network Analytics, cuando el análisis está habilitado. |
| https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz | Requerido por la fuente de amenazas, que se utiliza para las alertas y observaciones de Secure Network Analytics, cuando el análisis está habilitado. |
| https://lancope.flexnetoperations.com/control/lncp/LancopeDownload | Requerido por la fuente de inteligencia de amenazas de Secure Network Analytics, que |

| | |
|---|---|
| | se utiliza para alarmas y eventos de seguridad de Secure Network Analytics. Esto requiere la licencia de la fuente de inteligencia de amenazas de Secure Network Analytics. |
| https://mx*.sse.itd.cisco.com | Necesario para el envío y la recopilación de métricas de éxito del cliente |
| https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json | Permite acceder a la información de MITRE para las alertas cuando el análisis está activado. |
| https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json | Permite acceder a la información de MITRE para las alertas cuando el análisis está activado. |
| https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json | Permite acceder a la información de MITRE para las alertas cuando el |

| | |
|---|---|
| | análisis está activado. |
| https://s3.amazonaws.com/onconfig/global-blacklist | Fuente de amenazas necesaria, que se utiliza para las alertas y observaciones de Secure Network Analytics, cuando el análisis está habilitado. |
| https://sensor.anz-prod.obsrvbl.com | Cisco lo requiere para el tránsito de datos a Amazon Web Services (AWS) para la región de Asia Pacífico, Japón y China (APJC). Se utiliza al reenviar alertas a Cisco XDR y también para las métricas de servicio al cliente. |
| https://sensor.eu-prod.obsrvbl.com | Requerido por Cisco para el tránsito de datos a Amazon Web Services (AWS) para la región de Europa (UE). Se utiliza al reenviar alertas a Cisco XDR y |

| | |
|---|---|
| | también para las métricas de servicio al cliente. |
| https://sensor.ext.obsrvbl.com | Requerido por Cisco para el tránsito de datos a Amazon Web Services (AWS) para la región de Estados Unidos (US). Se utiliza al reenviar alertas a Cisco XDR y también para las métricas de servicio al cliente. |
| smartreceiver.cisco.com | Se utiliza para acceder a Cisco Smart Software Licensing. Consulte la Guía de licencias inteligentes para obtener más información. Si lo prefiere, puede obtener licencias sin conexión alternativas. Consulte las Notas de la versión para obtener más información. |
| https://software.cisco.com | Utilizado por Secure Network |

| | |
|---|---|
| | Analytics para la función de descargas directas de software. |
| https://www.cisco.com | Necesario para el dominio de Cisco, que se utiliza para las pruebas de conexión de Smart Licensing, proxy de nube y firewall. |

# Additional Information

Para evaluar más a fondo cómo y por qué se utilizan conexiones de terminales y dominios específicos, consulte los siguientes temas:

- Intercambio seguro de servicios (SSE) de Cisco
- Descargas directas de software (Beta)
- Marco MITER ATT&CK®
- Fuente sobre amenazas

## Intercambio seguro de servicios (SSE) de Cisco

Los terminales SSE se utilizan para el tránsito de datos a Amazon Web Services (AWS), por parte de Cisco para las métricas de servicio al cliente y también se utilizan al reenviar alertas a Cisco XDR. Estos varían
basado en la región y los hosts. Estos extremos se detectan dinámicamente mediante un mecanismo de detección de servicios proporcionado por el conector SSE. Al publicar detecciones en Cisco XDR, Secure Network Analytics intenta descubrir un servicio llamado "xdr-data-platform" y su terminal API "Events".

Región y hosts

Dependiendo de la región en los entornos de producción, los hosts son los siguientes.

US:

- https://api-sse.cisco.com
- https://sensor.ext.obsrvbl.com

UE:

- https://api.eu.sse.itd.cisco.com
- https://sensor.eu-prod.obsrvbl.com

Asia Pacífico, Japón y China:

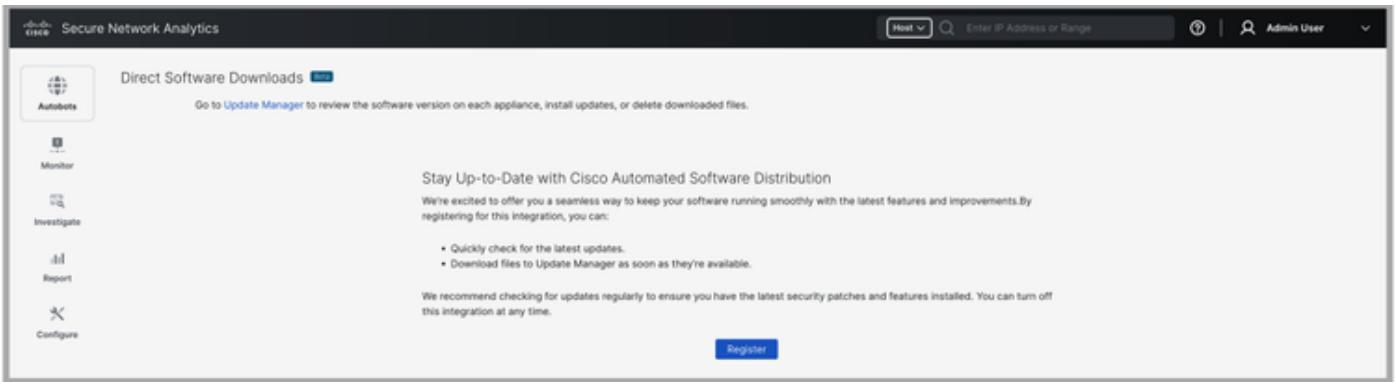
- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

## Descargas directas de software (Beta)

La función Direct Software Downloads (Descargas directas de software) utiliza las conexiones siguientes:

- https://apix.cisco.com
- https://software.cisco.com
- https://id.cisco.com

Para utilizar esta nueva función para descargar el software y aplicar parches a los archivos de actualización directamente en el Administrador de actualizaciones, asegúrese de que se ha registrado con su ID de usuario de cisco.com (CCOID).
1. Inicie sesión en el jefe.
2. En el menú principal, seleccione Configure > Global > Central Management.
3. Haga clic en la pestaña Update Manager.
4. Haga clic en el enlace Descargas directas de software para abrir la página de registro.
5. Haga clic en el botón Register para iniciar el proceso de registro.



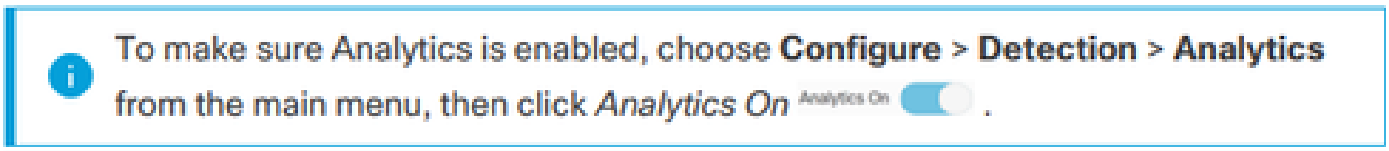

6. Haga clic en el enlace proporcionado.
7. Accederá a la página Activate Your Device (Activar el dispositivo). Para continuar, haga clic en Next (Siguiente).
8. Inicie sesión con su ID de usuario de cisco.com (CCOID).
9. Recibirá el mensaje "Device Activated" (Dispositivo activado) una vez que se complete la activación.

10. Vuelva a la página Descargas directas de software de su jefe y haga clic en Continuar.
11. Haga clic en los enlaces de los acuerdos EULA y K9 para leer y aceptar los términos. Una vez aceptados los términos, haga clic en Continue (Continuar).

Para obtener más información sobre las descargas directas de software, póngase en contacto con el servicio de asistencia de Cisco

## Marco MITER ATT&CK®

El Marco MITER ATT&CK® es una base de conocimiento disponible públicamente de tácticas y técnicas de adversario basadas en observaciones del mundo real. Una vez habilitados los análisis en Secure Network Analytics, las tácticas y técnicas de MITER le ayudan con la inteligencia, detección y respuesta ante amenazas de ciberseguridad.




Las siguientes conexiones permiten que Secure Network Analytics acceda a la información de MITER
para alertas:

- https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
- https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobileattack.json
- https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterpriseattack.json

## Fuente sobre amenazas

La fuente de amenazas de Cisco Secure Network Analytics (anteriormente Stealthwatch Threat Intelligence Feed) proporciona datos de la fuente de amenazas global sobre las amenazas a su red. La fuente se actualiza con frecuencia e incluye direcciones IP, números de puerto, protocolos, nombres de host y URL que se sabe que se utilizan para actividades malintencionadas. En la fuente se incluyen los siguientes grupos de hosts: servidores de control y mando, bogons y Tors.

Para habilitar la fuente de amenazas en la Administración central, siga las instrucciones de la Ayuda.

1. Inicie sesión en el jefe principal.
2. Seleccione Configurar > Global > Administración central.
3. Haga clic en el icono (Ayuda). Seleccione Ayuda.
4. Seleccione Appliance Configuration > Threat Feed.


Para obtener más información sobre la fuente de amenazas, consulte la Guía de configuración del sistema.

## Contacto del soporte

Si necesita asistencia técnica, siga uno de estos procedimientos:

- Póngase en contacto con su partner local de Cisco
- Póngase en contacto con Cisco Support
- Para abrir un caso por Web: http://www.cisco.com/c/en/us/support/index.html
- Para obtener asistencia telefónica: 1-800-553-2447 (EE.UU.)
- Para números de asistencia internacionales: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).