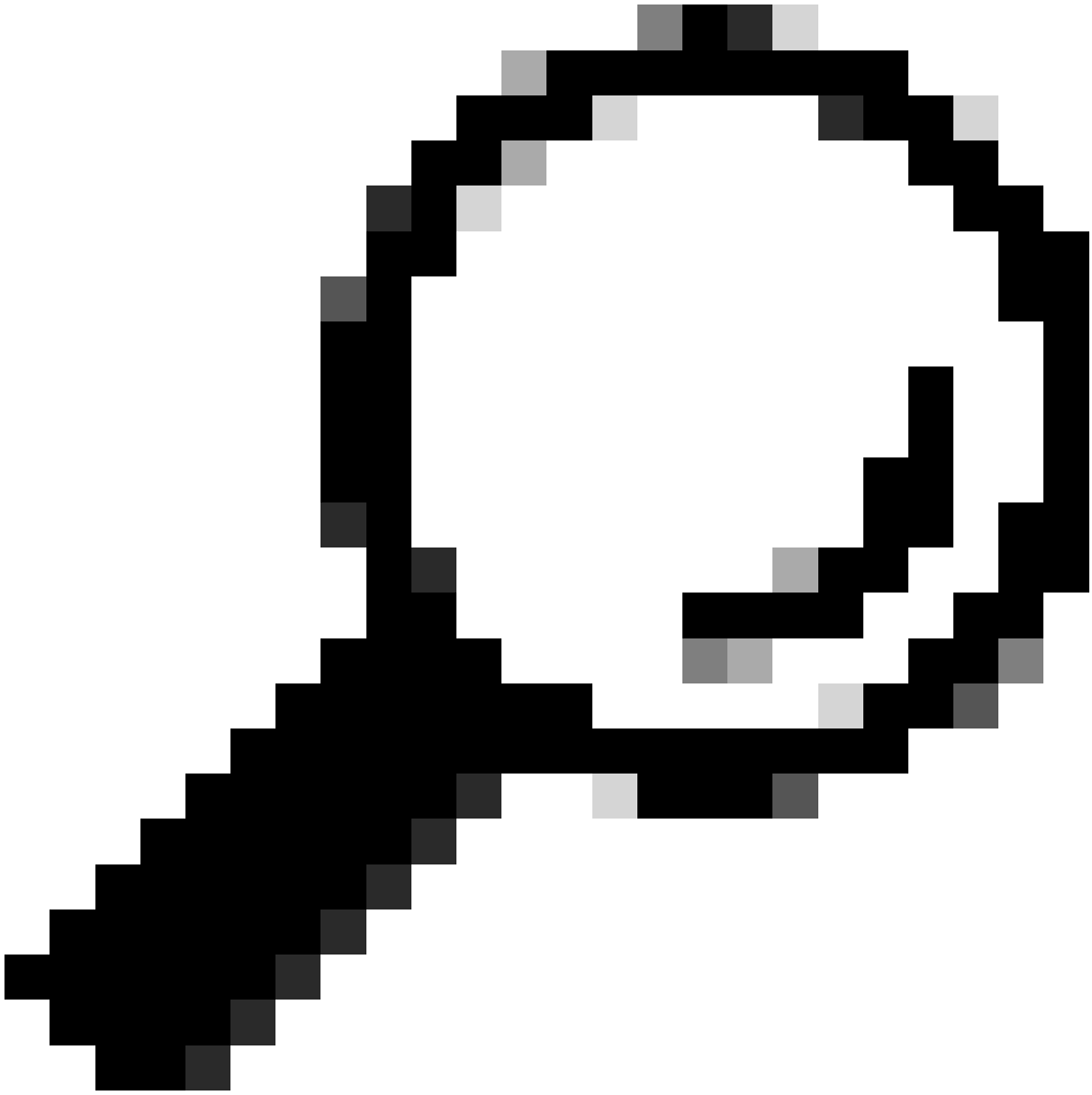
Gids voor het begrijpen van externe verbindingen voor veilige netwerkanalyse

Inhoud

Inleiding

Gebruik deze handleiding om externe verbindingen te bekijken die nodig zijn om bepaalde functies van Secure Network Analytics snel te laten werken. Deze externe verbindingen kunnen domeinen of eindpunten zijn. Domeinnamen zijn namen die worden gebruikt voor het identificeren van bronnen op internet, meestal websites of services; en eindpunten zijn daadwerkelijke apparaten of knooppunten die via een netwerk communiceren. Aangezien de focus voor deze gids webservices is, worden deze weergegeven als URL's. In de tabel staan de URL's van de externe verbinding in alfabetische volgorde.



Tip: In de tabel staan de externe verbindings-URL's in alfabetische volgorde.

Externe verbindingen

URL voor externe verbinding	Doel
https://analytics.int.obsrvbl.com	Gebruikt door Secure Network Analytics voor telemetrie-gegevensuitwisseling met Secure Cloud Analytics-services.
https://api.apj.sse.itd.cisco.com	Vereist door Cisco voor gegevensdoorvoer naar

	Amazon Web Services (AWS) voor de regio Azië-Pacific, Japan en China (APJC). Wordt gebruikt bij het doorsturen van meldingen naar Cisco XDR en ook voor statistieken van de klantenservice.
https://api.eu.sse.itd.cisco.com	Vereist door Cisco voor gegevensdoorvoer naar Amazon Web Services (AWS) voor de regio Europa (EU). Wordt gebruikt bij het doorsturen van meldingen naar Cisco XDR en ook voor statistieken van de klantenservice.
https://api-sse.cisco.com	Vereist door Cisco voor gegevensoverdracht naar Amazon Web Services (AWS) voor de regio Verenigde Staten (VS). Wordt gebruikt bij het doorsturen van meldingen naar Cisco XDR en ook voor statistieken over klantenservice/succes.
https://apix.cisco.com	Gebruikt door Secure Network Analytics voor de functie Direct Software Downloads.
https://dex.sse.itd.cisco.com	Vereist voor het verzenden en verzamelen van klantsuccesstatistieken
https://est.sco.cisco.com	Vereist voor het verzenden en verzamelen van klantsuccesstatistieken
https://eventing-ingest.sse.itd.cisco.com	Vereist voor het verzenden en verzamelen van klantsuccesstatistieken
https://feodotracker.abuse.ch/downloads/ipblocklist.txt	Vereist door Threat Feed, dat wordt gebruikt voor Secure Network Analytics-waarschuwingen en -waarnemingen, wanneer

	Analytics is ingeschakeld.
https://id.cisco.com	Gebruikt door Secure Network Analytics voor de functie Direct Software Downloads.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/ip-filter.gz	Vereist door Threat Feed, dat wordt gebruikt voor Secure Network Analytics-waarschuwingen en -waarnemingen, wanneer Analytics is ingeschakeld.
https://intelligence.sourcefire.com/auto-update/auto-dl.cgi/00:00:00:00:00:00/Download/files/url-filter.gz	Vereist door Threat Feed, dat wordt gebruikt voor Secure Network Analytics-waarschuwingen en -waarnemingen, wanneer Analytics is ingeschakeld.
https://lancope.flexnetoperations.com/control/lncp/LancopeDownload	Vereist door Secure Network Analytics Threat Intelligence Feed, dat wordt gebruikt voor Secure Network Analytics-alarmen en beveiligingsgebeurtenissen. Hiervoor is de Secure Network Analytics Threat Intelligence Feed-licentie vereist.
https://mx*.sse.itd.cisco.com	Vereist voor het verzenden en verzamelen van klantsuccesstatistieken
https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json	Maakt toegang tot MITER-informatie mogelijk voor waarschuwingen wanneer Analytics is ingeschakeld.
https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json	Maakt toegang tot MITER-informatie mogelijk voor waarschuwingen wanneer Analytics is ingeschakeld.
https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json	Maakt toegang tot MITER-informatie mogelijk voor waarschuwingen wanneer Analytics is ingeschakeld.
https://s3.amazonaws.com/onconfig/global-blacklist	Vereiste Threat Feed, die wordt gebruikt voor Secure Network Analytics-

	waarschuwingen en -waarnemingen, wanneer Analytics is ingeschakeld.
https://sensor.anz-prod.obsrvbl.com	Vereist door Cisco voor gegevensdoorvoer naar Amazon Web Services (AWS) voor de regio Azië-Pacific, Japan en China (APJC). Wordt gebruikt bij het doorsturen van meldingen naar Cisco XDR en ook voor statistieken van de klantenservice.
https://sensor.eu-prod.obsrvbl.com	Vereist door Cisco voor gegevensdoorvoer naar Amazon Web Services (AWS) voor de regio Europa (EU). Wordt gebruikt bij het doorsturen van meldingen naar Cisco XDR en ook voor statistieken van de klantenservice.
https://sensor.ext.obsrvbl.com	Vereist door Cisco voor gegevensoverdracht naar Amazon Web Services (AWS) voor de regio Verenigde Staten (VS). Wordt gebruikt bij het doorsturen van meldingen naar Cisco XDR en ook voor statistieken van de klantenservice.
smartreceiver.cisco.com	Gebruikt om toegang te krijgen tot Cisco Smart Software Licensing. Raadpleeg de Smart Licensing Guide voor meer informatie. Alternatieve offline licenties zijn beschikbaar, indien gewenst. Zie de Release Notes voor meer informatie.
https://software.cisco.com	Gebruikt door Secure Network Analytics voor de functie Direct Software Downloads.

https://www.cisco.com	Vereist voor het Cisco-domein, dat wordt gebruikt voor Smart Licensing-, cloud-proxy- en firewallverbindingstests.

Aanvullende informatie

Om verder te beoordelen hoe en waarom specifieke domein- en eindpuntverbindingen worden gebruikt, raadpleegt u de volgende onderwerpen:

- Cisco Secured Service Exchange (SSE)
- Directe softwaredownloads (bèta)
- MITRE ATT&CK® Framework
- bedreigingsvoeding

Cisco Secured Service Exchange (SSE)

SSE-eindpunten worden gebruikt voor gegevensoverdracht naar Amazon Web Services (AWS), door Cisco voor statistieken over klantenservice en ook gebruikt bij het doorsturen van waarschuwingen naar Cisco XDR. Deze variëren
gebaseerd op regio en hosts. Deze eindpunten worden dynamisch ontdekt met behulp van een Service Discovery-mechanisme dat wordt geleverd door de SSE-connector. Bij het publiceren van detecties naar Cisco XDR probeert Secure Network Analytics een service te vinden met de titel "xdr-data-platform" en het API-eindpunt "Events".

Regio en gastheren

Afhankelijk van de regio in productieomgevingen zijn de hosts als volgt.

VS:

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

EU:

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

APJC:

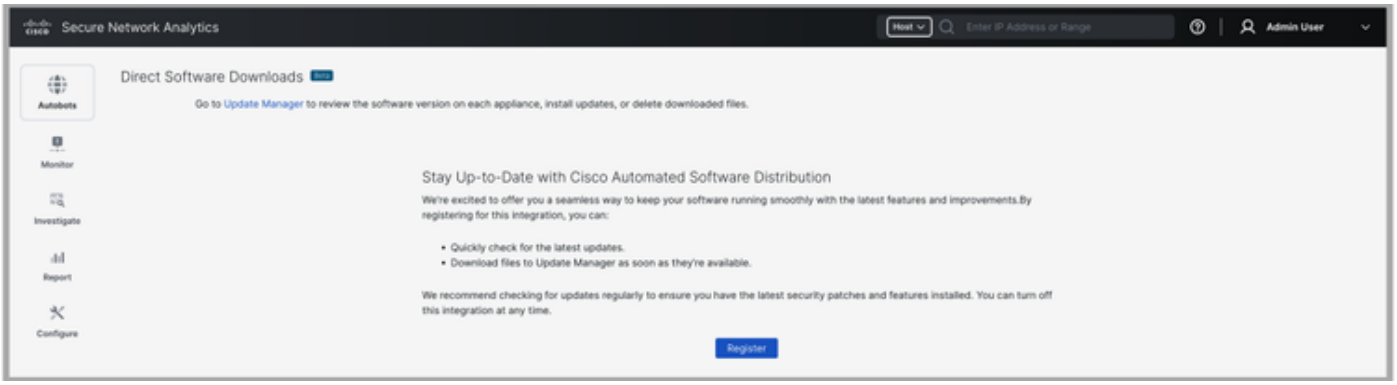
- https://api.apj.sse.itd.cisco.com
- https://sensor.anz-prod.obsrvbl.com

Directe softwaredownloads (bèta)

De volgende verbindingen worden gebruikt door de functie Direct Software Downloads:

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

Als u deze nieuwe functie wilt gebruiken om software te downloaden en bestanden rechtstreeks naar uw Update Manager te patchen, controleert u of u zich hebt geregistreerd met uw cisco.com-gebruikersnaam (CCOID).
1. Meld u aan bij de beheerder.
2. Kies in het hoofdmenu Configureren > Globaal > Centraal beheer.
3. Klik op het tabblad Update Manager.
4. Klik op de link Direct Software Downloads om de registratiepagina te openen.
5. Klik op de knop Registreren om het registratieproces te starten.

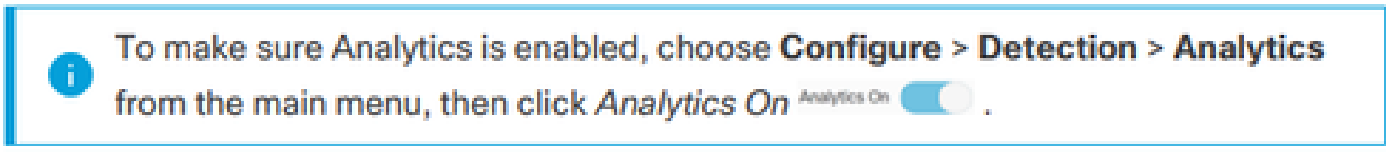


6. Klik op de link die wordt aangeboden.
7. U wordt naar de pagina Uw apparaat activeren geleid. Klik op Volgende om door te gaan.
8. Log in met uw cisco.com gebruikersnaam (CCOID).
9. U ontvangt een bericht "Apparaat geactiveerd" zodra uw activering is voltooid.
10. Ga terug naar de pagina Direct Software Downloads op uw Manager en klik op Doorgaan.
11. Klik op de links voor de EULA- en K9-overeenkomsten om de voorwaarden te lezen en te accepteren. Klik op Doorgaan zodra de voorwaarden zijn geaccepteerd.

Neem voor meer informatie over directe softwaredownloads contact op met Cisco Support

MITRE ATT&CK® Framework

Het MITRE ATT&CK® Framework is een publiek beschikbare kennisbank van tactieken en technieken van tegenstanders op basis van waarnemingen in de echte wereld. Wanneer u Analytics hebt ingeschakeld binnen Secure Network Analytics, helpen MITER-tactieken en -technieken bij cybersecurity-dreigingsintelligentie, -detectie en -reactie.



Met de volgende verbindingen heeft Secure Network Analytics toegang tot MITER-informatie voor waarschuwingen:

- 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

bedreigingsvoeding

De Cisco Secure Network Analytics Threat Feed (voorheen Stealthwatch Threat Intelligence Feed) biedt gegevens uit de wereldwijde Threat Feed over bedreigingen voor uw netwerk. De feed wordt regelmatig bijgewerkt en bevat IP-adressen, poortnummers, protocollen, hostnamen en URL's waarvan bekend is dat ze worden gebruikt voor schadelijke activiteiten. De volgende hostgroepen zijn opgenomen in de feed: command-and-control-servers, bogons en Tors.

Als u Threat Feed wilt inschakelen in Centraal beheer, volgt u de instructies in de Help.

1. Meld u aan bij uw primaire manager.
2. Selecteer Configureren > Algemeen > Centraal beheer.
3. Klik op het (Help)pictogram. Selecteer Help.
4. Selecteer Toestelconfiguratie > Threat Feed.

Raadpleeg de systeemconfiguratiehandleiding voor meer informatie over Threat Feed.

Contact opnemen met ondersteuning

Als u technische ondersteuning nodig hebt, voert u een van de volgende handelingen uit:

- Neem contact op met uw lokale Cisco-partner
- Neem contact op met Cisco Support
- Een kwestie openen via web: http://www.cisco.com/c/en/us/support/index.html
- Voor telefonische ondersteuning: 1-800-553-2447 (VS)
- Voor wereldwijde supportnummers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.