# Wijzigingen in Secure Web applicatie release

## Inhoud



## Inleiding

Dit document beschrijft de belangrijkste wijzigingen en toegevoegde functies in verschillende versies van Secure Web Appliance (SWA).

## Voorwaarden

### Vereisten

Er zijn geen speciale vereisten voor dit artikel.

De gebruikte afkortingen zijn de volgende:

**LD**: Beperkte implementatie.

**GD**: algemene implementatie.

**MD**: implementatie van onderhoud

**ED**: Vroege inzet.

**HP**: Hot Patch.

**CLI**: opdrachtregelinterface.

**GUI**: grafische gebruikersinterface

**HTTP**: Hypertext Transfer Protocol.

**HTTPS**: Hypertext Transfer Protocol beveiligd.

**ECDSA**: Elliptic Curve Digital Signature Algorithm.

**PID:** Process Identifier.

**CTR**: Cisco-bedreigingsrespons.

**AMP**: Advanced Malware Protection.

**URL**: Uniform Resource Locator.

**CDA**: Context Directory Agent.

### Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Geschiedenis per release wijzigen

| Versie | Type | Veranderingen in gedrag | Verbeteringen / extra functies |
|---|---|---|---|
| 12.0.1-268 | LD | - De systeem CPU en geheugenvereisten worden gewijzigd vanaf 12.0 release.<br><br>- Standaard is TLSv1.3 ingeschakeld op het apparaat.<br><br>- Het cijfer "TLS_AES_256_GCM_SHA384" wordt toegevoegd aan de standaardlijst met algoritmen. | - De Cisco AsyncOS 12.0-release biedt Web Security Appliance met hoogwaardige (HP) voor platforms S680, S690 en S695.<br><br>- Een nieuwe sub-commando **hoge prestatie** wordt toegevoegd onder de belangrijkste **geavanceerde proxyconfig** opdracht om de high performance modus in en uit te schakelen.<br><br>- Integratie van de SWA met Cisco Threat Response (CTR) Portal.<br><br>- Het apparaat ondersteunt versie TLSv1.3.<br><br>- De back-up optie van het configuratiebestand wordt verplaatst van het submenu '**Log Abonnementen**' naar '**Configuration File**' onder **Systeembeheer**.<br><br>- Het apparaat ondersteunt nu het uploaden van **ECDSA-**certificaat voor **HTTPS-**proxy.<br><br>- Een nieuwe diagnostische **CLI proxyscannermap** sub-commando wordt toegevoegd onder **diagnostische** > **proxy**. Hiermee wordt de **PID-**toewijzing weergegeven tussen elke proxy en corresponderend scannerproces.<br><br>- Nieuwe optie **zoekopdrachten details** wordt toegevoegd onder de **CLI** opdracht **authcache**.<br><br>- Nieuwe subopdracht **CTROBSERVABLE** wordt toegevoegd onder de **CLI-**opdracht **rapportageConfig** om de **CTR** |

| | | | |
|---|---|---|---|
| | | | waarneembare gebaseerde indexering in- of uit te schakelen. |
| 12.0.1-334 | GD | | - Een nieuwe sub-commando scanners wordt toegevoegd onder de belangrijkste **geavanceerde proxyconfig** opdracht om de MIME-types die gescand worden door de **AMP** engine uit te sluiten. |
| 12.0.2-004 | MD | - Gebruik TLS 1.2 of hoger om het apparaat aan te sluiten op de AMP File Reputation-server.<br><br>- AmericAS (Legacy) cloud-sa.amp.sourcefire.com kan niet worden geconfigureerd op het apparaat. | - Een nieuwe optie "Voer het aantal gelijktijdige scans in dat door AMP moet worden ondersteund" wordt toegevoegd in de **CLI**-opdracht **advanced proxyconfig** > **scanners** > **AMP**.<br><br>u kunt het standaard Unscannable oordeel van lange lopende scanuitzetting wijzigen in Time-out en vice versa van nieuwe CLI sub-commando **uitzetting** in de belangrijkste **CLI** opdracht **advanced proxyconfig** > **scanners**. |
| 12.02-012 | MD | | - Er worden waarschuwingsberichten geactiveerd op de webgebruikersinterface van het apparaat<br><br>wanneer de proxy **Malloc Memory** 90% van de proxy Malloc Memory limiet overschrijdt en er een e-mailbericht wordt verstuurd naar alle 'Alert-ontvangers' die zijn geconfigureerd om 'Web Proxy' kritische waarschuwingen te ontvangen.<br><br>- De nieuwe webinterface biedt een nieuwe look voor het **monitoren van** rapporten en het **volgen van** webdiensten. |
| 12.0.3-005 | MD | | |
| 12.0.3-007 | MD | | - Nieuwe **URL** Categorieën |
| 12.0.4-002 | MD | | |
| 12.0.5-011 | MD | - TLSv1.2 is standaard ingeschakeld voor applicatiebeheer en webgebruikersinterface | - Een bericht wordt toegevoegd om het einde van de ondersteuning voor CDA in de CDA configuratie sectie aan te geven. |

| | | | |
|---|---|---|---|
| | | - **Sessiehervatting** is standaard uitgeschakeld. | |
| 12.5.1-011 | LD | - Standaard is de functie Cisco Success Network ingeschakeld op het apparaat.<br><br>- Deze logbestanden worden aangepast om meer details te omvatten:<br><br>De toegangslogbestanden geven nu de gebruikersnaam weer wanneer de verificatie mislukt.<br><br>De logbestanden van het verificatiekader tonen nu het IP-adres van de client voor deze mislukte verificatieprotocollen: NTLM, BASIC, SSO (Transparent) | - De Cisco AsyncOS 12.5 release biedt Web Security Appliance met hoogwaardige (HP) voor platforms S680, S690 en S695. Dit verhoogt de verkeersprestaties van de huidige high-end toestellen.<br><br>- U kunt nu upgraden naar versie 12.5 en de High Performance Mode gebruiken op de modellen (S680, S690, S695, S680F, S690F en S695F), zelfs als u deze functies op uw apparaat hebt ingeschakeld:<br><br>• Web traffic tap<br>• Volume- en tijdquota<br>• Algemene bandbreedtelimieten<br><br>- U kunt Web Proxy IP-spoofing nu configureren door een IP-spoofingprofiel te maken en aan het routeringsbeleid toe te voegen.<br><br>- U kunt nu een aangepaste URL-categorie voor YouTube maken en beleid instellen op de aangepaste YouTube-categorie voor beveiligde toegangscontrole.<br><br>- In de nieuwe webinterface heeft het apparaat een nieuwe pagina (Monitoring > System Status) om de huidige status en configuratie van het apparaat weer te geven.<br><br>- Met de functie Cisco Success Network (CSN) kan Cisco telemetrie van gebruiksinformatie voor functies van het apparaat verzamelen.<br><br>- REST API voor netwerk-, log-abonnement en andere configuraties. |
| 12.5.1-035 | GD | - Afwijking van TLS 1.0/1.1 :<br><br>Gebruik TLS 1.2 of hoger om het apparaat aan te sluiten op de AMP File Reputation-server. AmericAS (Legacy) **cloud-sa.amp.sourcefire.com** wordt verwijderd uit de AMP File Reputation-serverlijst, zodat AmericAS (Legacy) **cloud-** | - De configuratie van de cachegrootte voor verificatie (Netwerk > Verificatie > Verificatie-instellingen > Credentials opties) wordt niet ondersteund vanuit AsyncOS 12.5.1-035 en latere versies. |

| | | | |
|---|---|---|---|
| | | **sa.amp.sourcefire.com** niet op het apparaat kan worden geconfigureerd. | |
| 12.5.1-043 | GD | | - De waarschuwingsberichten worden weergegeven op de web-gebruikersinterface van het apparaat (Systeembeheer > Waarschuwingen > Bovenste meldingen bekijken):<br>• wanneer het proxy malloc geheugen 90% van proxy malloc geheugen limiet overschrijdt<br>• wanneer de proxy opnieuw opgestart wordt op 100% van het malloc geheugen<br>In beide gevallen wordt een e-mailbericht verzonden naar alle 'waarschuwingsontvangers' die zijn geconfigureerd om 'Web Proxy' kritische waarschuwingen te ontvangen. |
| 12.5.2-007 | MD | | - Een nieuwe URL Categorieën Update melding wordt geïntroduceerd in de banner. Een e-mailbericht over de komende URL categorie updates wordt ook verzonden naar de gebruikers. |
| 12.5.2-011 | MD | | |
| 12.5.3-002 | MD | | |
| 12.5.4-005 | MD | - Vanaf Cisco AsyncOS 12.5.4-versie is TLSv1.2 standaard ingeschakeld voor Application Management Web User Interface.<br>- Na een upgrade naar Cisco AsyncOS 12.5.4-versie wordt de hervatting van de sessie standaard uitgeschakeld.<br>- Het bericht wordt toegevoegd om het einde van de ondersteuning voor CDA in de CDA configuratie sectie aan te geven | |

| | | | |
|---|---|---|---|
| 12.5.4-011 | MD-vernieuwing | | |
| 12.5.5-004 | MD | | - Na een upgrade naar Cisco AsyncOS 12.5 wordt u gevraagd om het proxy-proces opnieuw te starten wanneer u voor het eerst de **networktuning-**opdracht uitvoert. |
| 12.5.5-008 | MD-vernieuwing | | |
| 14.0.1-014 | LD | - Standaard is de HTTP 2.0-functie uitgeschakeld. Gebruik de opdracht <HTTP2> om deze functie in te schakelen.<br><br>- De AsyncOS 14.0 voor Cisco Web Security Applicatie ondersteunt TLSv1.3 sessiehervatting in client en server.<br><br>- de geldigheidsduur van deze certificaten wordt gewijzigd:<br><br>• HTTPS<br>• ISE<br>• SAAS<br>• Toepassingscertificaten<br>• Demo-/beheercertificaat<br><br>- De CLI en de GUI van het apparaat geven nu een bericht weer wanneer een upgrade mislukt vanwege ongeldige lognaam en bestandsnaam in de logabonnementen.<br><br>- Standaard is het pollinginterval ingesteld op 24 uur.<br><br>- Nadat u een upgrade naar deze release hebt uitgevoerd, kunt u de Start Test voor LDAP-verificatie niet uitvoeren als het veld Base DN (Base Distinguished Name) (Network > Authenticatie > Add Real) leeg is. | - Cisco Web Security applicatie ondersteunt nu integratie met Cisco SecureX.<br><br>- U kunt aangepaste headerprofielen configureren voor HTTP-aanvragen en meerdere headers maken onder een header-herschrijfprofiel.<br><br>- U kunt nu de Header Based Verification scheme configureren voor een actieve directory. De client en de Web security applicatie beschouwen de gebruiker als geverifieerd en vragen niet opnieuw om verificatie of gebruikersreferenties. De functie X-Authenticated werkt wanneer de Web Security Applicatie als een upstream apparaat fungeert.<br><br>-<br><br>Het Dashboard met systeemstatus van het apparaat is verbeterd:<br><br>• Capaciteit Tabâ€”A met informatie over tijdbereik, systeem-CPU en geheugengebruik, bandbreedte en RPS, CPU-gebruik per functie en client- of serververbindingen.<br><br>• De eigenschappen van het verkeer van de Volmacht onder het tabblad Status verstrekt client- en serververbindingen details.<br><br>• De Service Response Time bevat nu meer details over staafdiagrammen en legendagegevens voor eerdere datums.<br><br>- U kunt nu configuratie-informatie ophalen en wijzigingen uitvoeren (zoals het wijzigen |

| | | | |
|---|---|---|---|
| | | | van huidige informatie, het toevoegen van nieuwe informatie of het verwijderen van een vermelding) in de configuratiegegevens van het apparaat via REST API's voor beheerbeleid, toegangsbeleid en omzeilingsbeleid<br><br>- Cisco AsyncOS 14.0 versie ondersteunt HTTP 2.0 voor webaanvraag en -respons via TLS. Voor HTTP 2.0-ondersteuning is TLS ALPN-gebaseerde onderhandeling vereist, die alleen vanaf TLS 1.2-versie beschikbaar is.<br><br>In deze release wordt HTTPS 2.0 niet ondersteund voor deze functies:<br><br>• Web traffic tap<br>• Externe DLP<br>• Algemene bandbreedte en toepassingsbandbreedte<br><br>- Een nieuwe CLI-opdracht <HTTP2> wordt geïntroduceerd om HTTP 2.0-configuraties in of uit te schakelen. U kunt HTTP 2.0 niet in- of uitschakelen en het domein voor HTTP 2.0 niet beperken via de gebruikersinterface van het apparaat.<br><br>- De configuratie van HTTP 2.0 wordt niet ondersteund door Cisco Secure Email en Web Manager<br><br>- De CLI geeft het nieuwe waarschuwingsbericht weer wanneer u probeert het standaardcertificaat van een van deze functies te gebruiken:<br><br>• Certificaat van applicatie (Ga in de webgebruikersinterface naar Netwerk > Certificaatbeheer > Certificaat van applicatie)<br>• Certificaat voor aanmeldingsversleuteling (Ga in de webgebruikersinterface naar Netwerk > Verificatie > Instellingen bewerken > Geavanceerd)<br>• HTTPS Management UI-certificaat (Gebruik certconfig > SETUP in de opdrachtregel)<br><br>- Een nieuwe sub-commando OCSPVALIDATION_FOR_SERVER_CERT wordt toegevoegd onder de **certconfig**. Met deze nieuwe subopdracht kunt u de OCSP- |

| | | | |
|---|---|---|---|
| | | | validatie voor LDAP- en Updater-servercertificaten inschakelen. Als de certificaatvalidatie is ingeschakeld, kunt u een waarschuwing ontvangen als de bij de communicatie betrokken certificaten worden ingetrokken.<br><br>- Er wordt een nieuwe CLI-opdracht **Collecerdconfig** toegevoegd om de opiniepeilfunctie tussen het apparaat en de verificatieserver te configureren.<br><br>- U kunt nu kiezen tussen Beheer en Data Interface, terwijl u de functie voor slimme licenties op het apparaat configureert. |
| 14.0.1-040 | LD | - Wanneer u slimme softwarelicenties inschakelt en uw Web Security Appliance registreert met Cisco Smart Software Manager, zijn de Cisco Cloud Services<br><br>(Netwerk > Cloud-serviceconfiguraties) schakelt uw Secure Web-applicatie automatisch in en registreert deze via het Cisco Cloud Services portal.<br><br>- U kunt Cisco Cloud Service niet uitschakelen of deregistreren als slimme licenties op uw apparaat zijn geregistreerd.<br><br>- Als u uw toestellen al hebt geregistreerd voor Cisco Smart Software Manager en Cisco Cloud Services niet hebt geconfigureerd, wordt Cisco Cloud Services automatisch ingeschakeld nadat u hebt geupgrade naar AsyncOS 14.0.1-040. De regio is standaard geregistreerd als Amerika en u kunt de regio (Europa en APJC) naar wens wijzigen.<br><br>- U kunt Cisco Cloud Service niet uitschakelen of deregistreren als slimme licentie op uw apparaat is geregistreerd. | - U kunt de details van de slimme account die in het Cisco Smart Software Manager-portal is gemaakt, bekijken vanuit de opdracht **smartaccountinfo** in de CLI.<br><br>- Als het Cisco Cloud Services-certificaat is verlopen of binnenkort verloopt, wordt het certificaat na de upgrade naar AsyncOS 14.0.1-040 automatisch verlengd door de Cisco Cloud Service.<br><br>- Als het Cisco Cloud Services-certificaat is verlopen, kunt u nu een nieuw certificaat downloaden van het Cisco Talos Intelligence Services-portal vanuit **cloudserviceconfig** > **fetchcertificate**-subopdracht in de CLI.<br><br>- U kunt de Web Security Applicatie automatisch registreren via het Cisco Cloud Service portal (**cloudserviceconfig** > **autoregister** subopdracht in de CLI)<br><br>- U kunt het certificaat voor virtuele apparaat- en hardwareapparatuur laden via **updateconfig** > **clientcertificaat** subopdracht in de CLI.<br><br>- Een nieuwe URL Categorieën Update melding wordt geïntroduceerd in de banner.<br><br>Er wordt ook een e-mailbericht naar de gebruikers gestuurd over de aanstaande updates van de URL-categorie. |
| 14.0.1-053 | GD | | |

| | | | |
|---|---|---|---|
| 14.0.1-503 | HP | | |
| 14.0.2-012 | MD | - In Cisco AsyncOS 14.0.2-versie is TLSv1.2 standaard ingeschakeld voor Application Management Web User Interface onder Systeembeheerder > SSL Configuration.<br><br>- Sessiehervatting is standaard uitgeschakeld. | - Een bericht wordt toegevoegd om het einde van de ondersteuning voor CDA in de CDA configuratie sectie aan te geven.<br><br>- U kunt nu kiezen tussen Data of Management interface voor Smart License Registration uit de vervolgkeuzelijst Test Interface. |
| 14.0.3-014 | MD | - Na een upgrade naar Cisco AsyncOS 14.0 wordt u gevraagd om het proxy-proces opnieuw te starten wanneer u de **netwerk tuning** opdracht voor het eerst uitvoert. | |
| 14.0.3-502 | HP | - Wanneer Secure Web Applicatie werkt in de modus met hoge prestaties, wordt de hoge latentie uitgeschakeld en worden handlers geaccepteerd door de maximale wachttijd. Dit resulteert in een kleiner aantal verbindingen. | |
| 14.0.4-005 | MD | | |
| 14.5.0-498 | LD | - Product-rebrand:<br>• AMP voor endpoints, Advanced Malware Protection en AMP zijn gewijzigd in **Secure-endpoint**<br>• Thread Grid ( File Analysis) gewijzigd in **Malware Analytics**<br><br>- De aanvraag voor een foutieve classificatie wordt via HTTPS verzonden en dus ontvangt u geen veiligheidswaarschuwing.<br><br>- De Samba-versie is opgewaardeerd naar versie 4.11.15.<br><br>- TLSv1.2 is standaard ingeschakeld | - De Secure Web Applicatie kan nu de DNS-respons valideren die van de DNS-server wordt ontvangen en cryptografische handtekeningen ondersteunt.<br><br>- De Secure Web Applicatie beperkt het aantal gelijktijdige verbindingen die door de client worden geïnitieerd tot een ingestelde waarde.<br><br>- Met AsyncOS release 14.5 is de Cisco Web Security Applicatie geherbrandd naar Cisco Secure Web Applicatie<br><br>- De acceslog-beslissingtag in de Decrypt Policy-groep wordt toegevoegd met EUN (End User Notification) wanneer de EUN-pagina wordt weergegeven op de client-webbrowser. |

| | | | |
|---|---|---|---|
| | | voor de webgebruikersinterface voor Appliance Management onder Systeembeheerder > SSL-configuratie.<br><br>- Op een nieuwe installatie van AsyncOS 14.5, wordt de Verlopen en Mismatched Hostname certificaat configuraties waarde in de HTTPS Proxy pagina standaard geselecteerd als **Drop** in plaats van **Monitor**. | - De functie van het kloonbeleid staat u toe om de configuraties van een beleid te kopiëren of te klonen en een nieuw beleid te creëren.<br><br>- U kunt de verkeersbandbreedte beheren door de bandbreedtewaarde te configureren in het quotumprofiel en het quotumprofiel in de URL-categorie van het toegangsbeleid of de algemene webactiviteitsquota in kaart te brengen.<br><br>- REST API om beheerbeleid, decryptie beleid, routing beleid, IP spoofing beleid, anti-malware en reputatie, verificatie gebieden, Cisco Smart Software Licentie, Cisco Umbrella Naadloze ID, Identity services, en System setup te configureren.<br><br>- U kunt de implementatie van ISE-SXP integreren met Cisco Secure Web Applicatie voor passieve verificatie. Hiermee kunt u alle gedefinieerde toewijzingen verkrijgen, inclusief SGT-to-IP-adrestoewijzingen die worden gepubliceerd via SXP.<br><br>- Met de functie Cisco Umbrella Seamless ID kunt u de informatie over gebruikersidentificatie na succesvolle verificatie doorgeven aan de Cisco Umbrella Secure Web Gateway (SWG).<br><br>- Een bericht wordt toegevoegd om het einde van de ondersteuning voor CDA in de CDA configuratie sectie aan te geven.<br><br>- U kunt nu kiezen tussen Data of Management interface voor Smart License Registration uit de vervolgkeuzelijst Test Interface.<br><br>- Na een upgrade naar Cisco AsyncOS 14.5 ontvangt u een prompt om het proxy proces opnieuw te starten wanneer u de **netwerk tuning** opdracht voor het eerst uitvoert. |
| 14.5.0-537 | GD | | - Dit beleid met kloonoptie in Secure Web Applicatie kan ook worden beheerd door Cisco Secure Email and Web Manager (SMA):<br><br>• Toegangsbeleid<br>• Identificatieprofiel |

| | | | |
|---|---|---|---|
| | | | • Decryptie beleid<br>• Routing-beleid |
| 14.5.1-008 | MD | | |
| 14.5.1-016 | MD | | |
| 14.6.0-108 | LD | | - AsyncOS 14.6 biedt ondersteuning aan Cisco Umbrella met Cisco Secure Web Applicatie (SWA). De integratie van Umbrella en Secure Web Applicatie vergemakkelijkt de implementatie van gemeenschappelijk webbeleid van Umbrella naar Secure Web Applicatie. |
| 15.0.0-322 | LD | - FreeBSD-versie is opgewaardeerd naar FreeBSD 13.0.<br><br>- Cisco SSL versie 1.0.2 naar Cisco SSL versie 1.1.1.<br><br>- Talos-motoren zoals AVC, WBRSD, DCA en Beaker zijn opgewaardeerd.<br><br>- Scanner-motoren zoals Webroot en McAfee zijn geüpgraded. | - Deze verbeteringen die zijn aangebracht in de functie Smart Software Licensing:<br><br>• Licentiereservering<br>• Conversie met apparaatlampjeâ€”Nadat u Secure Web Applicatie met slimme licentie hebt geregistreerd, worden alle huidige geldige klassieke licenties automatisch geconverteerd naar slimme licenties via het DLC-proces (Device Led Conversion). Deze geconverteerde licenties worden bijgewerkt in de virtuele account van de CSSM-portal.<br><br>- U kunt de verkeersbandbreedte beheren door bandbreedtewaarde in quotumprofiel te configureren en het quotumprofiel in kaart te brengen in decryptie beleid en toegangsbeleid, URL categorie of algemene webactiviteitsquota.<br><br>- De functie van het kloonbeleid staat u toe om de configuraties van een beleid te kopiëren of te klonen en een nieuw beleid te creëren.<br><br>- Application Discovery and Control (ADC)-engine:<br><br>een beleidscomponent voor acceptabel gebruik die webverkeer inspecteert om een beter begrip en controle te krijgen van webverkeer dat voor toepassingen wordt gebruikt. |

| | | | |
|---|---|---|---|
| | | | Met AsyncOS 15.0 kunt u AVC of ADC engine gebruiken om webverkeer te monitoren. Standaard is AVC ingeschakeld. De ADC-motor ondersteunt de high performance modus.<br><br>- REST API voor ADC-configuratie<br><br>- Admin kan ervoor kiezen om aangepaste SNMPv3-gebruikersnaam te configureren anders dan de standaardgebruikersnaam v3get.<br><br>- De maximale lengte van de aangepaste header is 16k.<br><br>- Optie om de beveiligde tunnelinterface en externe toegangsverbinding te kiezen. |

# Open-broncomponenten

Hier zijn de veranderingen in open broncomponent die in SWA wordt gebruikt:

| Versie | 11.8.X | 12.0.X | 12.5.X | 14.0.X | 14.5.X | 14.6.X | 15.0.x |
|---|---|---|---|---|---|---|---|
| **ongehuwd** | 10.4 | 10.4 | 10.4 | 11.2 | 11.2 | 11.2 | 13.0 |

# Gerelateerde informatie

- Releaseopmerkingen voor AsyncOS 12.0 voor Cisco Web Security applicaties - Cisco
- Releaseopmerkingen voor AsyncOS 12.5 voor Cisco Web Security applicaties - Cisco
- Releaseopmerkingen voor AsyncOS 14.0 voor Cisco Web Security applicaties - Cisco
- Releaseopmerkingen voor AsyncOS 14.5 voor Cisco Secure Web Applicatie - Cisco
- Wat is de releaseterminologie voor contentbeveiliging? (cisco.com)
- Installatiehandleiding voor Cisco Secure Email and Web Virtual Appliance
- **Technische ondersteuning en documentatie â€“ Cisco Systems**

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.