FMC 6.6.1+ - Tips voor en na een upgrade

Inhoud

Inleiding

Dit document beschrijft de best practices voor verificatie en configuratie die moeten worden voltooid voor en na de upgrade van Cisco Secure Firewall Management Center (FMC) naar versie 6.6.1+.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Hardware: Cisco VCC 1000
- in Cisco IOS®-software: release 7.0.0 (gebouw 94)

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 levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Belangrijkste dingen die moeten worden gedaan voor de FMC-upgrade

Kies de FMC doelsoftwareversie

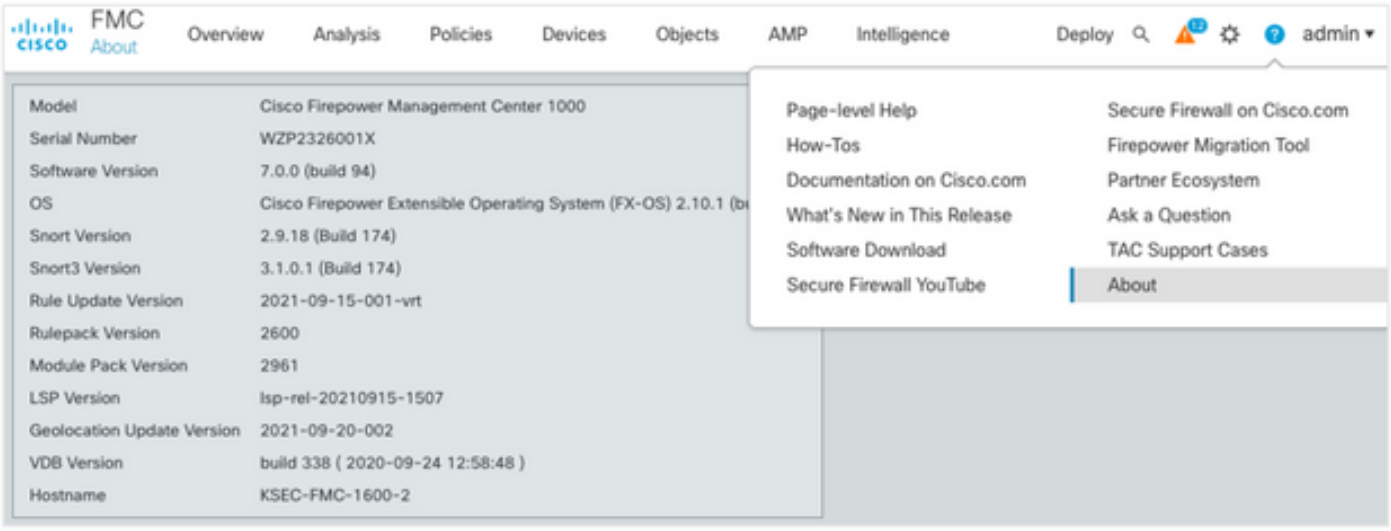
Controleer de Firepower release Notes voor de doelversie en vervang de volgende informatie:

- Compatibiliteit
- Functionaliteit en functies
- Opgeloste problemen
- Bekende problemen

Controleer de huidige FMC-model en -softwareversie

Controleer het huidige FMC-model en de huidige softwareversie:

1. Navigeer naar **Help > Info**.
2. Controleer de **versie van model** en **software**.



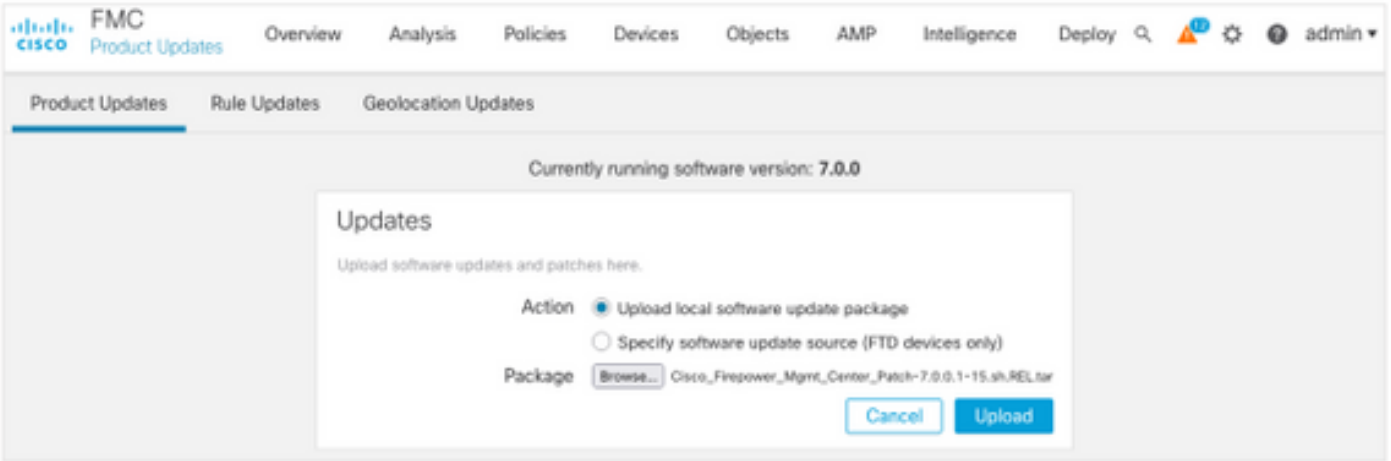
Het upgrade-pad plannen

Afhankelijk van de huidige en beoogde versie van de FMC-software kan een tussentijdse upgrade nodig zijn. In de Cisco Firepower Management Center Upgradegids kunt u het **upgradepad** bekijken: Gedeelte **van FireSIGHT Management Center** en plan het upgradepad.

Upload-upgrade-pakketten

Voltooi de volgende stappen om het upgradepakket naar het apparaat te uploaden:

1. Download het upgradepakket van de Software Download pagina.
2. navigeer in het VCC naar **Systeem > Bijwerken**.
3. Kies de **update uploaden**.
4. Klik op de radioknop **Upload Local software update**.
5. Klik op **Bladeren** en kies het pakket.
6. Klik op **Upload**.



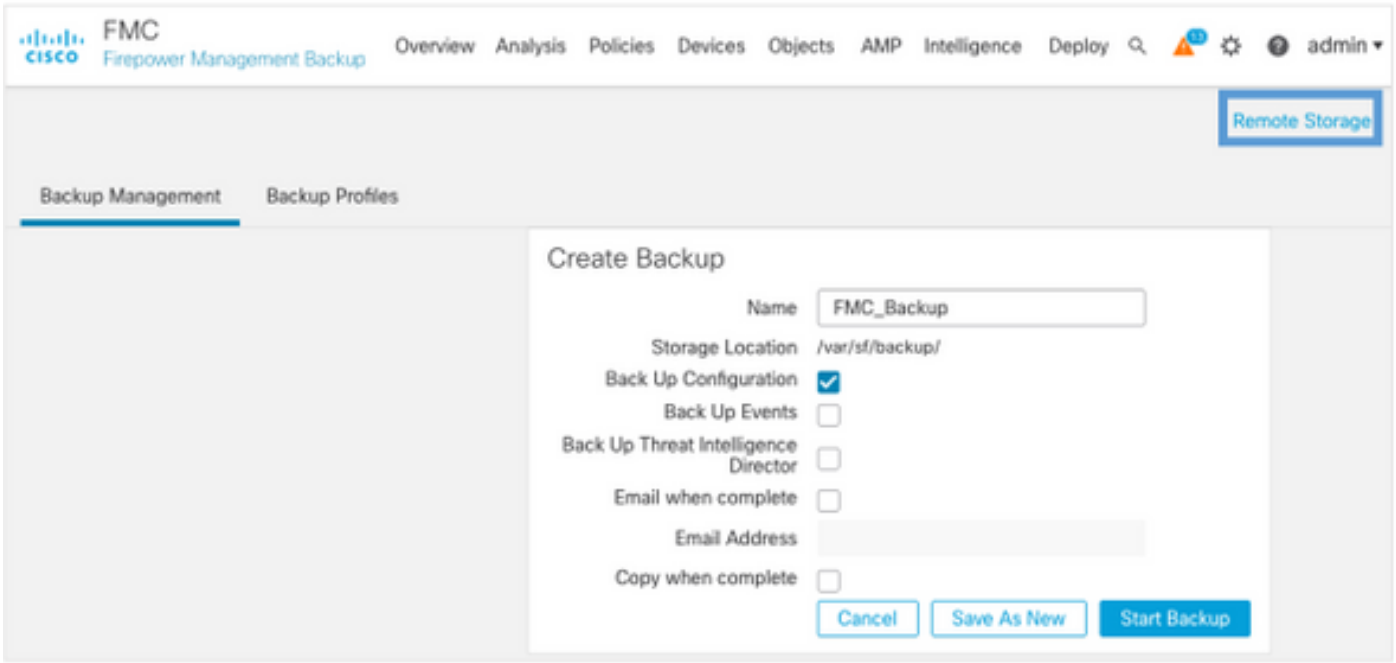
De FMC-back-up maken

Back-up is een belangrijke stap voor het herstel van rampen, die het mogelijk maakt de configuratie te herstellen indien een upgrade niet in een catastrofale toestand verkeert.

1. Blader naar **Systeem > Gereedschappen > Terug/herstellen**.
2. Kies de **back-up voor Firepower Management**.

3. Voer in het veld **Naam** de reservenaam in.
4. Kies de opslaglocatie en de informatie die in de back-up moet worden opgenomen.
5. Klik op **Start Backup**.
6. Vanaf **Meldingen > Taken**, controleer de voortgang van de back-up-conversie.

Tip: We raden aan om back-ups te maken van een beveiligde locatie op afstand en om het succes van de overdracht te controleren. Afstandsopslag kan worden ingesteld op de pagina Back-upbeheer.



Zie voor meer informatie:

- Firepower Management Center Configuration Guide, versie 7.0 - hoofdstuk: Terug en herstellen
- Firepower Management Center Configuration Guide, versie 7.0 - Beheer van externe opslag

Controleer NTP-synchronisatie

Voor een succesvolle FMC-upgrade is NTP-synchronisatie vereist. Voltooi de volgende stappen om NTP-synchronisatie te controleren:

1. Navigeer naar **systeem > Configuratie > Tijd**.
2. Controleer de **NTP-status**.

Opmerking: Status: "Gebruikt worden" geeft aan dat het apparaat gesynchroniseerd is met de NTP-server.

Current Setting Via NTP (based on System Configuration Time Synchronization)
Current Time 2021-09-21 13:50

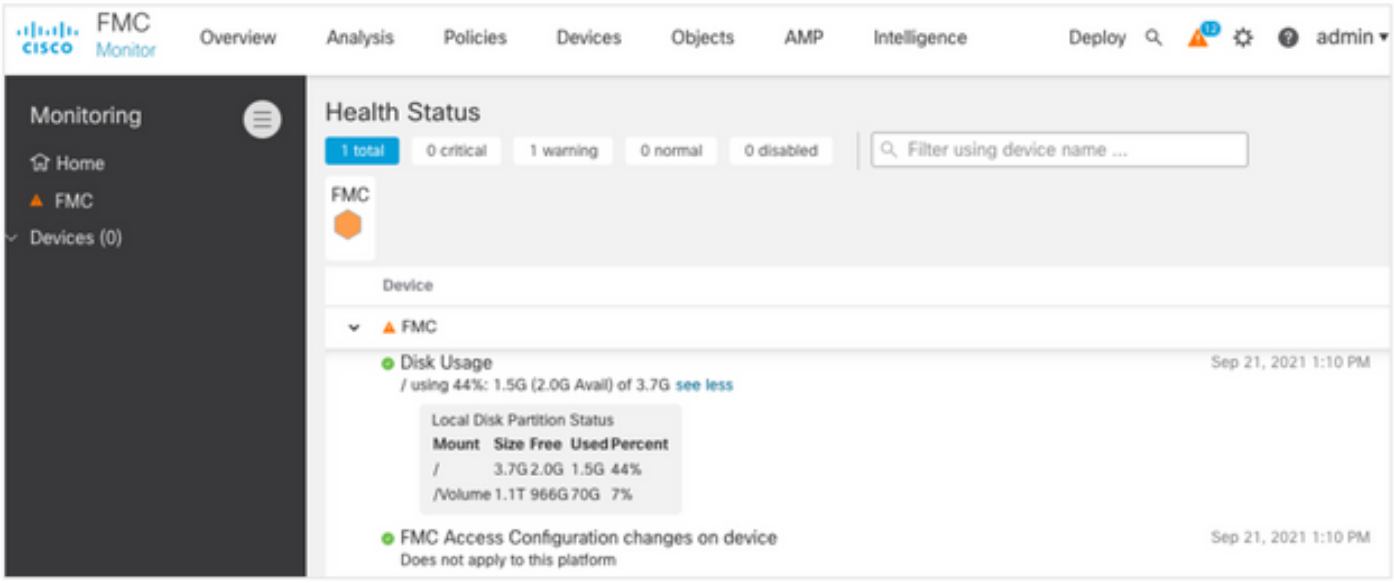
NTP Server	Status	Authentication	Offset	Last Update
173.38.201.115	Being Used	none	+0.011(milliseconds)	126(seconds)
173.38.201.67	Available	none	+0.042(milliseconds)	223(seconds)
127.127.1.1	Unknown	none	+0.000(milliseconds)	12d(seconds)

Zie Firepower Management Center Configuration Guide, versie 7.0 - Time and Time Synchronization.

Controleer de schijfruimte

Zorg er, afhankelijk van het FMC-model en de doelversie, voor dat er genoeg vrije schijfruimte beschikbaar is, anders wordt de upgrade mislukt. Voltooi de volgende stappen om de beschikbare schijfruimte te controleren:

1. Navigeer naar **Systeem > Gezondheid > Monitor**.
2. Kies het VCC.
3. Gebruik van de **schijf** uitvouwen en **zoeken**.
4. De vereisten voor de schijfruimte zijn te vinden in tijdtests en schijfruimtevereisten.

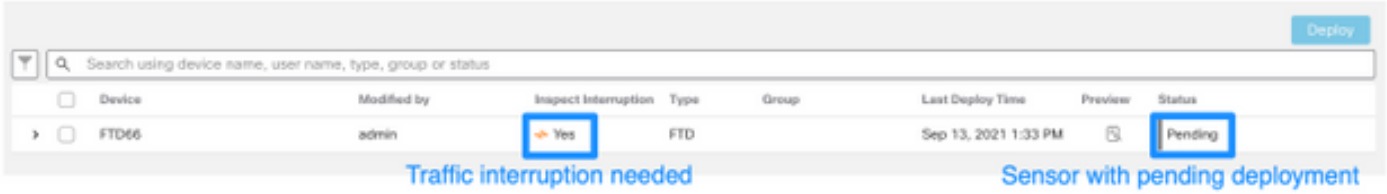


Alle hangende beleidswijzigingen implementeren

Vóór de installatie van de bijwerking of de pleister moeten veranderingen in de sensoren worden aangebracht. Voltooi de volgende stappen om ervoor te zorgen dat alle hangende wijzigingen worden uitgevoerd:

1. Navigeren in om **te stellen > Plaatsing**.
2. Kies alle apparaten in de lijst en **implementeer**.

Voorzichtig: De kolom Onderbreking van de inspectie wijst op verkeersonderbreking

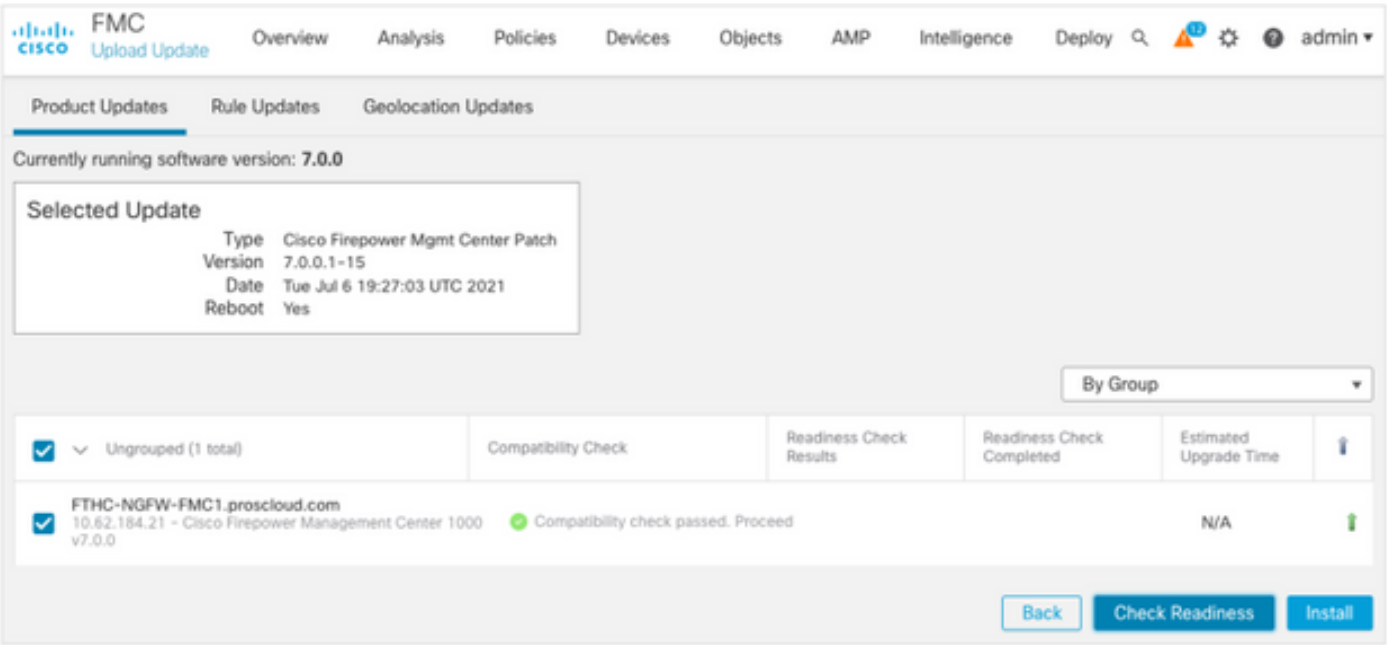


Controleren of de software klaar is met FirePOWER.

Tijdens de leesbaarheidscontroles wordt beoordeeld in hoeverre een FirePOWER-apparaat klaar is voor een softwareupgrade.

Voltooi de volgende stappen om de leesbaarheidscontroles van de software uit te voeren:

1. Navigeer naar **systeem > updates**.
2. Selecteer het pictogram **Install** naast de doelversie.
3. Kies het VMC en klik op **Gereedschap controleren**.
4. Klik in het pop-upvenster op **OK**.
5. Controleer het proces voor leescontrole aan de hand van **meldingen > Taken**.



Zie [Cisco FireSIGHT Management Center Upgradegids](#) voor [FirePOWER-softwareleescontrole](#).

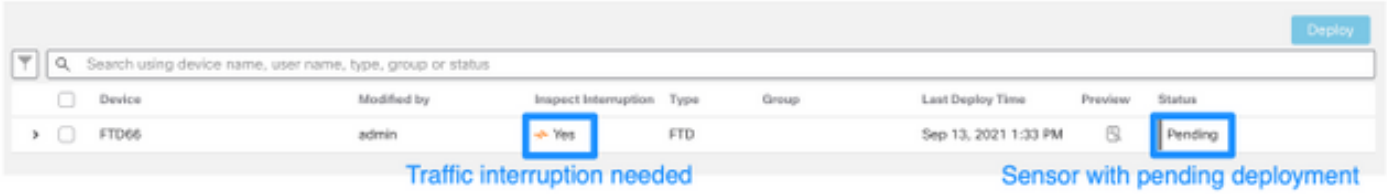
Belangrijkste dingen om te doen na de upgrade van de FMC

Alle hangende beleidswijzigingen implementeren

Onmiddellijk na elke update- of patchinstallatie moet men veranderingen in de sensoren aanbrengen. Voltooi de volgende stappen om ervoor te zorgen dat alle hangende wijzigingen worden uitgevoerd:

1. Navigeren in om **te stellen > Plaatsing**.
2. Kies alle apparaten in de lijst en klik op **Uitvoeren**.

Voorzichtig: De kolom Onderbreking van de inspectie wijst op verkeersonderbreking



Controleer of de laatste kwetsbaarheids- en Fingerprint-database is geïnstalleerd

Voltooi de volgende stappen om de huidige versie van Fingerprint (VDB) te controleren:

1. Navigeer naar **Help > Info**.
2. Controleer de **VDB versie**.

Om de VDB-updates rechtstreeks van cisco.com te kunnen downloaden, is bereikbaarheid van het FMC naar cisco.com vereist.

1. Navigeer naar **Systeem > updates > Productupdates**.
2. Kies **Download updates**.
3. Installeer de laatst beschikbare versie.
4. Je moet de sensoren daarna opnieuw inzetten.

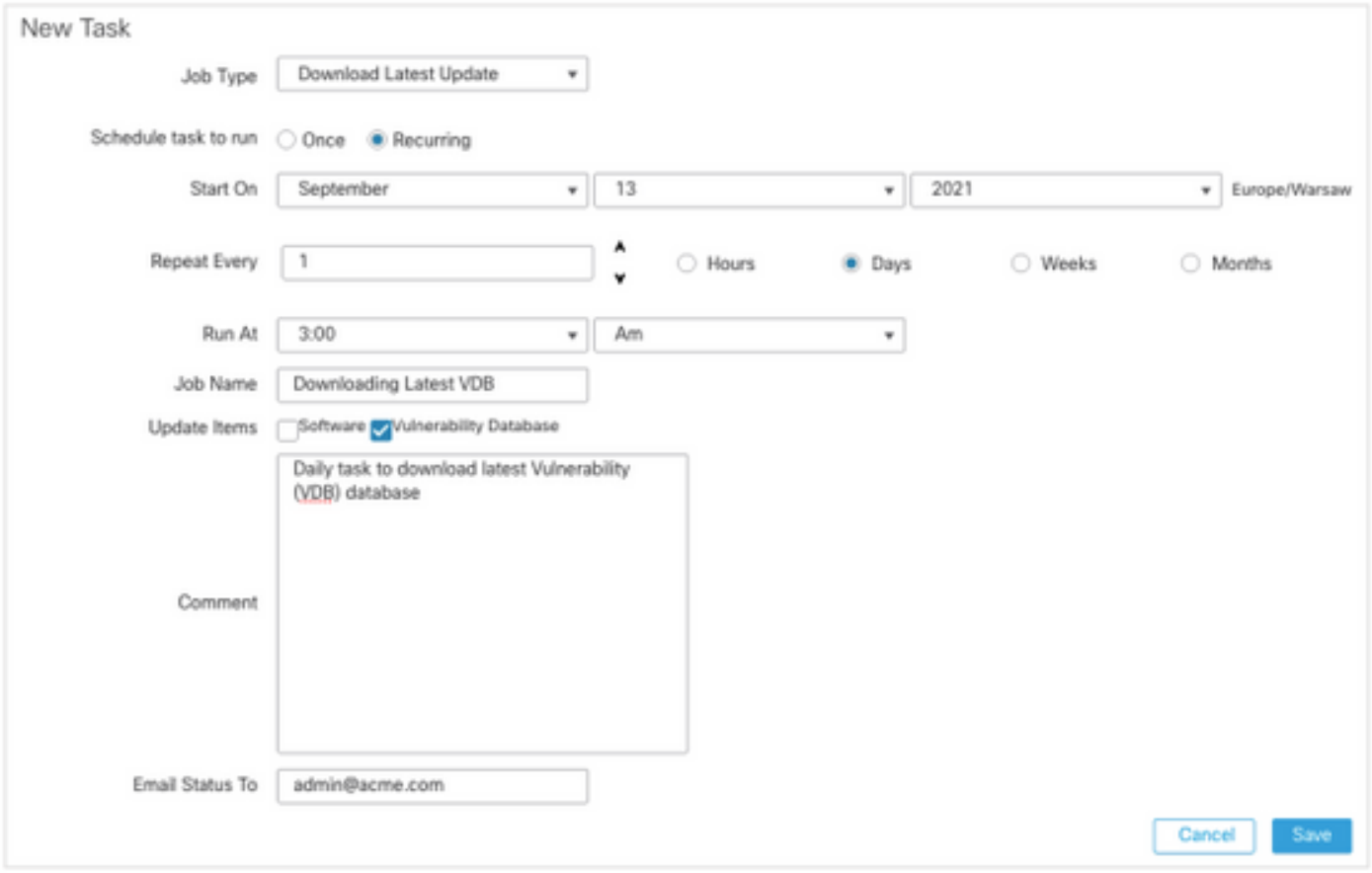
> **Opmerking:** Als het FMC geen internettoegang heeft, kan het VDB-pakket rechtstreeks van software.cisco.com worden gedownload.

Het wordt aanbevolen taken uit te voeren om automatische VDB-pakketdownloads en -installaties uit te voeren.

Als goede praktijk, controleer dan dagelijks op VDB-updates en installeer ze op het VMC tijdens de weekends.

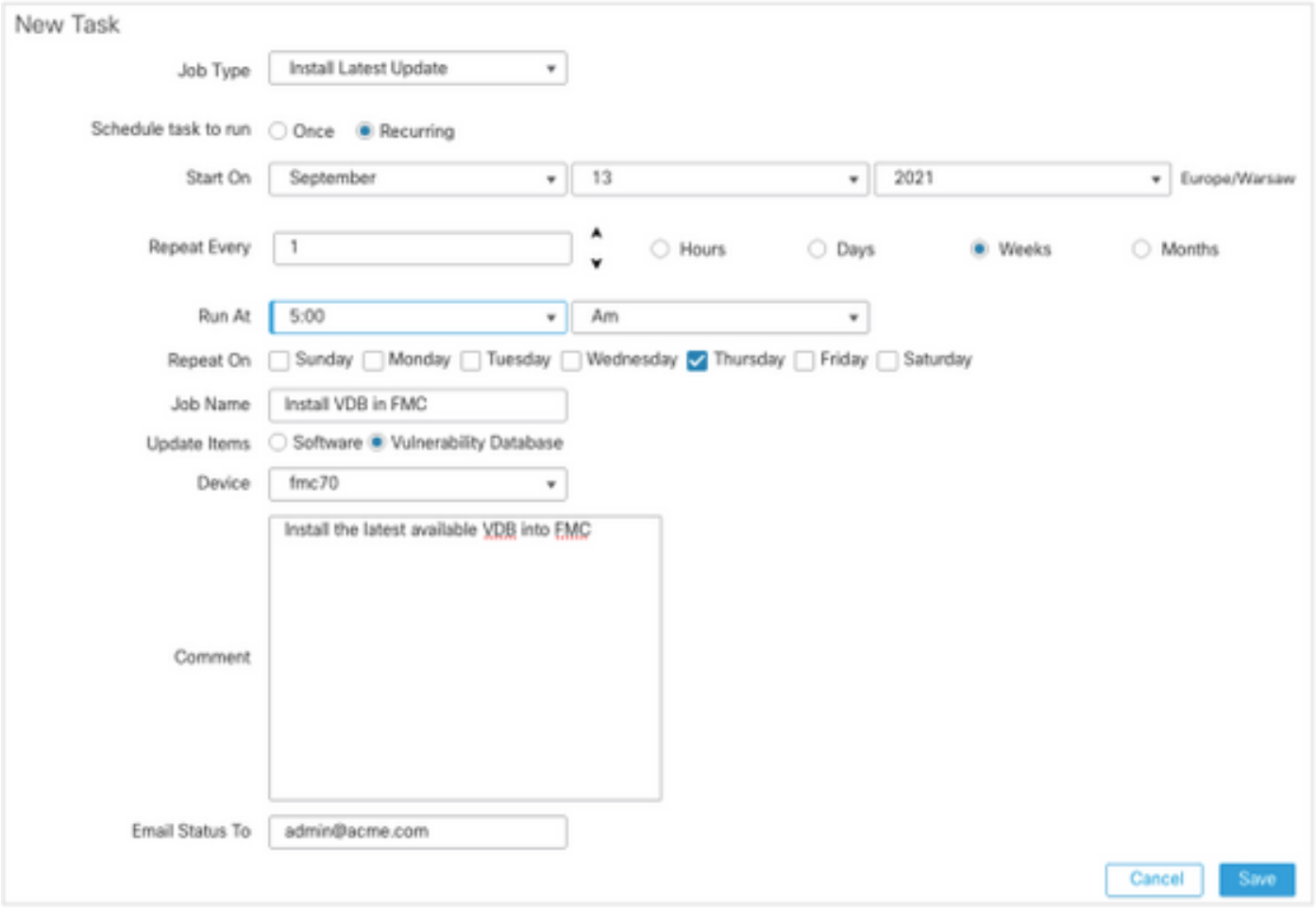
Voltooi de volgende stappen om de VDB-dagelijkse gegevensbank vanaf www.cisco.com te controleren:

1. Blader naar **Systeem > Gereedschappen > Scheduling**.
2. Klik op **Taakje toevoegen**.
3. Selecteer in de vervolgkeuzelijst **Functietype** de optie **Nieuwste update downloaden.**
4. Klik op de radioknop **Recurring** voor **Schedule Task** om de taak **uit te voeren.**
5. Herhaal de taak elke dag en voer deze uit om 15:00 uur of buiten de kantooruren.
6. Voor **opties voor bijwerken** , vinkt u het aankruisvakje voor de **Wulnerability Database.**



Stel het periodieke taakweekje in om de laatste VDB in het VMC te installeren:

1. Blader naar **Systeem > Gereedschappen > Scheduling**.
2. Klik op **Taakje toevoegen**.
3. Selecteer in de vervolgkeuzelijst **Functietype** de optie **Nieuwste update installeren**.
4. Klik op de knop **Terugkeren** voor **draaitaak**.
5. Herhaal de taak elke 1 week en voer deze om 5:00 uur of buiten de kantooruren uit.
6. Voor **opties voor bijwerken** , vinkt u het vakje **Vulnerability Database** aan.



Zie Firepower Management Center Configuration Guide, versie 7.0 - Update the Vulnerability Database (VDB)

Controleer de korte regel en de lichtgewicht security pakket - huidige versie

Voltooi de volgende stappen om de huidige software van de Synthetisch (SRU), het Lichtgewicht Security Packet (LSP) en de Geolocatie te controleren:

1. Navigeer naar **Help > Info**.
2. Controleer de **versie van de Regel** en de **LSP versie**.

Om de SRU en LSP direct van www.cisco.com te kunnen downloaden, is bereikbaarheid van het FMC naar www.cisco.com vereist.

1. Navigeer naar **systeem > updates > Regelupdates**.
2. Kies **in** het tabblad **Eenmalige aanpassing/Regels importeren** de optie **Nieuwe regel downloaden op de ondersteuningswebsite**.
3. Kies **Importeren**.
4. Stel de configuratie daarna in op de sensoren.

Opmerking: Als het FMC geen internettoegang heeft, kunnen de SRU- en LSP-pakketten rechtstreeks worden gedownload van software.cisco.com.

Inbraakregelupdates zijn cumulatief en het wordt aanbevolen om altijd de laatste update in te voeren.

Voltooi de volgende stappen om de wekelijkse download en implementatie van korte regelupdates (SRU/LSP) in te schakelen:

1. Navigeer naar **systeem > updates > Regelupdates**.
2. In het tabblad **Terugkerende** bijwerking **van de regel** Invoer, controleert u het vakje **Regelmatige invoer uit de** sectie **Ondersteuningssite** inschakelen.
3. Kies de importfrequentie als week, kies één dag van de week en laat in de namiddag voor de download- en beleidslijn.
4. Klik op **Opslaan**.

Zie Firepower Management Center Configuration Guide, versie 7.0 - Update Inbraakregels.

Controleer de huidige versie van Geolocatie bijwerken

Voltooi de volgende stappen om de huidige versie van Geolocation te controleren:

1. Navigeer naar **Help > Info**.
2. Controleer de **versie van Geolocation Update**.

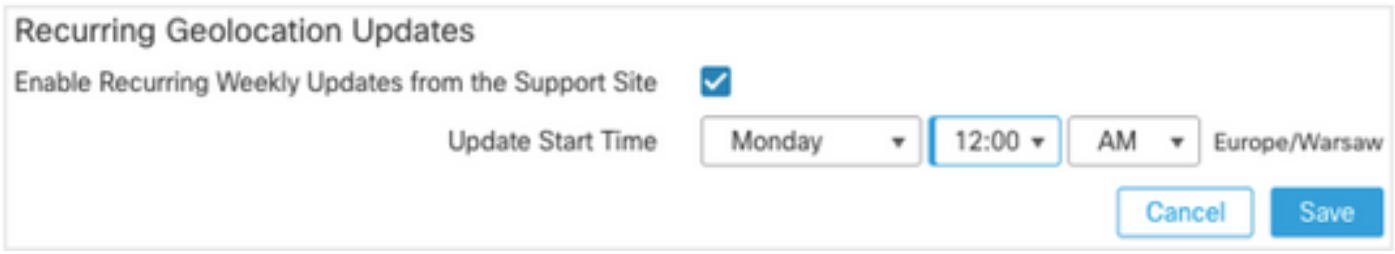
Om Geolocatie-updates rechtstreeks van www.cisco.com te kunnen downloaden, is bereikbaarheid van het FMC naar www.cisco.com vereist.

1. Navigeer naar **Systeem > updates > Geolocatie updates**.
2. Kies **in** het tabblad **One-Time Geolocation Update** de **geolocation-update van de ondersteuningswebsite en installeer deze**.
3. Klik op **Importeren**.

Opmerking: Als het FMC geen internettoegang heeft, kan het pakket Geolocatie-updates rechtstreeks worden gedownload van software.cisco.com.

Voltooi de volgende stappen om de automatische Geolocation-updates in te schakelen:

1. Navigeer naar **Systeem > updates > Geolocatie updates**.
2. Controleer in het gedeelte Terugkerende geolocatie-updates de optie **wekelijkse updates inschakelen in het** dialoogvenster **Support Site**.
3. Kies de importfrequentie als week en kies maandag om middernacht.
4. Klik op **Opslaan**.

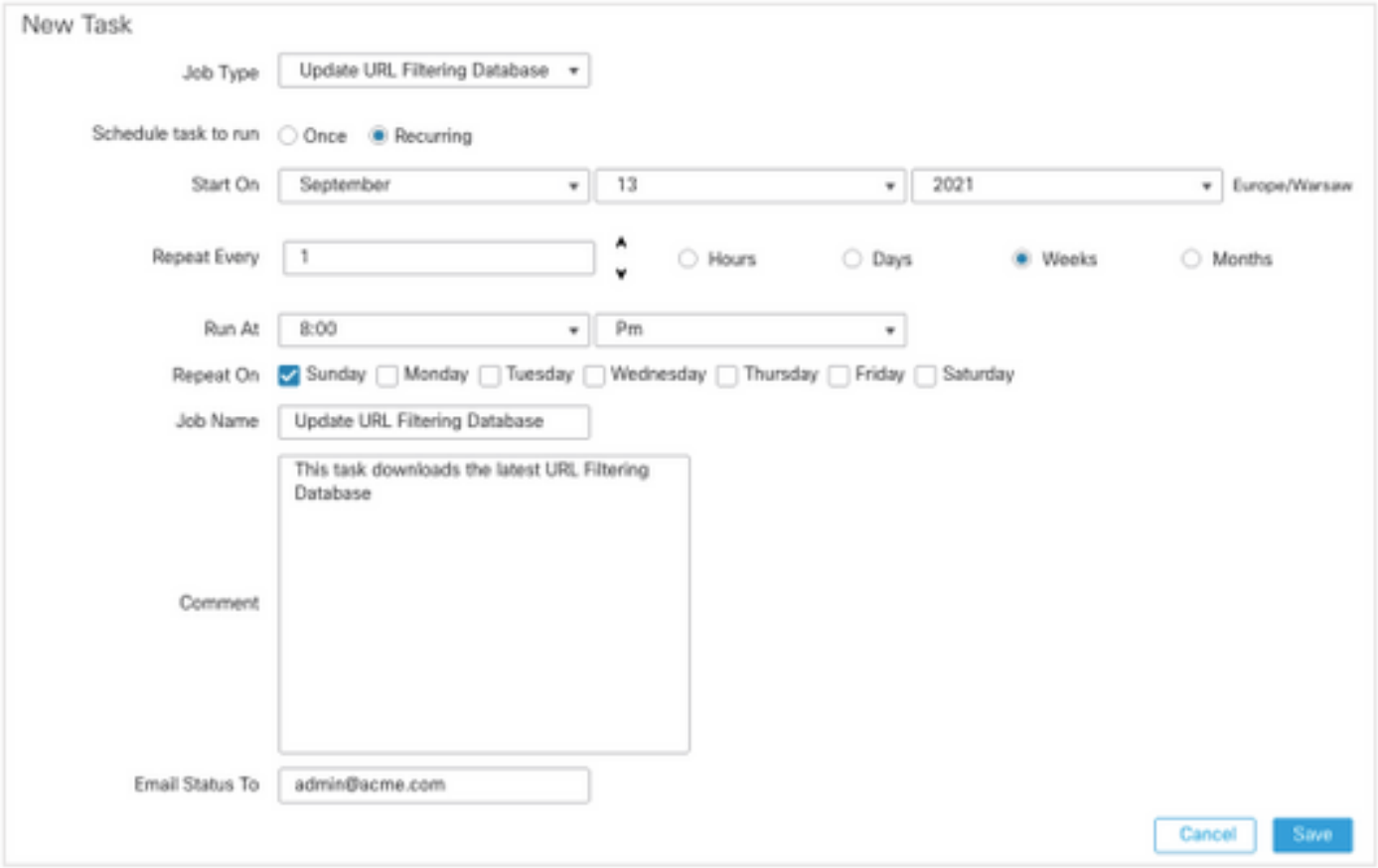


Zie Firepower Management Center Configuration Guide, versie 7.0 - update de Geolocation Database (GeoDB) voor meer informatie.

Automation URL-filtering van database met geplande taak

Om ervoor te zorgen dat de bedreigingsgegevens voor URL-filtering actueel zijn, moet het systeem gegevensupdates van de Cisco Collective Security Intelligence (CSI) cloud verkrijgen. Om dit proces te automatiseren, volgt u de volgende stappen:

1. Blader naar **Systeem > Gereedschappen > Scheduling**.
2. Klik op **Taakje toevoegen**.
3. Kies in de vervolgkeuzelijst **Functietype** de optie **URL-filtering database bijwerken.**
4. Klik op de knop **Terugzetten** voor **de** taak **Schedule**.
5. Herhaal de taak elke week en voer deze om 20:00 uur op zondag of buiten de kantooruren uit.
6. Klik op **Opslaan**.

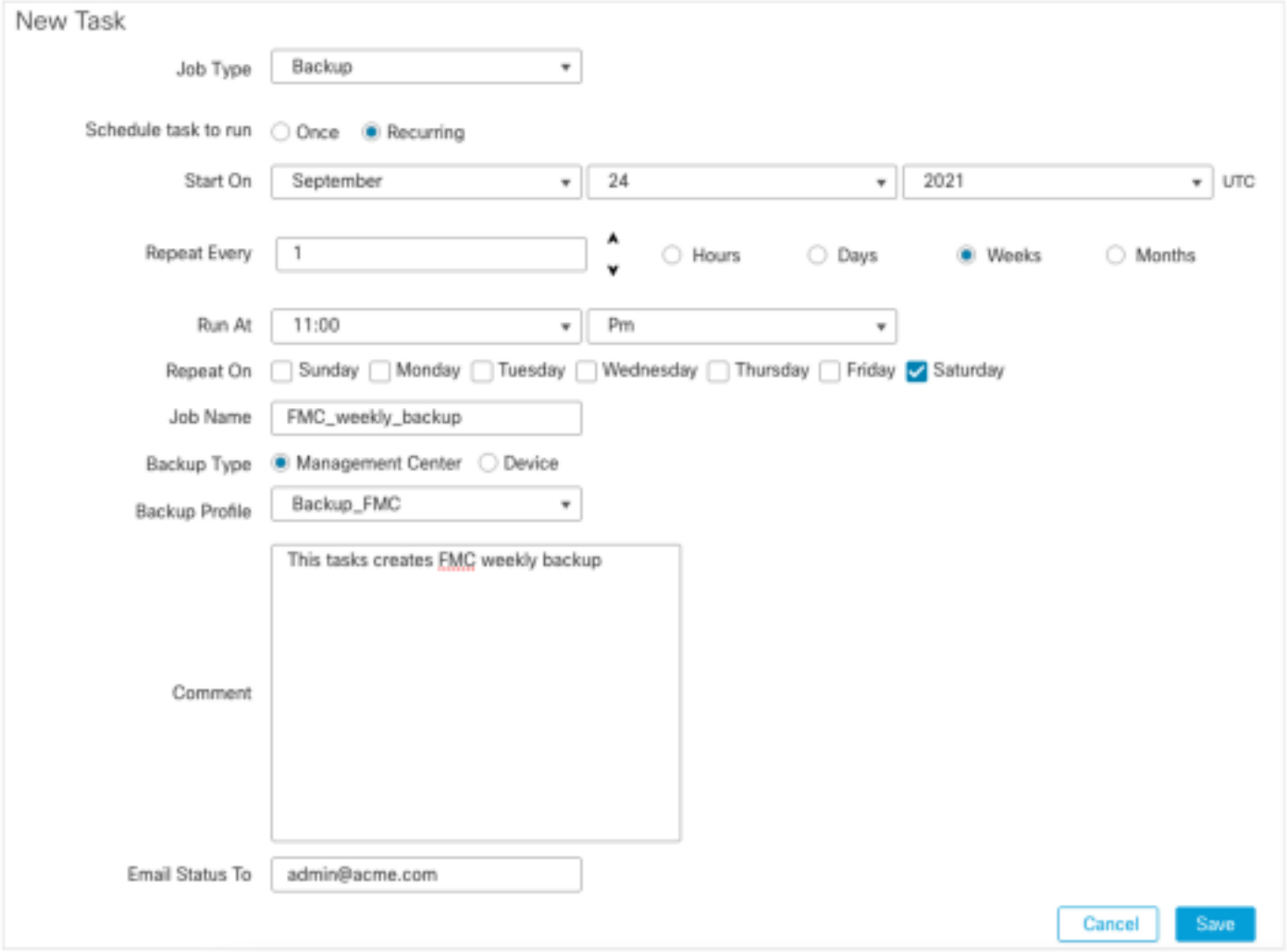


Zie Firepower Management Center Configuration Guide, versie 7.0 - URL-filtering met behulp van een geplande taak automatiseren voor meer informatie.

Periodieke back-ups configureren

Als onderdeel van het noodherstelplan wordt het aanbevolen om periodieke back-ups te maken.

1. Zorg ervoor dat je in het **mondiale domein** bent.
2. Maak het FMC-reserveprofiel. Zie voor meer informatie het gedeelte **Backup** maken.
3. Blader naar **Systeem > Gereedschappen > Scheduling**.
4. Klik op **Taakje toevoegen**.
5. Selecteer in de vervolgkeuzelijst **Functietype** de optie **Back-up.**
6. Klik op de knop **Terugzetten** voor **de** taak **Schedule**.
   De reservefrequentie moet aan de behoeften van de organisatie worden aangepast. We raden aan om back-ups te maken tijdens een onderhoudsvenster of een ander tijdstip van weinig gebruik.
7. Klik voor **back-uptype** op de knop **Management Center**.
8. Kies in de vervolgkeuzelijst **Back-upprofiel** de optie Back-upprofiel.
9. Klik op **Opslaan**.



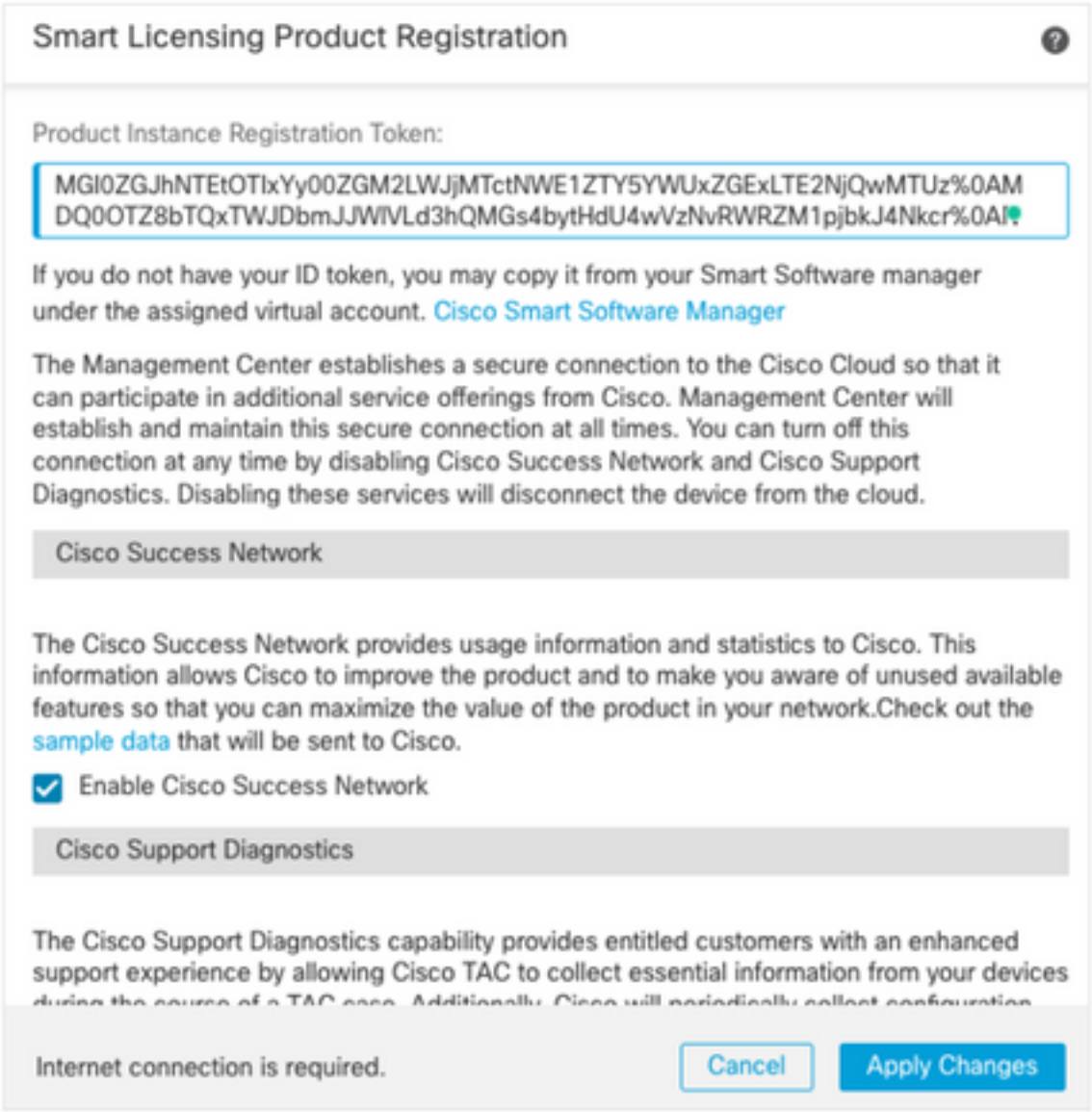
Zie [Firepower Management Center Configuration Guide, versie 7.0 - Hoofdstuk: Terug en herstellen].

Zorg ervoor dat de slimme licentie is geregistreerd

Voltooi de volgende stappen om het Cisco Firewall Management Center met Cisco Smart Software Manager te registreren:

1. In https://software.cisco.com kunt u navigeren naar **Smart Software Manager > Licenties**

beheren.
2. Navigeer naar **inventaris > Algemeen** tabblad en maak een **Nieuw Token**.
3. In de FMC UI, navigeer naar **Systeem > Licenties > Smart Licenties**.
4. Klik op **Registreren**.
5. Steek de Token die in het Cisco Smart Software Licensing-portaal is gegenereerd.
6. Zorg ervoor dat **Cisco Success Network is ingeschakeld**.
7. Klik op **Wijzigingen toepassen**.
8. Controleer de slimme licentiestatus.



Zie [Firepower Management Center Configuration Guide, versie 7.0 - Registreer slimme licenties] voor meer informatie.

Bekijk de configuratie van de variabelen

Zorg ervoor dat de variabele HOME_NET alleen de interne netwerken/subnetten in de organisatie bevat. Onjuiste variabele definitie heeft een negatief effect op de prestaties van de firewall.

1. Navigeer naar **objecten > Variabele set**.
2. Bewerk de variabele die door uw inbraakbeleid wordt gebruikt. Het is toegestaan om per inbraakbeleid één variabele in te stellen met verschillende instellingen.
3. Pas de variabelen aan op basis van uw omgeving en klik op **Opslaan**.

Andere relevante variabelen zijn DNS_SERVERS OF HTTP_SERVERS.

Zie Firepower Management Center Configuration Guide, versie 7.0 - Variable Series.

Controleer de mogelijkheden voor cloudservices

Om gebruik te maken van de verschillende clouddiensten,Ga naar **systeem > Integratie > Cloudservices**.

URL-filtering

1. URL-filtering inschakelen en automatische updates toestaan, schakelt u de Cisco-cloud voor onbekende URL's in.
   Een frequentere URL-verloopdatum van cache vereist meer vragen naar de cloud, wat leidt tot langzamere webladingen.
2. **De wijzigingen opslaan.**

Tip: Voor cacheURL-verloopdatums laat u de standaard **nooit** achter. Indien een strengere webherindeling nodig is, kan deze instelling dienovereenkomstig worden gewijzigd.

Advanced Malware Protection voor netwerken

1. Zorg ervoor dat beide instellingen zijn ingeschakeld: **Schakel automatische lokale Malware Detectie-updates in** en **deel URI van Malware gebeurtenissen met Cisco**.
2. In FMC 6.6.X, blokkeer het gebruik van legacy-poort 32137 voor AMP voor netwerken zodat de TCP-poort in plaats daarvan 443 is.
3. **De wijzigingen opslaan.**

Opmerking: Deze instelling is niet langer beschikbaar in FMC 7.0+ en de poort is altijd 443.

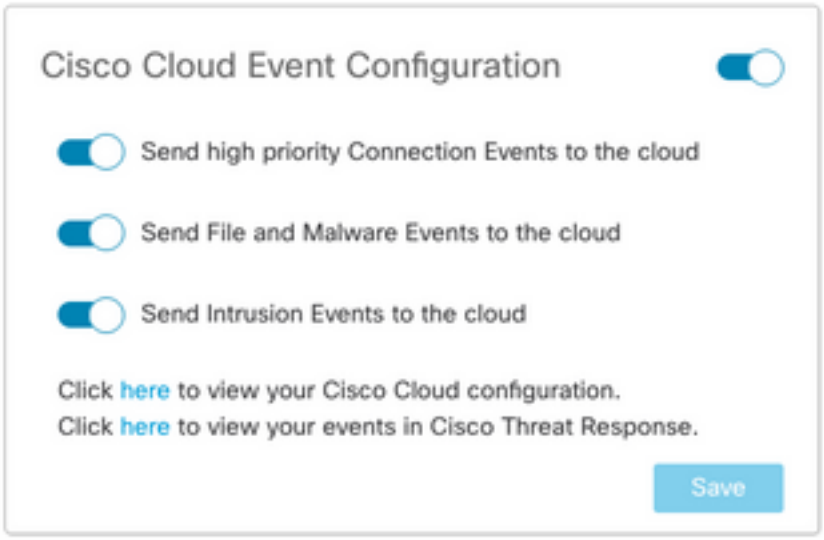
Cisco Cloud-gebied

1. Het wolgebied moet overeenkomen met het SecureX-organisatiegebied. Als de SecureX-organisatie niet is gemaakt, kiest u het gebied dichter bij de FMC-installatie: APJ-regio, EU-regio of VS-regio.
2. **De wijzigingen opslaan.**

Cisco-configuratie van cloudgebeurtenissen

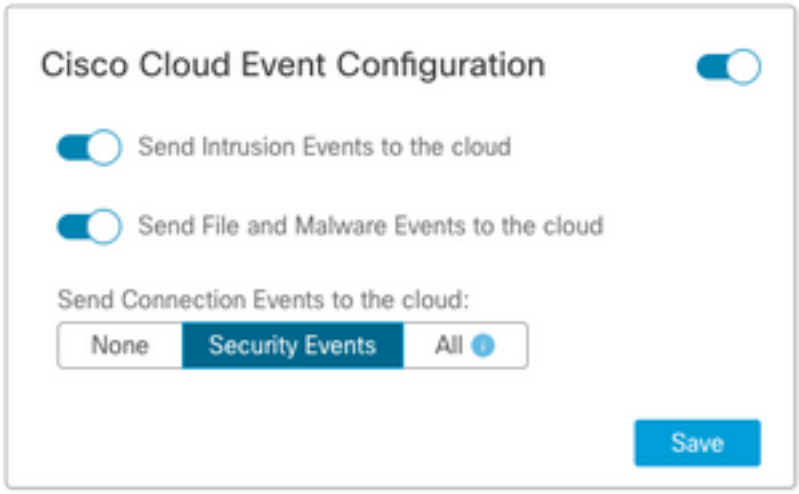
Voor FMC.6.x

1. Zorg voor alle drie de opties: **Verzend gebeurtenissen van de hoge prioriteit verbinding naar de cloud**, **Verzend gebeurtenissen van het bestand en van Malware naar de cloud**, en **Verzend** inbraakgebeurtenissen **naar de cloud** worden geselecteerd.
2. **De wijzigingen opslaan.**



Voor FMC 7.0+

1. Zorg ervoor dat beide opties zijn geselecteerd: **Verzend inbraakgebeurtenissen naar de cloud** en **Verzend bestanden en Malware gebeurtenissen naar de cloud**.
2. Voor het type verbindingsgebeurtenissen, kies **All** als Security Analytics en Logging Solutions in gebruik zijn. Kies voor SecureX alleen **Security gebeurtenissen**.
3. **De wijzigingen opslaan.**



SecureX-integratie inschakelen

De integratie SecureX biedt onmiddellijke zichtbaarheid in het bedreigingslandschap over uw Cisco security producten. Om SecureX aan te sluiten en het lintje in te schakelen, volgt u de volgende stappen:

Geïntegreerd SecureX-band

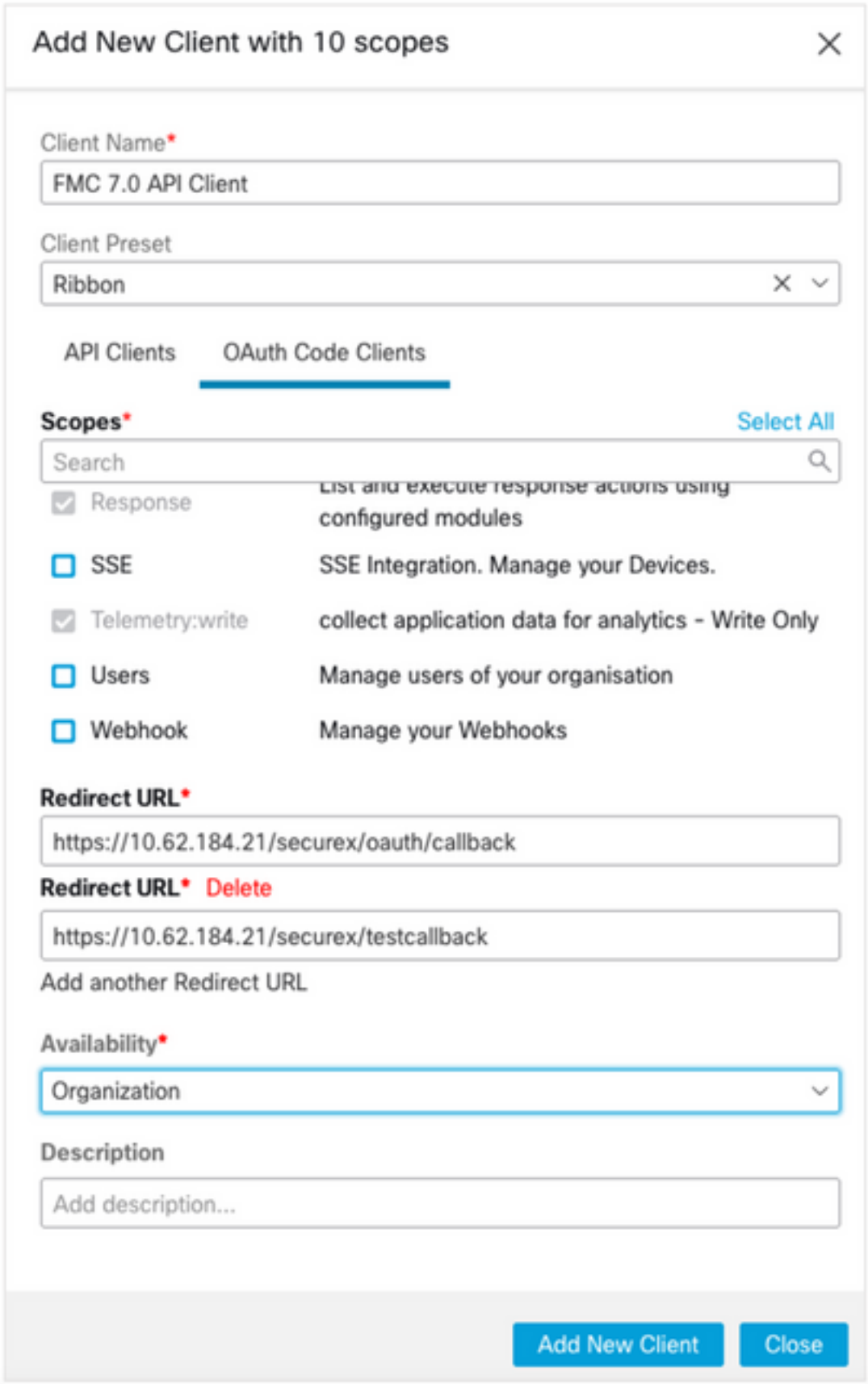
Opmerking: Deze optie is beschikbaar voor FMC versie 7.0+.

1. Meld u aan bij SecureX en maakt een API-client: Voer in het veld **Clientnaam** een beschrijvende naam van het VCC in. Bijvoorbeeld, FMC 7.0 API-client.Klik op het tabblad **Code Clients**.Kies in de vervolgkeuzelijst **Client Preset** de optie **lintje**. Het kiest het bereik: Casebook, Enrich:read, Global Intel:read, Inspect:read, notification, Orbital, Private Intel,

Profile, Response, Telemetry:Writ.Voeg de twee URL's toe die in het FMC worden getoond:
URL omleiden: <FMC_URL>/securex/auth/callback

Tweede omgekeerde URL: <FMC_URL>/securex/testcallback

1. Kies in de vervolgkeuzelijst **Beschikbaarheid** de optie **Organisatie**.Klik op **Nieuwe client toevoegen**.



2. Vanuit het VCC, navigeer naar **Systeem > SecureX**.

3. Zet de draaiknop in de rechterbovenhoek aan en bevestig dat het gebied overeenkomt met SecureX-organisatie.

4. Kopieer de **client-ID** en **clientwachtwoord** en plak deze op het VCC.

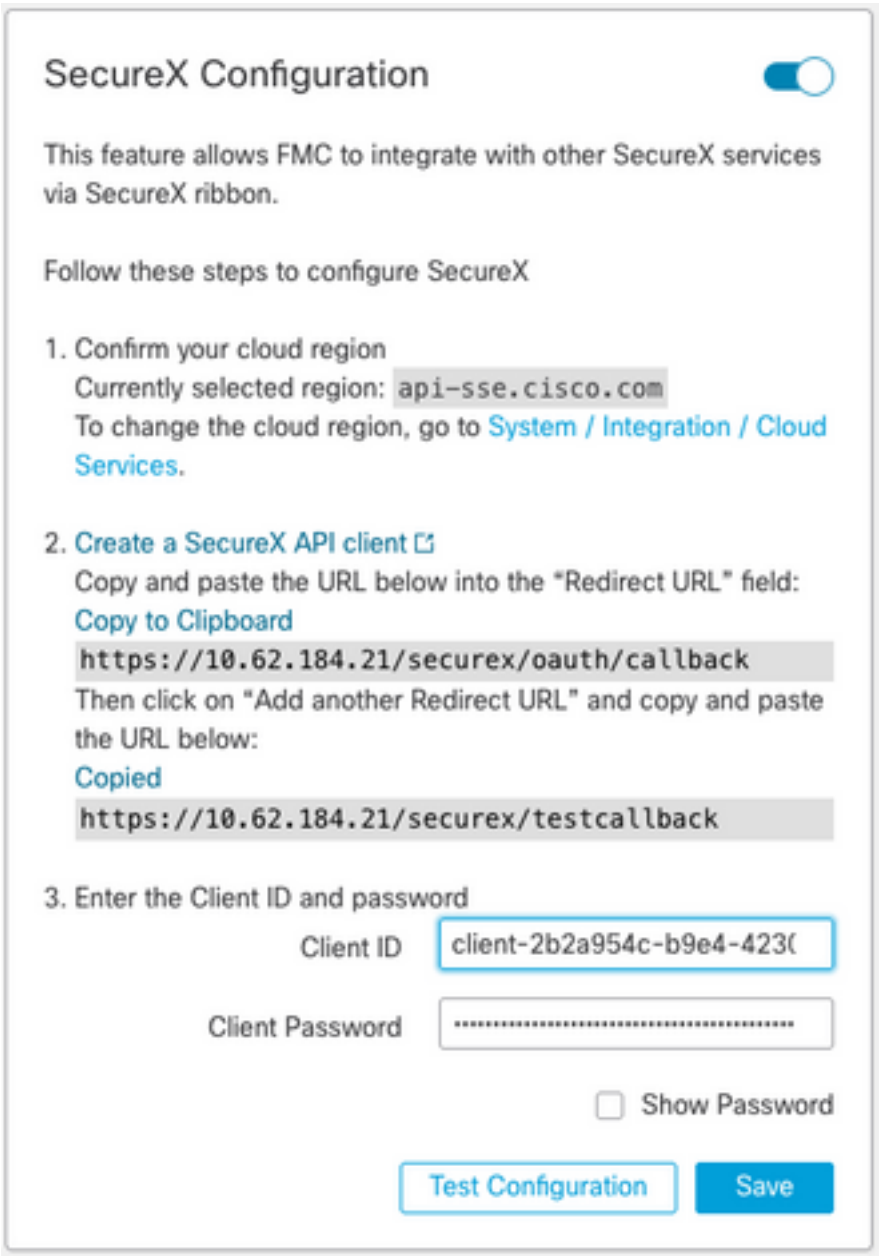
5. Kies **de configuratie**.

6. Meld u aan bij SecureX om de API-client te autoriseren.

7. Sla de wijzigingen op en verfrist de browser om het lintje onderaan te zien weergegeven.

8. Vergroot het lintje en kies **Get SecureX**. Voer de SecureX-referenties in indien dit wordt gevraagd.

9. Het SecureX-lintje is nu volledig functioneel voor uw FMC-gebruiker.

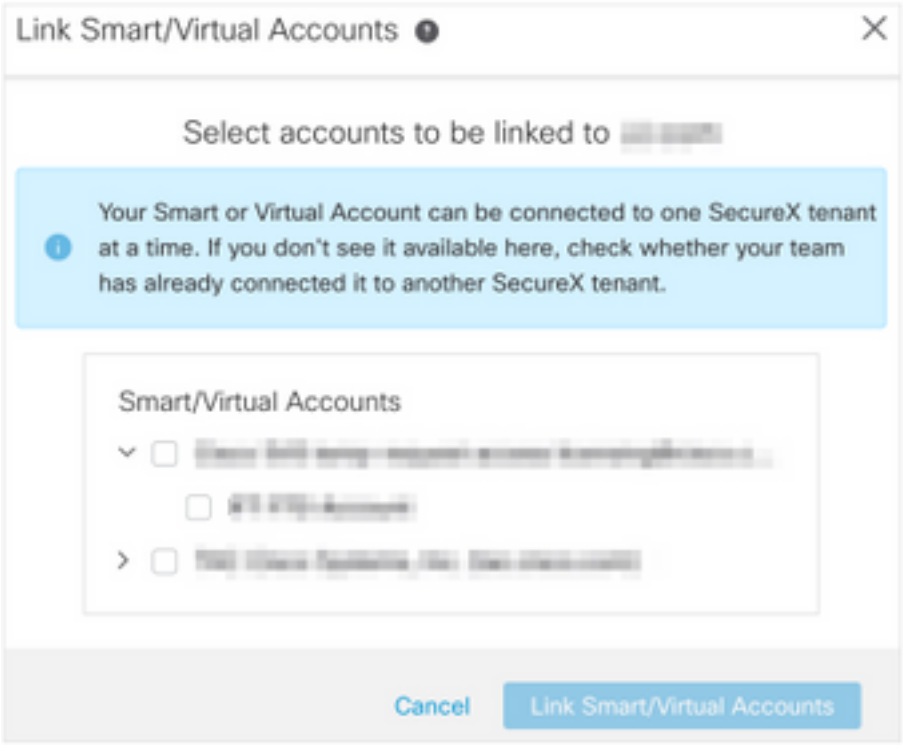


5-YVP GdzrkX8q8q0yYl-TDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

Opmerking: Als een andere FMC-gebruiker toegang tot het lintje nodig heeft, moet die gebruiker inloggen bij het lintje met SecureX-referenties.

Verzenden van verbindingsgebeurtenissen naar SecureX

1. In het FMC, navigeer naar **Systeem > Integratie > Cloudservices** en zorg ervoor dat de **Cisco Cloud Event Configuration** Inbraakgebeurtenissen, File and Malware verstuurt zoals uitgelegd in het gedeelte **Inzetten Cloud Services**.
2. Zorg ervoor dat de FMC is geregistreerd met een slimme licentie zoals wordt uitgelegd in **het** gedeelte **Smart Licenties registreren**.
3. Let op de naam van de **toegewezen virtuele account** zoals weergegeven in het FMC onder **Systeem > Licenties > Smart Licenties**.
4. Registreer de FMC in SecureX: In SecureX, navigeer naar **Administratie > Apparaten**.Kies **Apparaten beheren**.Zorg ervoor dat pop-up vensters in de browser zijn toegestaan.Meld u aan bij Security Services Exchange (SSE).Navigeer naar **het menu Gereedschappen > Verband slimme/virtuele accounts**.Kies **Link meer accounts**.Selecteer de virtuele account die aan het FMC is toegewezen (stap 3).Kies **Link Smart/Virtual Account.**



- Zorg ervoor dat het FMC-apparaat in de Apparaten is opgenomen.
- Navigeer naar het tabblad **Cloudservices**, schakel **Cisco SecureX-bedreigingsrespons** in en **uiteindelijk** functies.
- Kies de **extra service-instellingen** (pictogram versnelling) naast de optie Eindtijd.
- Kies op het tabblad Algemeen de **gegevens van gebeurtenis met Talos delen**.
- In het tabblad Auto-Promote gebeurtenissen kiest u in het gedeelte Per Event Type alle beschikbare eventtypen en **slaat u op**.

5. navigeren in het hoofdportaal SecureX naar **integratiemodules > Firepower** en voegen de FirePOWER integratiemodule toe.

6. Maak een nieuw dashboard.

7. Voeg de FirePOWER-gerelateerde tegels toe.

Geïntegreerd Secure Endpoint (AMP voor endpoints)

Om Secure Endpoint (AMP voor endpoints) integratie met uw FirePOWER-implementatie mogelijk te maken, volgt u deze stappen:

1. Navigeer naar **AMP > AMP Management**.
2. Kies **AMP-cloudverbinding toevoegen**.
3. Kies de cloud en **registreer** u.

Opmerking: De status **Ingeschakeld** betekent dat de verbinding met de cloud tot stand is gebracht.

integreren Secure Malware Analytics (Threat Grid)

Standaard kan het FireSIGHT Management Center verbinding maken met de openbare Cisco Threat Grid-wolk voor het indienen van bestanden en het ophalen van rapporten. Het is niet mogelijk om deze verbinding te verwijderen. Toch wordt aanbevolen de dichtstbijzijnde implementatiecloud te kiezen:

1. Navigeer naar **AMP > Dynamic Analysis Connections**.
2. Klik op **Bewerken** (potlood pictogram) in het gedeelte Action.
3. Kies de juiste naam voor de cloud.
4. Om de Threat Grid-account voor gedetailleerde rapportage en geavanceerde zandbakfuncties te associëren, klikt u op het pictogram **Associate**.

Zie Firepower Management Center Configuration Guide, versie 7.0 - Access to Dynamic Analysis Resultaten in the Public Cloud.

Zie Firepower Management Center Configuration Guide, versie 7.0 - Dynamic Analysis On-Premises Appliance (Cisco Threat Grid) voor de integratie van Threat Grid-apparaten.