FMC 6.6.1+ - Tips for Before and After an Upgrade

Contents

Introduction

This document describes the verification and configuration best practices to complete before and after the upgrade of Cisco Secure Firewall Management Center (FMC) to Version 6.6.1+.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Hardware: Cisco FMC 1000
- Software: Release 7.0.0 (build 94)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Top Things to Do Before the FMC Upgrade

Choose the FMC Target Software Version

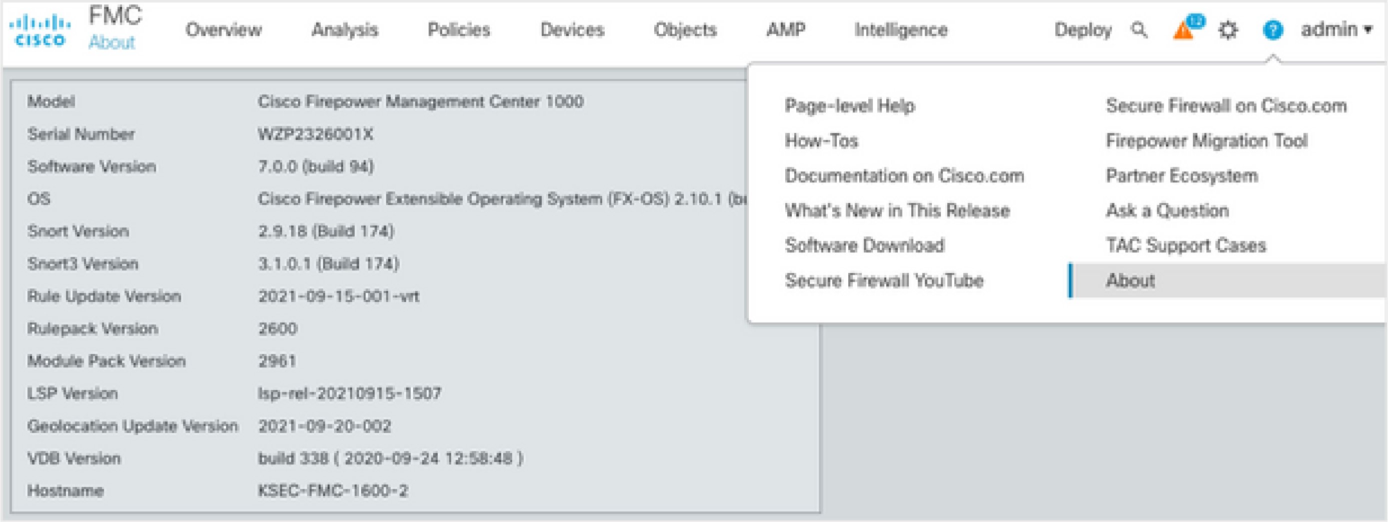
Review the [Firepower Release Notes]() for the Target Version and get familiar with:

- Compatibility
- Features and Functionality
- Resolved Issues
- Known Issues

Verify the Current FMC Model and Software Version

Verify the current FMC Model and Software Version:

1. Navigate to **Help > About**.
2. Verify the **Model** and **Software Version**.



Model	Cisco Firepower Management Center 1000
Serial Number	WZP2326001X
Software Version	7.0.0 (build 94)
OS	Cisco Firepower Extensible Operating System (FX-OS) 2.10.1 (b
Snort Version	2.9.18 (Build 174)
Snort3 Version	3.1.0.1 (Build 174)
Rule Update Version	2021-09-15-001-vrt
Rulepack Version	2600
Module Pack Version	2961
LSP Version	lsp-rel-20210915-1507
Geolocation Update Version	2021-09-20-002
VDB Version	build 338 (2020-09-24 12:58:48)
Hostname	KSEC-FMC-1600-2

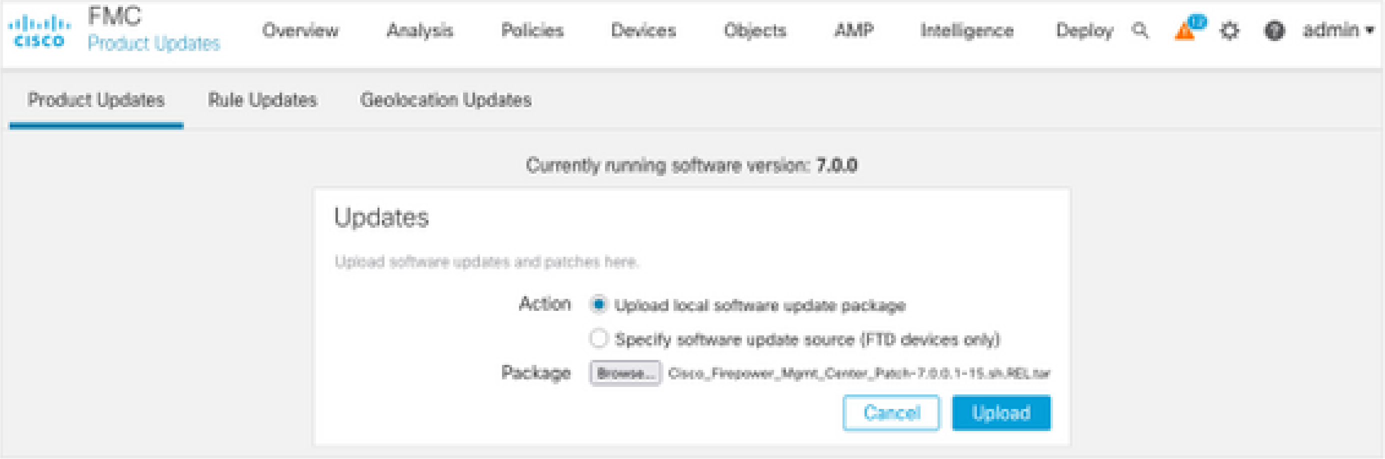
Plan the Upgrade Path

Subject to the current and target FMC software version, an interim upgrade might be required. In the Cisco Firepower Management Center Upgrade Guide, review the **Upgrade Path: Firepower Management Centers** section and plan the upgrade path.

Upload Upgrade Packages

In order to upload the upgrade package to the device, complete these steps:

1. Download the upgrade package from the Software Download page.
2. In the FMC navigate to **System > Updates**.
3. Choose the **Upload Update**.
4. Click the **Upload local software update package** radio button.
5. Click **Browse** and choose the package.
6. Click **Upload**.



Currently running software version: **7.0.0**

Updates

Upload software updates and patches here.

Action ● Upload local software update package
○ Specify software update source (FTD devices only)

Package Browse... Cisco_Firepower_Mgmt_Center_Patch-7.0.0.1-15.sh.REL.tar

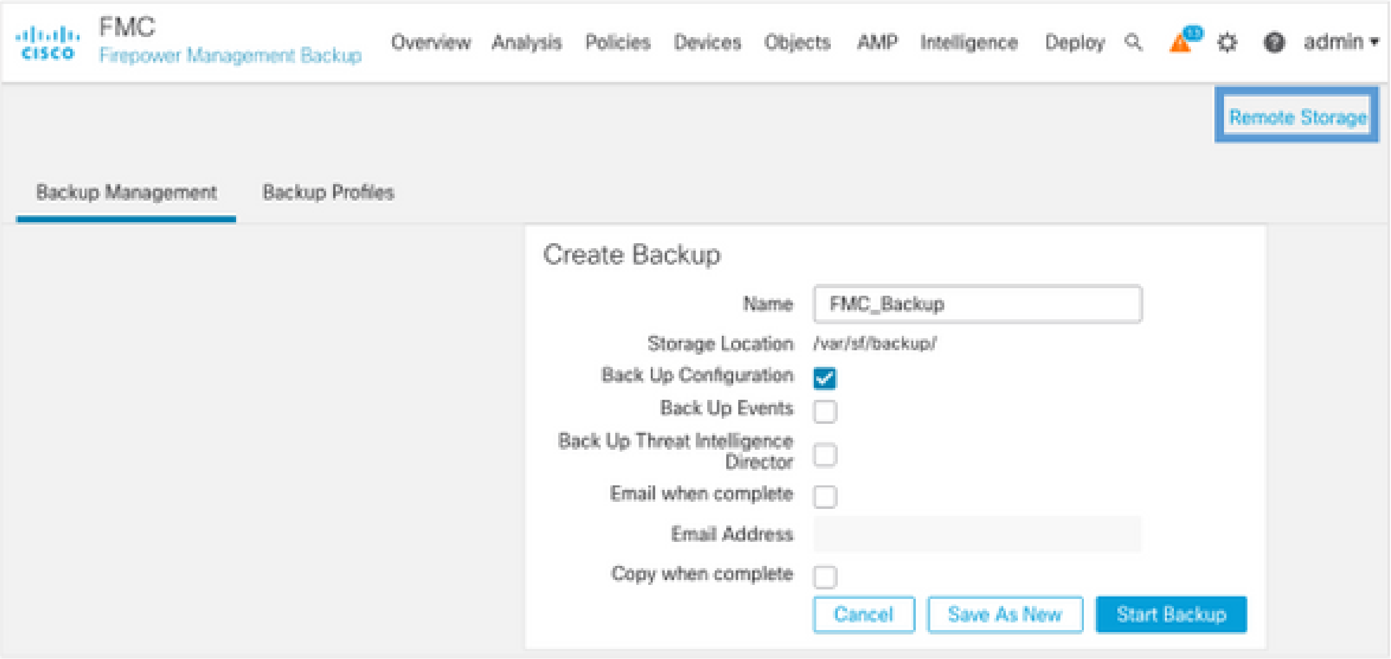
Cancel Upload

Create the FMC Backup

Backup is an important disaster recovery step, which allows to restore configuration if an upgrade fails catastrophically.

1. Navigate to **System > Tools > Backup/Restore**.
2. Choose the **Firepower Management Backup**.
3. In the **Name** field, enter the backup name.
4. Choose the Storage Location and information that should be included in the backup.
5. Click **Start Backup**.
6. From **Notification > Tasks**, monitor the Backup creation progress.

> **Tip**: We strongly recommend to back up to a secure remote location and verify transfer success. Remote Storage can be configured from the Backup Management page.



Create Backup

Name: FMC_Backup

Storage Location: /var/sf/backup/

Back Up Configuration ☑

Back Up Events □

Back Up Threat Intelligence Director □

Email when complete □

Email Address

Copy when complete □

For more information, see:

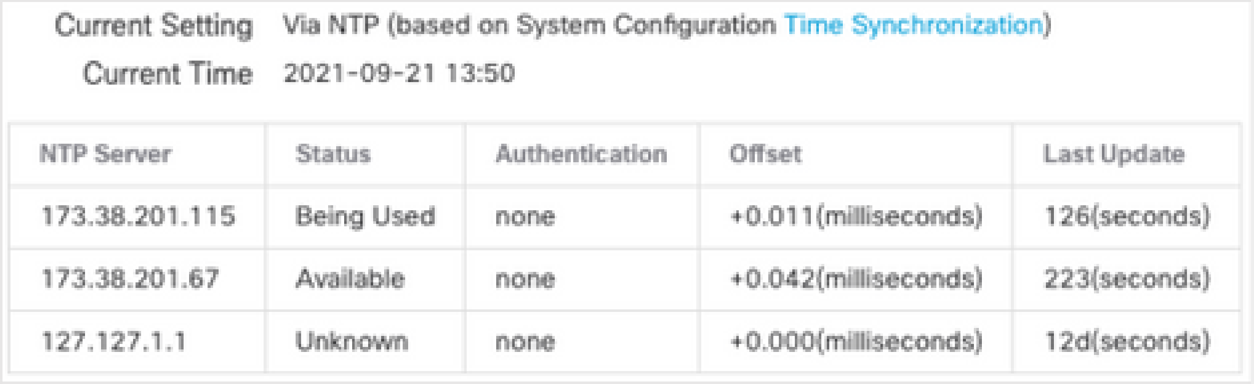
- [Firepower Management Center Configuration Guide, Version 7.0 - Chapter: Backup and Restore]
- [Firepower Management Center Configuration Guide, Version 7.0 - Remote Storage Management]

Verify NTP Synchronization

For a successful FMC upgrade, NTP synchronization is required. In order to check NTP synchronization, complete these steps:

1. Navigate to **System > Configuration > Time**.
2. Verify the **NTP Status**.

   Note: Status: "Being Used" indicates that the appliance is synchronized with the NTP server.



Current Setting: Via NTP (based on System Configuration Time Synchronization)

Current Time: 2021-09-21 13:50

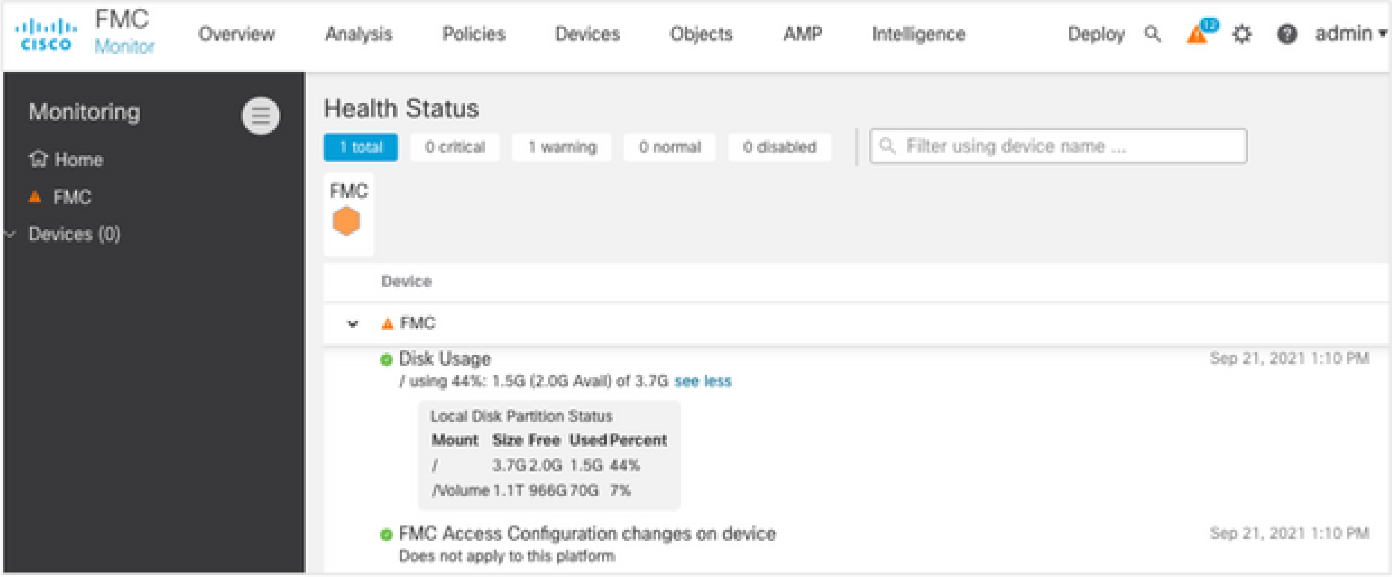
NTP Server	Status	Authentication	Offset	Last Update
173.38.201.115	Being Used	none	+0.011(milliseconds)	126(seconds)
173.38.201.67	Available	none	+0.042(milliseconds)	223(seconds)
127.127.1.1	Unknown	none	+0.000(milliseconds)	12d(seconds)

For more information, see [Firepower Management Center Configuration Guide, Version 7.0 - Time and Time Synchronization].

Verify the Disk Space

Dependent upon the FMC model and target version, ensure that there is enough of free disk space available, otherwise the upgrade fails. In order to check available FMC disk space, complete these steps:

1. Navigate to **System > Health > Monitor**.
2. Choose the FMC.
3. Expand the menu and search for **Disk Usage**.
4. The disk space requirements can be found in Time Tests and Disk Space Requirements.



Disk Usage — Sep 21, 2021 1:10 PM
/ using 44%: 1.5G (2.0G Avail) of 3.7G see less

Local Disk Partition Status

Mount	Size	Free	Used	Percent
/	3.7G	2.0G	1.5G	44%
/Volume	1.1T	966G	70G	7%

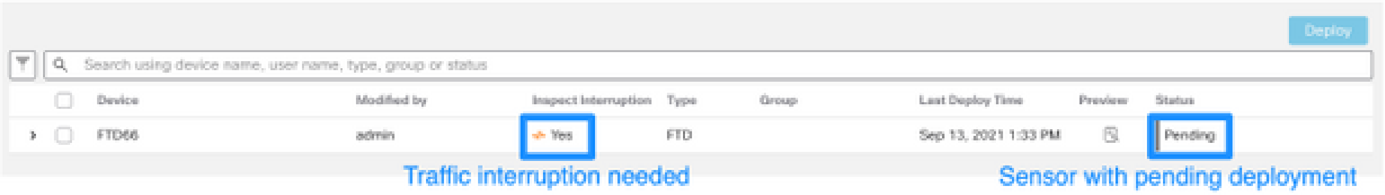
FMC Access Configuration changes on device — Sep 21, 2021 1:10 PM
Does not apply to this platform

Deploy All Pending Policy Changes

Before the update or patch installation, it is required to deploy changes into the sensors. In order to ensure that all pending changes are deployed, complete these steps:

1. Navigate to **Deploy > Deployment**.
2. Choose all devices in the list and **Deploy**.

   Caution: The Inspect Interruption column indicates traffic interruption



□	Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
□	FTD66	admin	Yes	FTD		Sep 13, 2021 1:33 PM		Pending

Traffic interruption needed

Sensor with pending deployment

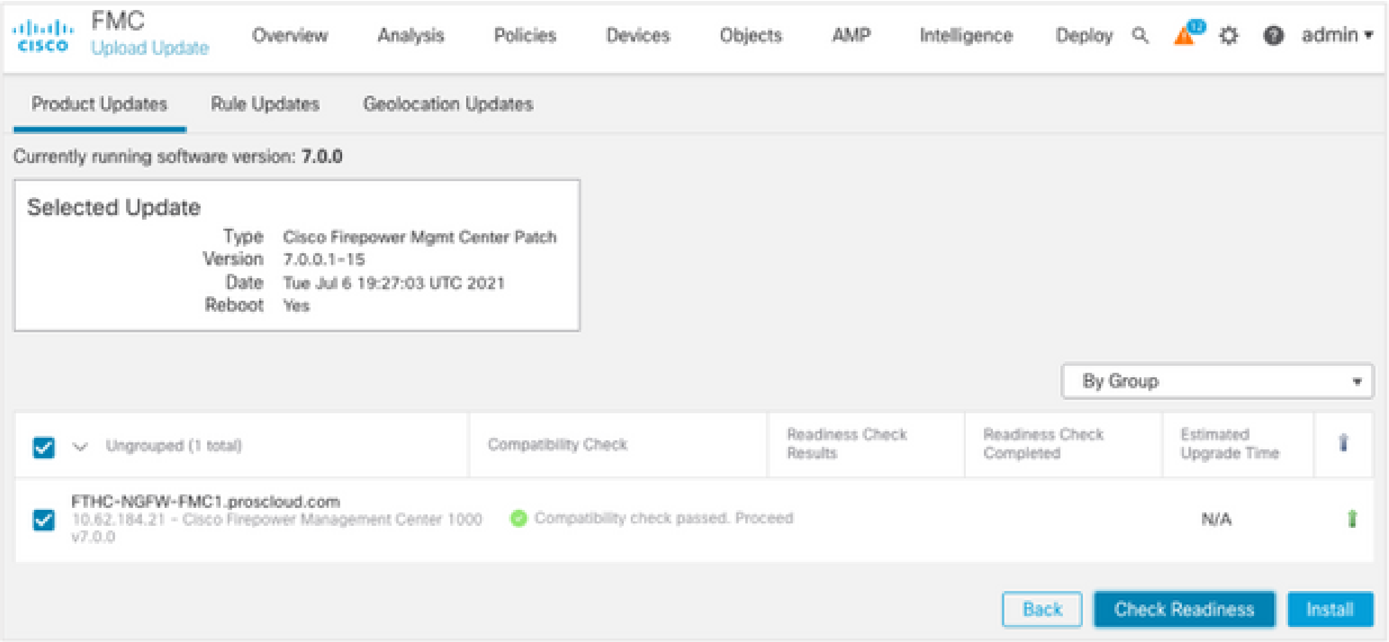
Run Firepower Software Readiness Checks

Readiness checks assess a Firepower appliance's preparedness for a software upgrade.

In order to perform the Software Readiness Checks, complete these steps:

1. Navigate to **System > Updates**.
2. Select the **Install** icon next to the target version.
3. Choose the FMC and click **Check Readiness**.
4. In the pop-up window, click **OK**.

5. Monitor the Readiness Check process from **Notifications > Tasks**.



Currently running software version: **7.0.0**

Selected Update

Type	Cisco Firepower Mgmt Center Patch
Version	7.0.0.1-15
Date	Tue Jul 6 19:27:03 UTC 2021
Reboot	Yes

By Group

☑ Ungrouped (1 total)	Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time
☑ FTHC-NGFW-FMC1.proscloud.com 10.62.184.21 - Cisco Firepower Management Center 1000 v7.0.0	Compatibility check passed. Proceed			N/A

For more information, see [Cisco Firepower Management Center Upgrade Guide - Firepower Software Readiness Checks]().

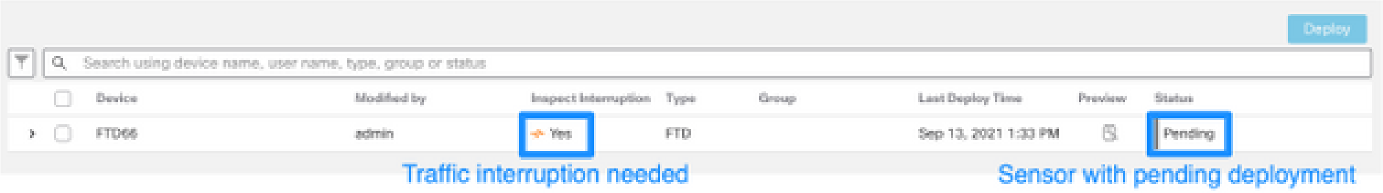
Top Things to Do After the FMC Upgrade

Deploy All Pending Policy Changes

Immediately after every update or patch installation, it is required to deploy changes into the sensors. In order to ensure that all pending changes are deployed, complete these steps:

1. Navigate to **Deploy > Deployment**.
2. Choose all devices in the list and click **Deploy**.

   Caution: The Inspect Interruption column indicates traffic interruption


Deploy
Search using device name, user name, type, group or status
Traffic interruption needed
Sensor with pending deployment

□ Device	Modified by	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
□ FTD66	admin	Yes	FTD		Sep 13, 2021 1:33 PM		Pending

Verify if the Latest Vulnerability and Fingerprint Database is Installed

In order to verify the current Fingerprint (VDB) version, complete these steps:

1. Navigate to **Help > About**.
2. Verify the **VDB Version**.

In order to download the VDB updates directly from cisco.com, reachability from the FMC to cisco.com is required.

1. Navigate to **System > Updates > Product Updates**.

2. Choose **Download updates**.
3. Install the latest version available.
4. You must redeploy the sensors afterward.

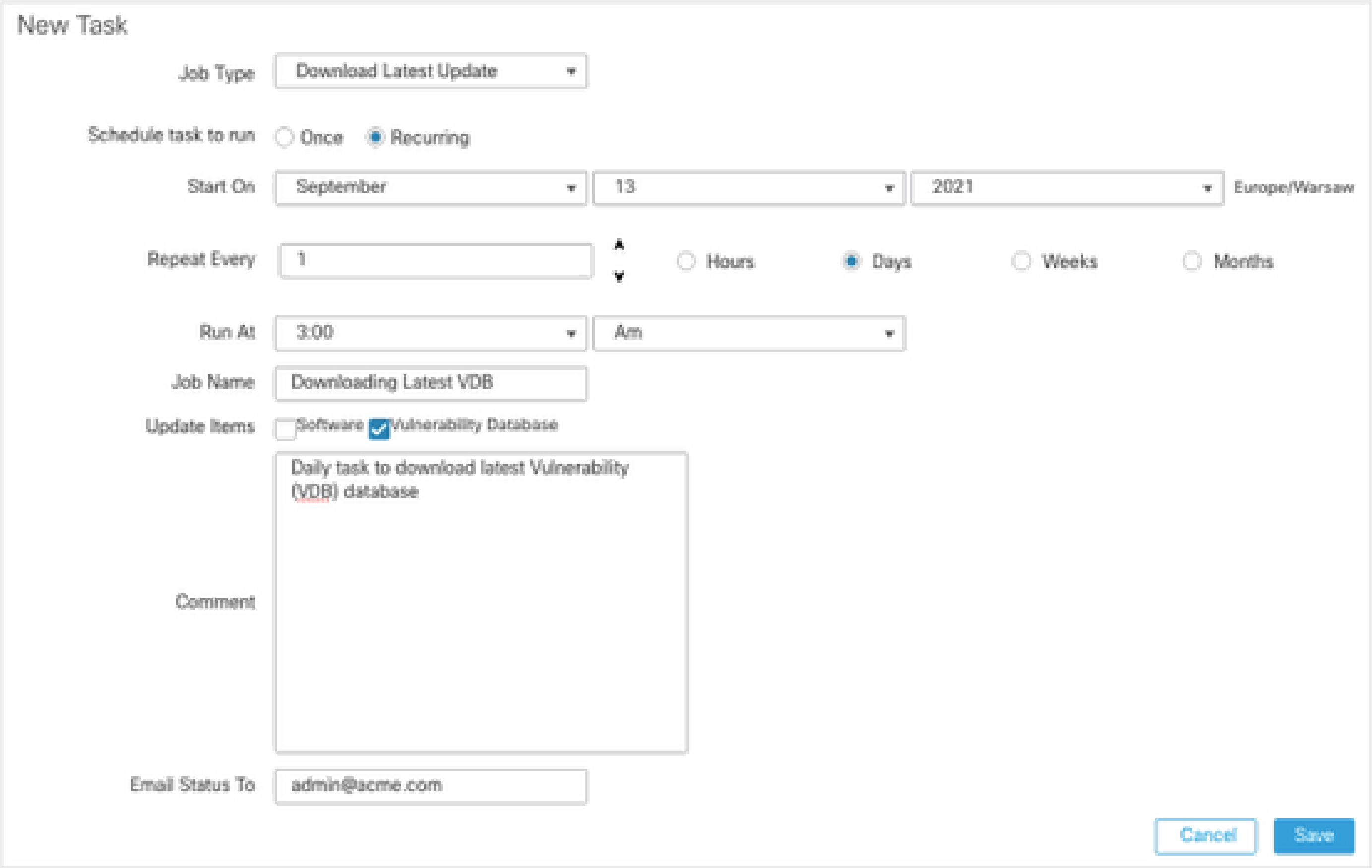
   Note: If the FMC does not have Internet access, the VDB package can be download directly from software.cisco.com.

It is recommended to schedule tasks to perform automatic VDB package downloads and installations.

As a good practice, check for VDB updates daily and install them on the FMC during the weekends.

In order to check the VDB daily from www.cisco.com, complete these steps:

1. Navigate to **System > Tools > Scheduling**.
2. Click **Add Task**.
3. From the **Job Type** drop-down list, choose **Download Latest Update.**
4. For **Schedule task to run**, click the **Recurring** radio button**.**
5. Repeat the task every day and run it at 3:00 AM or outside business hours.
6. For **Update Items**, check the **Vulnerability Database** check box**.**



New Task

Job Type: Download Latest Update

Schedule task to run: ○ Once ● Recurring

Start On: September 13 2021 Europe/Warsaw

Repeat Every: 1 ○ Hours ● Days ○ Weeks ○ Months

Run At: 3:00 Am

Job Name: Downloading Latest VDB

Update Items: □ Software ☑ Vulnerability Database

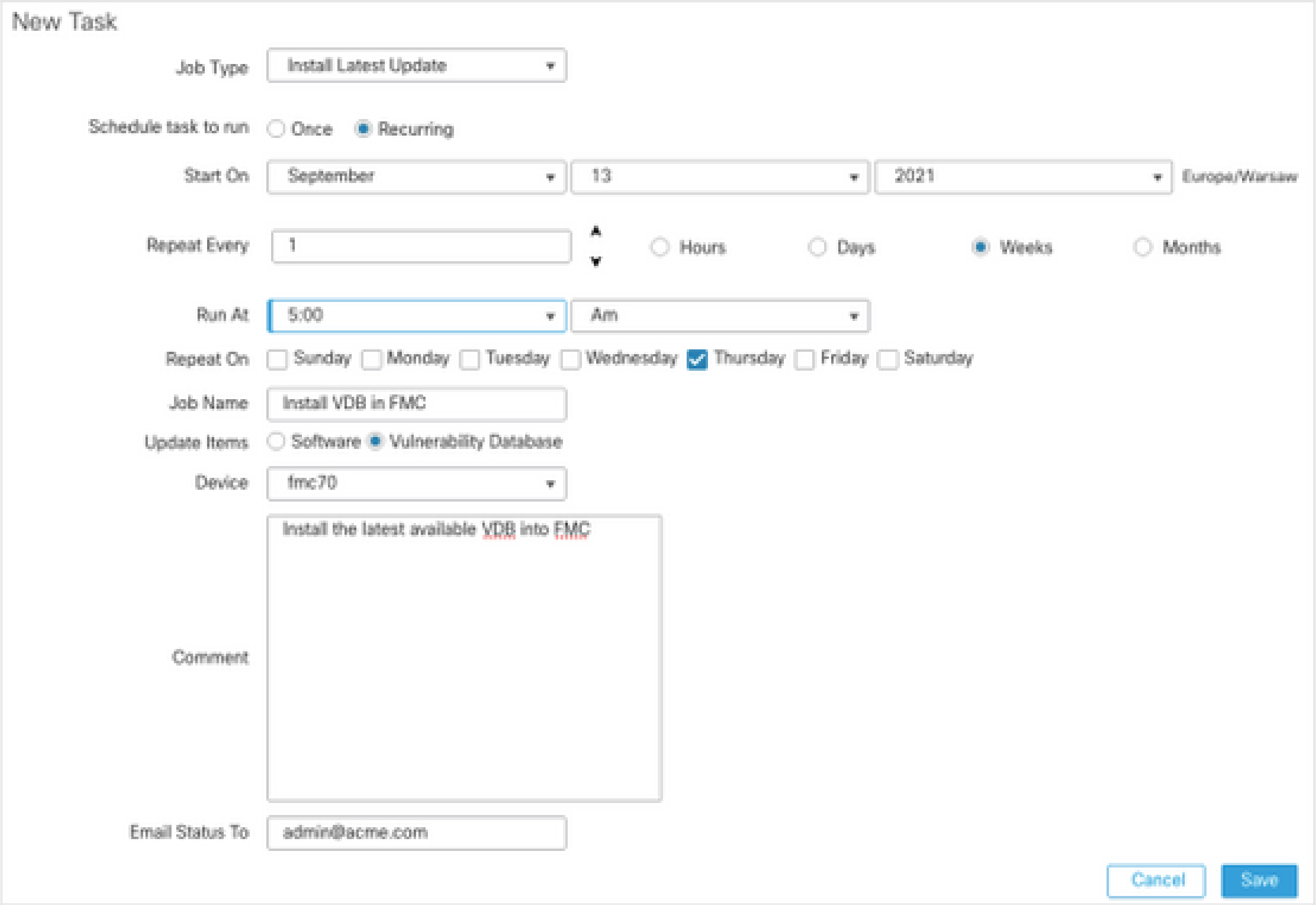
Comment: Daily task to download latest Vulnerability (VDB) database

Email Status To: admin@acme.com

In order to install the latest VDB into the FMC, set the periodic task weekly:

1. Navigate to **System > Tools > Scheduling**.
2. Click **Add Task**.
3. From the **Job Type** drop-down list, choose **Install Latest Update**.
4. For **Schedule Task to run**, click the **Recurring** radio button.

5. Repeat the task every 1 week and run it at 5:00 AM or outside business hours.
6. For **Update Items**, check the **Vulnerability Database** check box**.**



New Task

Job Type: Install Latest Update

Schedule task to run: ○ Once ● Recurring

Start On: September 13 2021 Europe/Warsaw

Repeat Every: 1 ○ Hours ○ Days ● Weeks ○ Months

Run At: 5:00 Am

Repeat On: □ Sunday □ Monday □ Tuesday □ Wednesday ☑ Thursday □ Friday □ Saturday

Job Name: Install VDB in FMC

Update Items: ○ Software ● Vulnerability Database

Device: fmc70

Comment: Install the latest available VDB into FMC

Email Status To: admin@acme.com

For more information, see [Firepower Management Center Configuration Guide, Version 7.0 - Update the Vulnerability Database (VDB)]

Verify the Snort Rule and Lightweight Security Package Current Version

In order to verify the current Snort Rule (SRU), Lightweight Security Package (LSP), and Geolocation versions, complete these steps:

1. Navigate to **Help > About**.
2. Verify the **Rule Update Version** and **LSP Version**.

To download the SRU and LSP directly from www.cisco.com, reachability from the FMC to www.cisco.com is required.

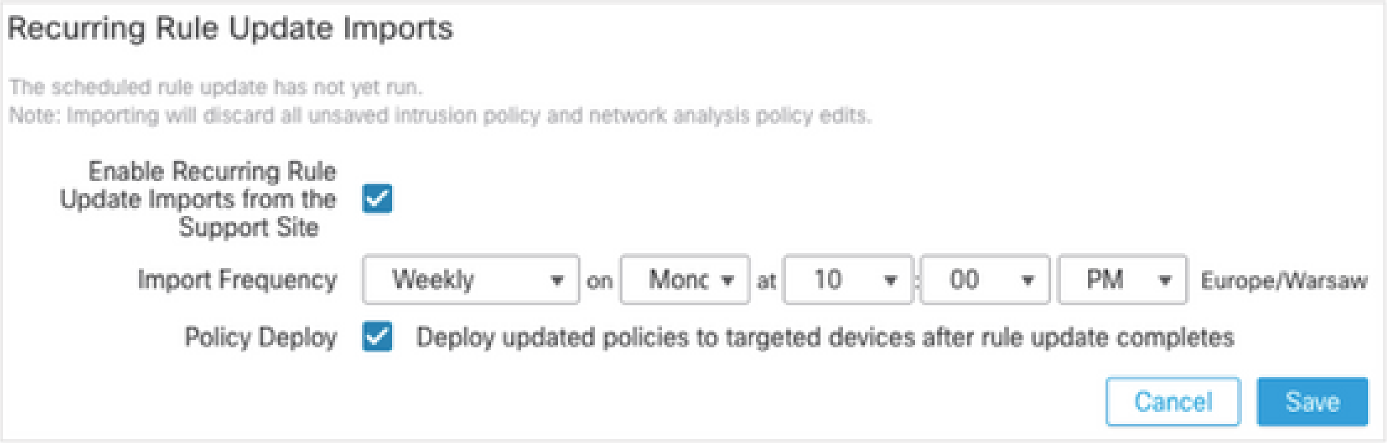
1. Navigate to **System > Updates > Rule Updates**.
2. From the **One-Time Rule Update/Rules Import** tab, choose **Download new rule update from the Support Site**.
3. Choose **Import**.
4. Deploy the configuration to the sensors afterwards.

> **Note**: If the FMC does not have Internet access, the SRU and LSP packages can be downloaded directly from software.cisco.com.

Intrusion rule updates are cumulative, and it is recommended to always import the latest update.

In order to turn on the weekly download and deployment of snort rule updates (SRU/LSP), complete these steps:

1. Navigate to **System > Updates > Rule Updates**.
2. In the **Recurring Rule Update Imports** tab, check the **Enable Recurring Rule Update Imports from the Support Site** check box.
3. Choose the import frequency as weekly, pick one day of the week and late afternoon for the download and policy deploy.
4. Click **Save**.



Recurring Rule Update Imports

The scheduled rule update has not yet run.
Note: Importing will discard all unsaved intrusion policy and network analysis policy edits.

Enable Recurring Rule Update Imports from the Support Site ☑

Import Frequency: Weekly on Monc at 10 : 00 PM Europe/Warsaw

Policy Deploy ☑ Deploy updated policies to targeted devices after rule update completes

For more information, see Firepower Management Center Configuration Guide, Version 7.0 - Update Intrusion Rules.

Verify the Geolocation Update Current Version

In order to verify the current Geolocation version, complete these steps:

1. Navigate to **Help > About**.
2. Verify the **Geolocation Update Version**.

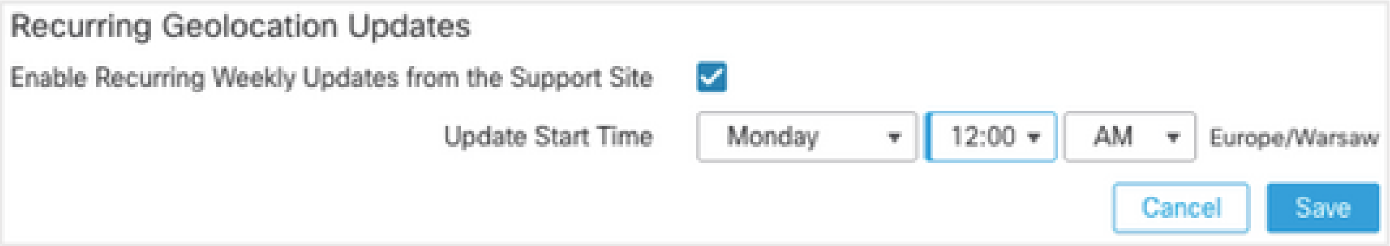
To download Geolocation Updates directly from www.cisco.com, reachability from the FMC to www.cisco.com is required.

1. Navigate to **System > Updates > Geolocation Updates**.
2. From the **One-Time Geolocation Update** tab, choose **Download and install geolocation update from the Support Site**.
3. Click **Import**.

> **Note**: If the FMC does not have Internet access, the Geolocation Updates package can be downloaded directly from software.cisco.com.

In order to turn on the automatic Geolocation Updates, complete these steps:

1. Navigate to **System > Updates > Geolocation Updates**.
2. In the Recurring Geolocation Updates section, check the **Enable Recurring Weekly Updates from the Support Site** check box.
3. Choose the import frequency as weekly, pick Monday at midnight.
4. Click **Save**.



Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site ☑

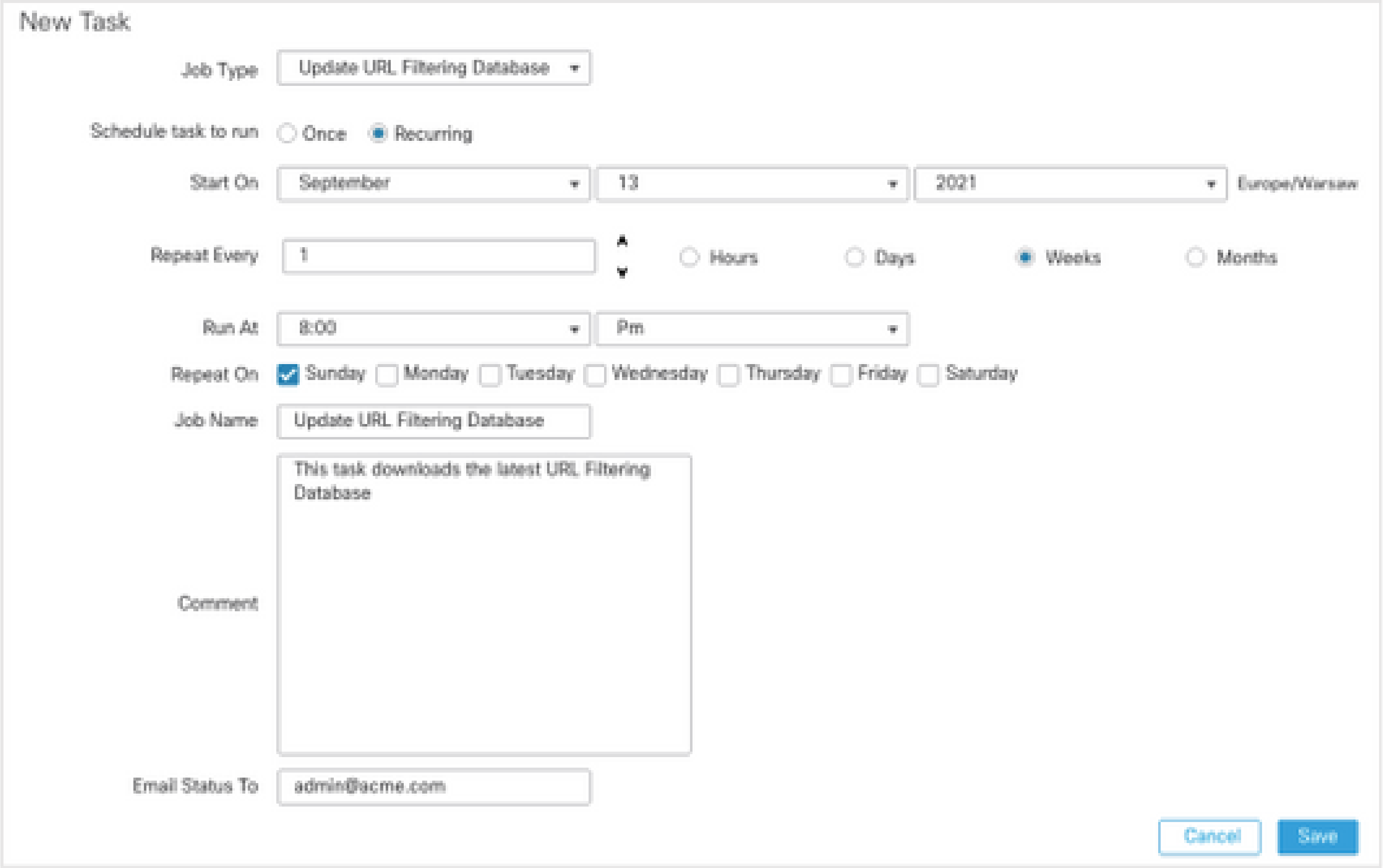
Update Start Time: Monday ▾ | 12:00 ▾ | AM ▾ | Europe/Warsaw

For more information, see [Firepower Management Center Configuration Guide, Version 7.0 - Update the Geolocation Database (GeoDB)]().

Automate URL Filtering Database Update with Scheduled Task

In order to ensure that threat data for URL filtering is current, the system must obtain data updates from the Cisco Collective Security Intelligence (CSI) cloud. To automate this process, follow these steps:

1. Navigate to **System > Tools > Scheduling**.
2. Click **Add Task**.
3. From the **Job Type** drop-down list, choose **Update URL Filtering Database.**
4. For **Schedule task to run**, click the **Recurring** radio button.
5. Repeat the task every week and run it at 8:00 PM on Sundays or outside business hours.
6. Click **Save**.



New Task

Job Type: Update URL Filtering Database ▾

Schedule task to run: ○ Once ● Recurring

Start On: September ▾ | 13 ▾ | 2021 ▾ | Europe/Warsaw

Repeat Every: 1 | ○ Hours ○ Days ● Weeks ○ Months

Run At: 8:00 ▾ | Pm ▾

Repeat On: ☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Job Name: Update URL Filtering Database

Comment: This task downloads the latest URL Filtering Database

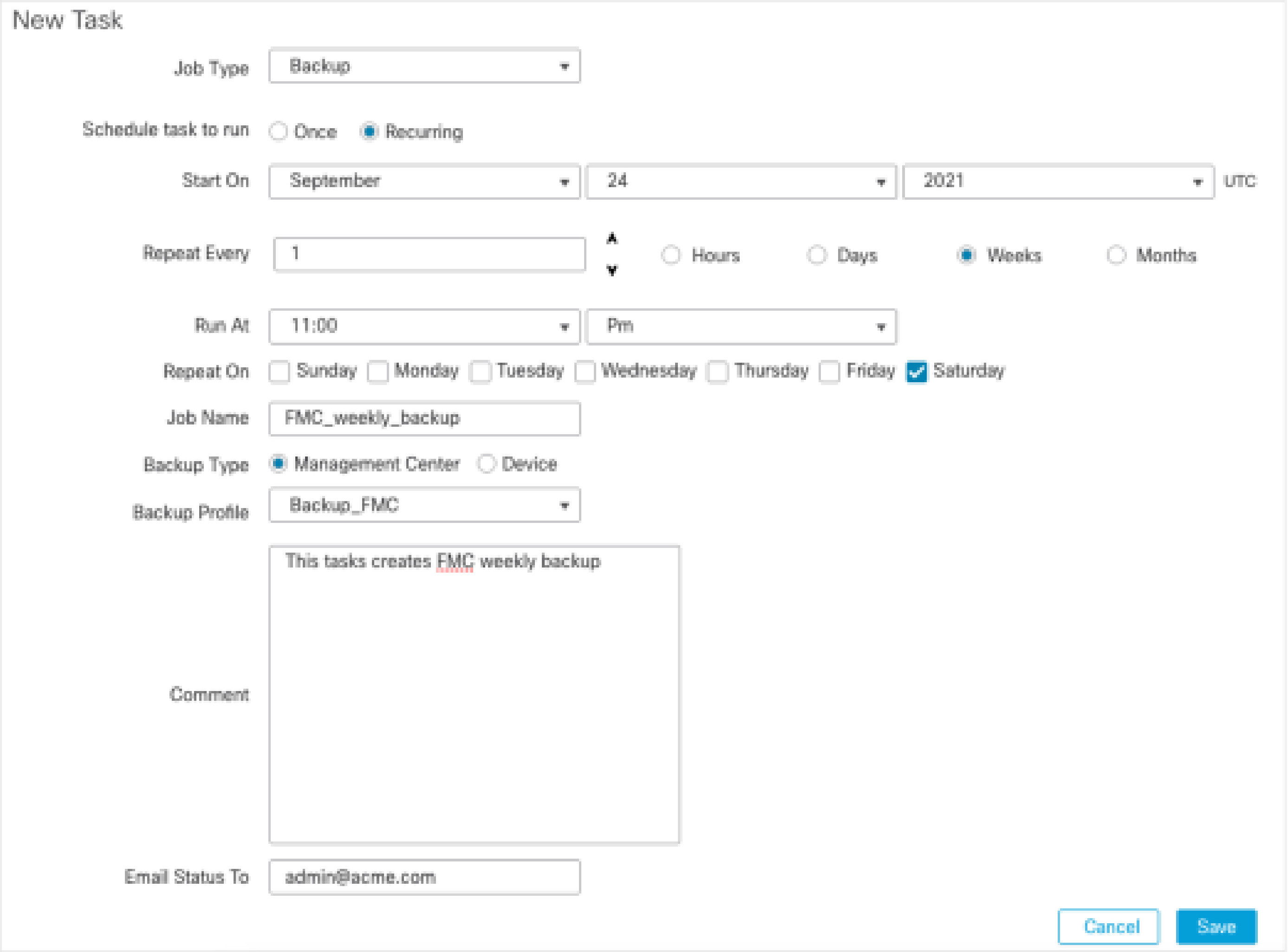
Email Status To: admin@acme.com

For more information, see [Firepower Management Center Configuration Guide, Version 7.0 - Automating URL Filtering Updates Using a Scheduled Task]().

Configure Periodic Backups

As part of the disaster recovery plan, it is recommended to perform periodic backups.

1. Ensure that you are in the **global domain**.
2. Create the FMC backup profile. For more information, see the **Create the FMC Backup** section.
3. Navigate to **System > Tools > Scheduling**.
4. Click **Add Task**.
5. From the **Job Type** drop-down list, choose **Backup.**
6. For **Schedule task to run**, click the **Recurring** radio button.
   The backup frequency must be adjusted to fit the organization's needs. We recommend to create backups during a maintenance window or other time of low use.
7. For **Backup Type**, click the **Management Center** radio button.
8. From the **Backup Profile** drop-down list, choose the Backup Profile.
9. Click **Save**.



New Task

Job Type: Backup

Schedule task to run: ○ Once ● Recurring

Start On: September | 24 | 2021 UTC

Repeat Every: 1 ○ Hours ○ Days ● Weeks ○ Months

Run At: 11:00 | Pm

Repeat On: □ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday ☑ Saturday

Job Name: FMC_weekly_backup

Backup Type: ● Management Center ○ Device

Backup Profile: Backup_FMC

Comment: This tasks creates FMC weekly backup

Email Status To: admin@acme.com

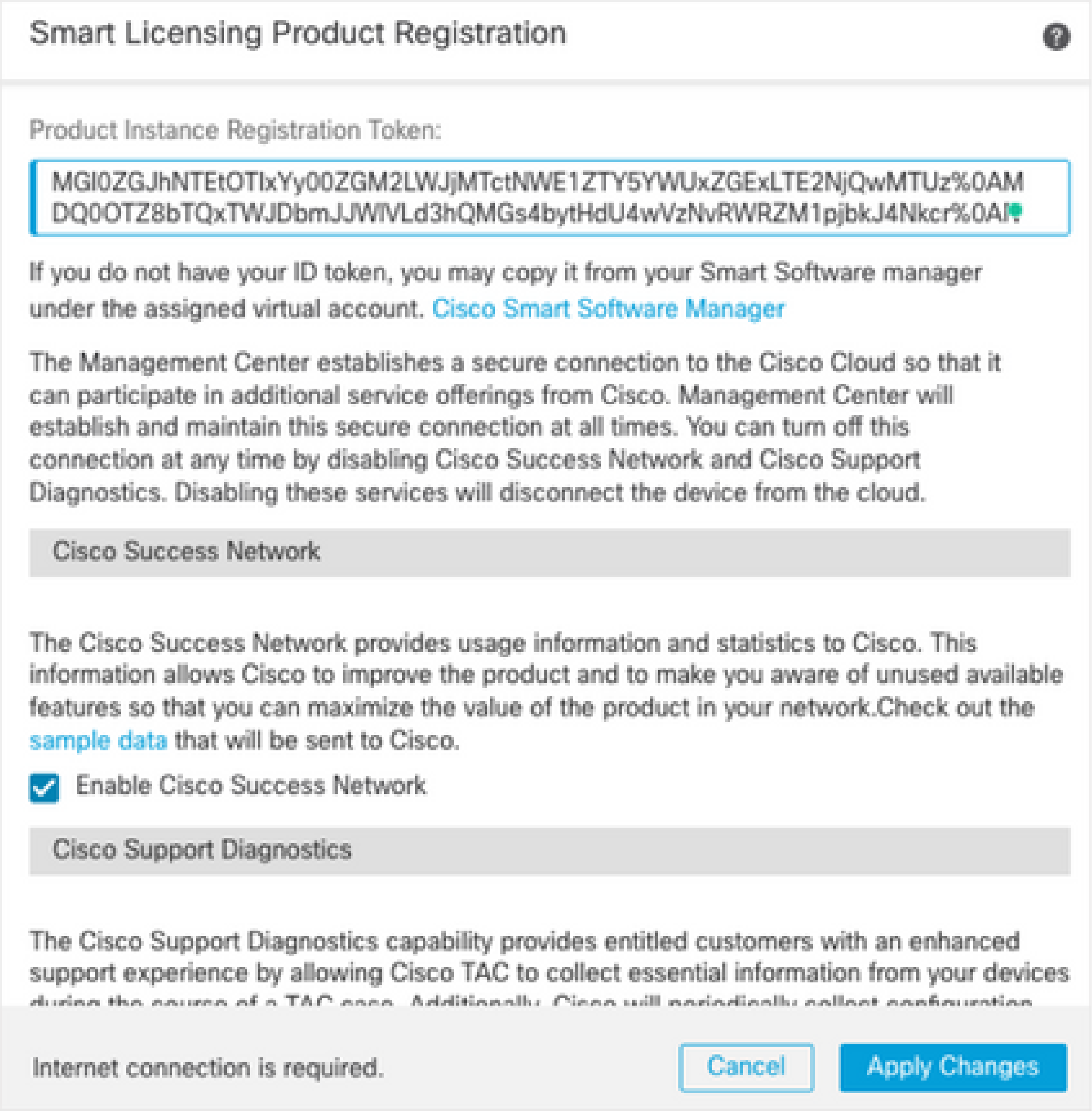
For more information, see [Firepower Management Center Configuration Guide, Version 7.0 - Chapter: Backup and Restore]().

Ensure that the Smart License is Registered

In order to register the Cisco Firewall Management Center with the Cisco Smart Software Manager, complete these steps:

1. In https://software.cisco.com, navigate to **Smart Software Manager > Manage licenses**.

2. Navigate to **Inventory > General** tab and create a **New Token**.
3. In the FMC UI, navigate to **System > Licenses > Smart Licenses**.
4. Click **Register**.
5. Insert the Token generated in the Cisco Smart Software Licensing portal.
6. Ensure that **The Cisco Success Network is enabled**.
7. Click **Apply Changes**.
8. Verify The Smart License Status.



Smart Licensing Product Registration

Product Instance Registration Token:

MGI0ZGJhNTEtOTIxYy00ZGM2LWJjMTctNWE1ZTY5YWUxZGExLTE2NjQwMTUz%0AM
DQ0OTZ8bTQxTWJDbmJJWlVLd3hQMGs4bytHdU4wVzNvRWRZM1pjbkJ4Nkcr%0AI

If you do not have your ID token, you may copy it from your Smart Software manager under the assigned virtual account. Cisco Smart Software Manager

The Management Center establishes a secure connection to the Cisco Cloud so that it can participate in additional service offerings from Cisco. Management Center will establish and maintain this secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network and Cisco Support Diagnostics. Disabling these services will disconnect the device from the cloud.

Cisco Success Network

The Cisco Success Network provides usage information and statistics to Cisco. This information allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.Check out the sample data that will be sent to Cisco.

☑ Enable Cisco Success Network

Cisco Support Diagnostics

The Cisco Support Diagnostics capability provides entitled customers with an enhanced support experience by allowing Cisco TAC to collect essential information from your devices during the course of a TAC case. Additionally, Cisco will periodically collect configuration

Internet connection is required.

For more information, see [Firepower Management Center Configuration Guide, Version 7.0 - Register Smart Licenses]().

Review the Configuration of the Variable Sets

Ensure HOME_NET variable contains only the inside networks/subnets in the organization. Improper variable set definition adversely impacts the firewall's performance.

1. Navigate to **Objects > Variable Set**.
2. Edit the variable set used by your intrusion policy. It is allowed to have one variable set per intrusion policy with different settings.
3. Adjust the variables according to your environment and click **Save**.

Other variables of interest are DNS_SERVERS OR HTTP_SERVERS.

For more information, see Firepower Management Center Configuration Guide, Version 7.0 - Variable Sets.

Verify the Cloud Services Enablement

In order to take advantage of the different cloud services, navigate to **System > Integration > Cloud Services**.

URL Filtering

1. Enable URL Filtering and allow automatic updates, turn on Query Cisco Cloud for Unknown URLs.
   A more frequent Cache URL expiration requires more queries to the cloud which results in slower web loads.
2. **Save the changes.**

   Tip: For cache URL expiration, leave the default **Never**. If stricter web reclassification is needed this setting can be modified accordingly.

AMP for Networks

1. Ensure both settings are on: **Enable automatic Local Malware Detection Updates** and **Share URI from Malware Events with Cisco**.
2. In FMC 6.6.X, disable the use of legacy port 32137 for AMP for Networks so the TCP port used instead is 443.
3. **Save the changes.**

   Note: This setting is no longer available in FMC 7.0+ and the port is always 443.

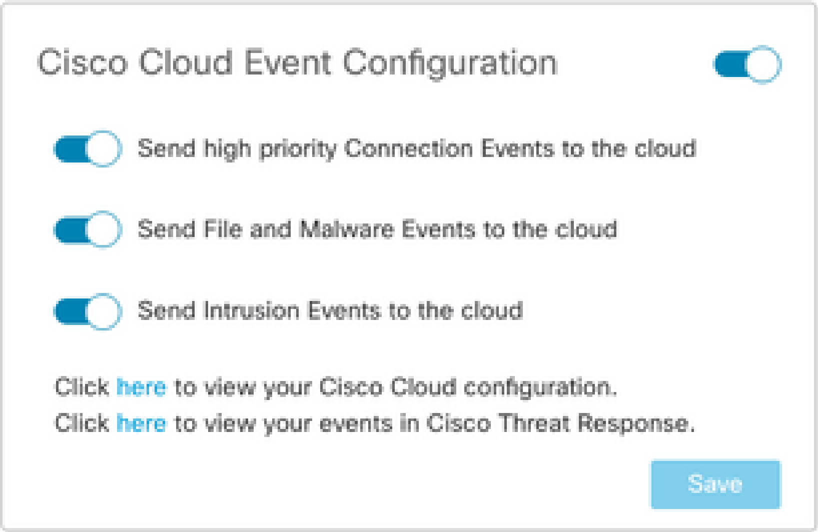
Cisco Cloud Region

1. The cloud region needs to match with the SecureX organization region. If the SecureX organization is not created, choose the region closer to the FMC installation: APJ Region, EU Region, or US Region.
2. **Save the changes.**

Cisco Cloud Event Configuration

For FMC 6.6.x

1. Ensure all three options: **Send high priority Connection Events to the cloud**, **Send File and Malware Events to the cloud**, and **Send Intrusion Events to the cloud** are chosen.
2. **Save the changes.**



Cisco Cloud Event Configuration

Send high priority Connection Events to the cloud

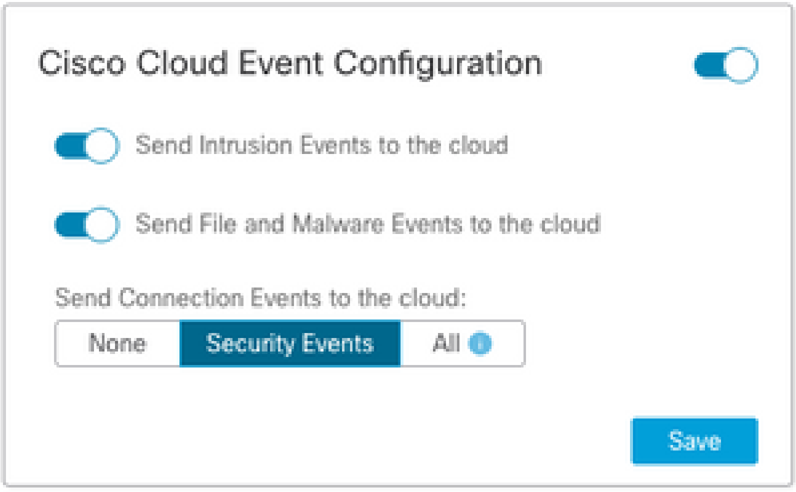
Send File and Malware Events to the cloud

Send Intrusion Events to the cloud

Click here to view your Cisco Cloud configuration.
Click here to view your events in Cisco Threat Response.

For FMC 7.0+

1. Ensure both options are chosen: **Send Intrusion Events to the cloud** and **Send File and Malware Events to the cloud**.
2. For the type of connection events, choose **All** if Security Analytics and Logging solution is in use. For SecureX, choose only **Security Events**.
3. **Save the changes.**



Cisco Cloud Event Configuration

Send Intrusion Events to the cloud

Send File and Malware Events to the cloud

Send Connection Events to the cloud:

None | Security Events | All

Enable SecureX Integration

The SecureX integration provides instant visibility into the threat landscape across your Cisco security products. In order to connect SecureX and enable the ribbon, follow these steps:

Integrate SecureX Ribbon

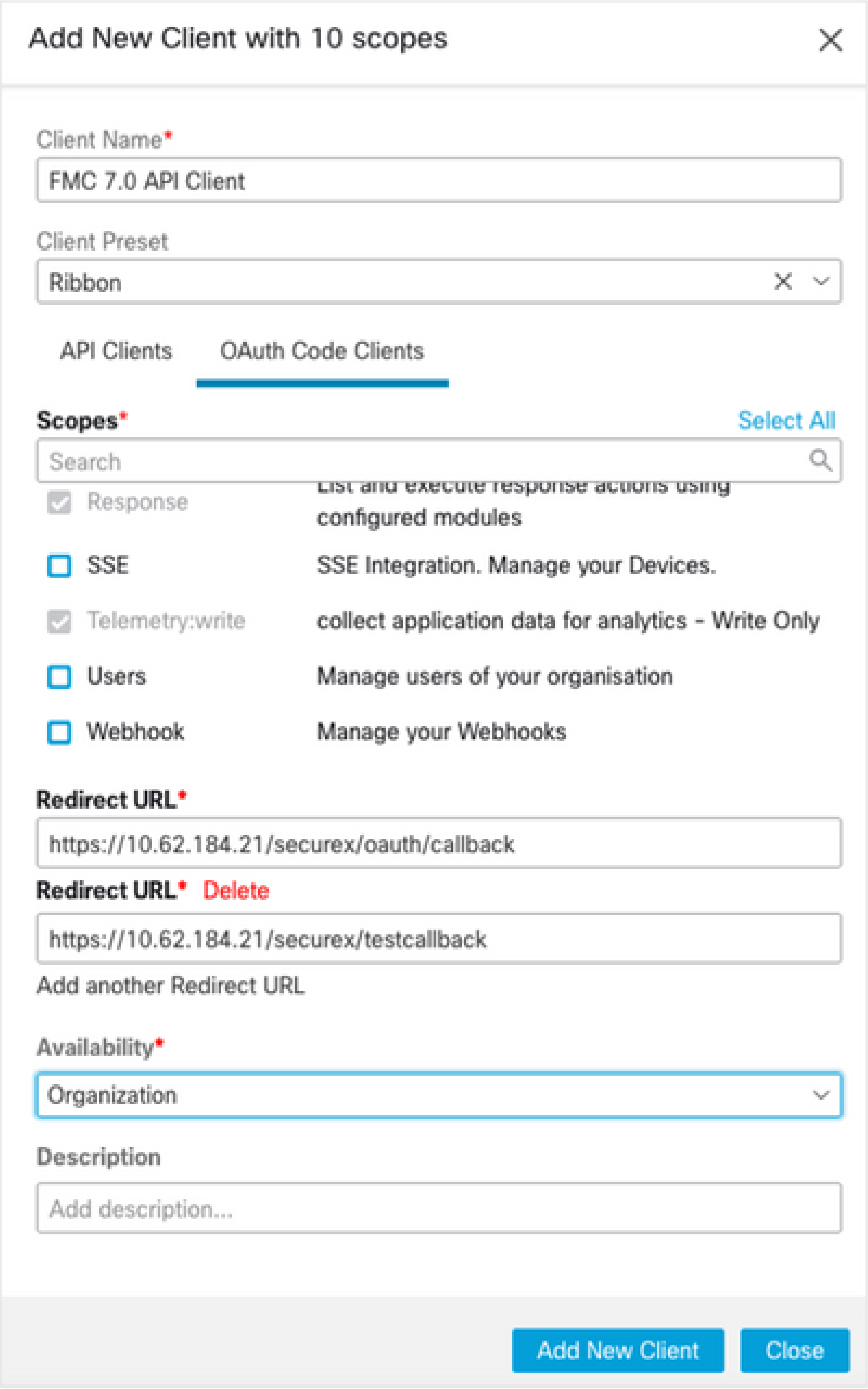
Note: This option is available for FMC version 7.0+.

1. Log into SecureX and create an API client: In the **Client Name** field, enter a descriptive name of the FMC. For example, FMC 7.0 API Client.Click the **Oauth Code Clients** tab.In the **Client Preset** drop-down list, choose **Ribbon**. It chooses the scopes: Casebook, Enrich:read, Global Intel:read, Inspect:read, Notification, Orbital, Private Intel, Profile, Response, Telemetry:write.Add the two redirect URLs presented in the FMC:

Redirect URL: <FMC_URL>/securex/oauth/callback

Second Redirect URL: <FMC_URL>/securex/testcallback

1. In the **Availability** drop-down list, choose **Organization**.Click **Add New Client**.



Add New Client with 10 scopes

Client Name*

FMC 7.0 API Client

Client Preset

Ribbon

API Clients   OAuth Code Clients

Scopes*   Select All

Search

☑ Response — List and execute response actions using configured modules

□ SSE — SSE Integration. Manage your Devices.

☑ Telemetry:write — collect application data for analytics - Write Only

□ Users — Manage users of your organisation

□ Webhook — Manage your Webhooks

Redirect URL*

https://10.62.184.21/securex/oauth/callback

Redirect URL* Delete

https://10.62.184.21/securex/testcallback

Add another Redirect URL

Availability*

Organization

Description

Add description...

2. From the FMC, navigate to **System > SecureX**.

3. Turn on the toggle in the upper right corner and confirm that the region shown matches with SecureX organization.

4. Copy the **Client Id** and **Client Password** and paste them into the FMC.

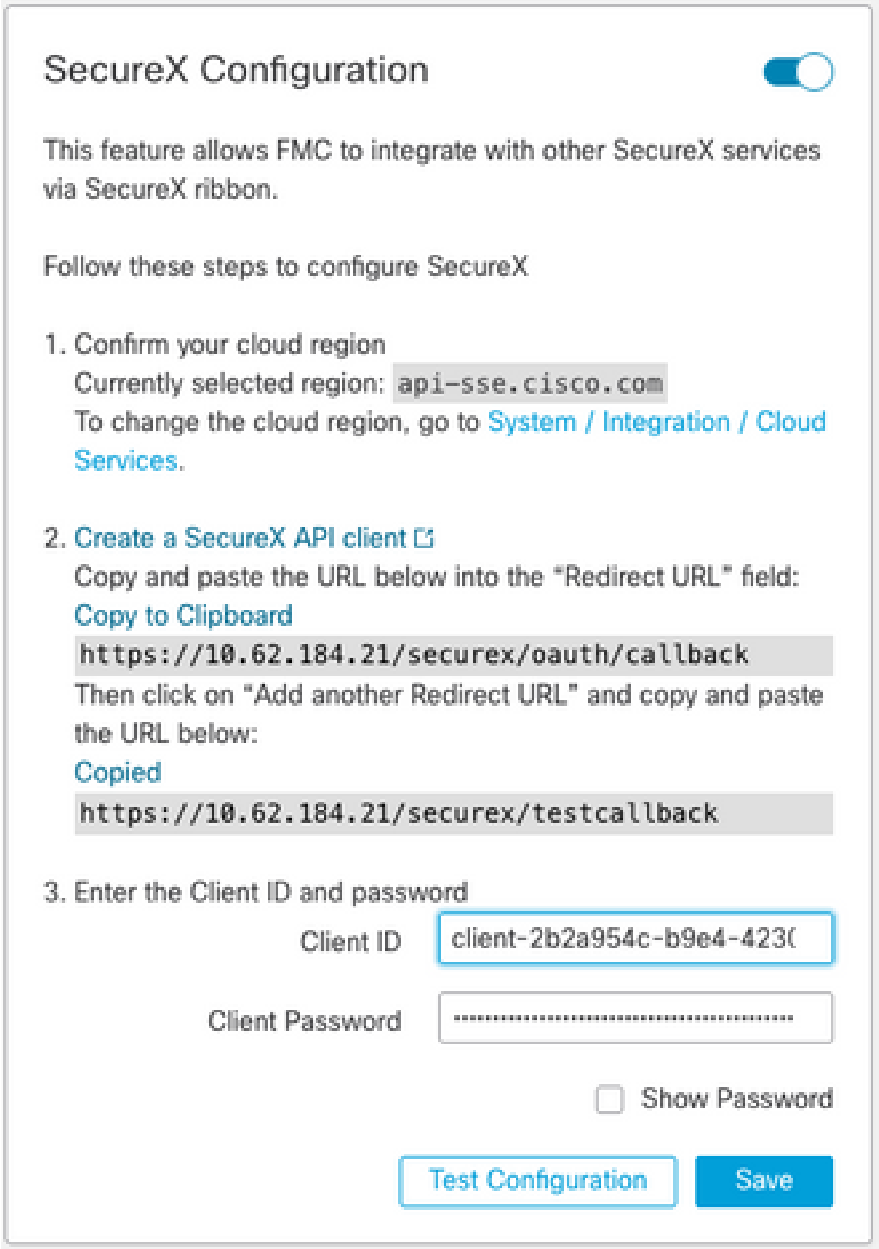
5. Choose **test the configuration**.

6. Log in to SecureX to authorize the API Client.

7. Save the changes and refresh the browser in order to see the ribbon displayed at the bottom.

8. Expand the Ribbon and choose **Get SecureX**. Enter the SecureX credentials if prompted.

9. The SecureX ribbon is now fully functional for your FMC user.



SecureX Configuration

This feature allows FMC to integrate with other SecureX services via SecureX ribbon.

Follow these steps to configure SecureX

1. Confirm your cloud region
   Currently selected region: `api-sse.cisco.com`
   To change the cloud region, go to System / Integration / Cloud Services.

2. Create a SecureX API client
   Copy and paste the URL below into the "Redirect URL" field:
   Copy to Clipboard
   `https://10.62.184.21/securex/oauth/callback`
   Then click on "Add another Redirect URL" and copy and paste the URL below:
   Copied
   `https://10.62.184.21/securex/testcallback`

3. Enter the Client ID and password
   Client ID: client-2b2a954c-b9e4-423(
   Client Password: ••

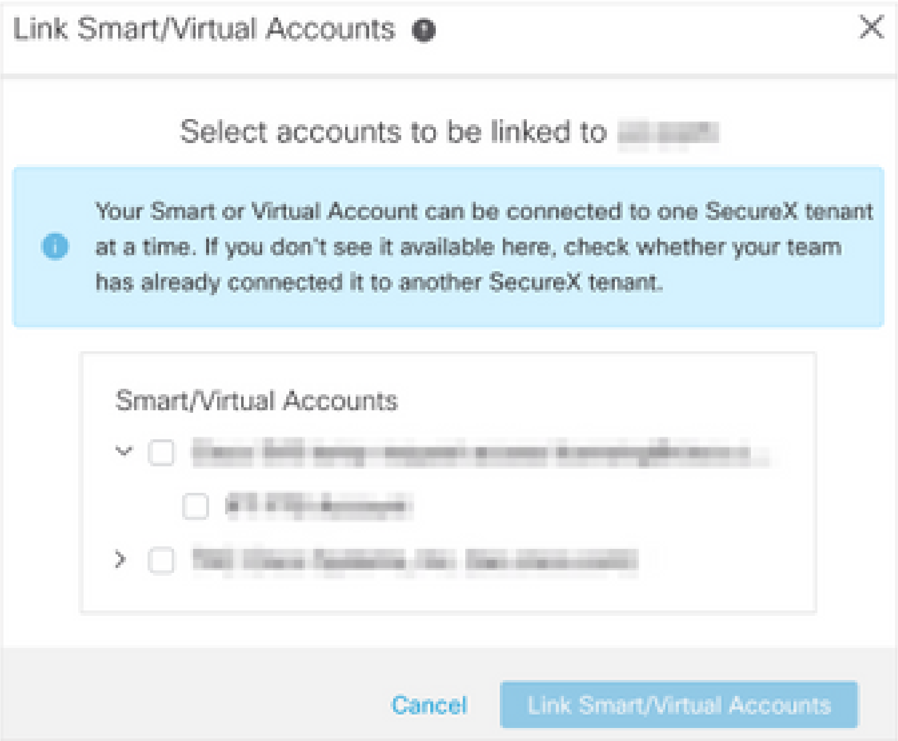
□ Show Password

5YVPsGdzrkX8q8q0yYl-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

> **Note**: If any other FMC user requires access to the ribbon, that user needs to log in to the ribbon with SecureX credentials.

Send Connection Events to SecureX

1. In the FMC, navigate to **System > Integration > Cloud Services** and ensure the **Cisco Cloud Event Configuration** sends Intrusion, File and Malware events as explained in the **Turn on Cloud Services** section.
2. Ensure the FMC is registered with a Smart License as explained in the **Register the Smart Licenses** section.
3. Take a note of the **Assigned virtual Account** name as displayed in FMC under **System > Licenses > Smart Licenses**.
4. Register the FMC into SecureX: In SecureX, navigate to **Administration > Devices**.Choose **Manage Devices**.Ensure that pop-up windows are allowed in the browser.Log in to Security Services Exchange (SSE).Navigate to **Tools menu > Link Smart/Virtual Accounts**.Choose **Link more accounts**.Select the virtual account assigned to the FMC (step 3).Choose **Link Smart/Virtual Accounts.**



Link Smart/Virtual Accounts

Select accounts to be linked to [redacted]

Your Smart or Virtual Account can be connected to one SecureX tenant at a time. If you don't see it available here, check whether your team has already connected it to another SecureX tenant.

Smart/Virtual Accounts

- □ [redacted]
  - □ [redacted]
- □ [redacted]

- Ensure that the FMC device is listed in the Devices.
- Navigate to the **Cloud Services** tab, turn on **Cisco SecureX threat response** and **Eventing** features.
- Choose the **Additional service settings** (gear icon) next to the Eventing feature.
- In the General tab, choose **Share event data with Talos**.
- In the Auto-Promote Events tab, in the section By Event Type choose all available event types and **Save**.

5. In the main SecureX portal, navigate to **Integration Modules > Firepower** and add the Firepower integration module.

6. Create a new dashboard.

7. Add the Firepower related tiles.

Integrate Secure Endpoint (AMP for Endpoints)

In order to enable Secure Endpoint (AMP for Endpoints) integration with your Firepower deployment, follow these steps:

1. Navigate to **AMP > AMP Management**.
2. Choose **Add AMP Cloud Connection**.
3. Choose the cloud and **Register**.

   Note: The status **Enabled** means that the connection to the cloud is established.

Integrate Secure Malware Analytics (Threat Grid)

By default, the Firepower Management Center can connect to the public Cisco Threat Grid cloud for file submission and report retrieval. It is not possible to delete this connection. Nevertheless, it is recommended to choose the closest to your deployment cloud:

1. Navigate to **AMP > Dynamic Analysis Connections**.
2. Click **Edit** (pencil icon) in the Action section.
3. Choose the correct cloud name.
4. To associate the Threat Grid account for detailed reporting and advanced sandbox functionalities, click the **Associate** icon.

For more information, see Firepower Management Center Configuration Guide, Version 7.0 - Enabling Access to Dynamic Analysis Results in the Public Cloud.

For on-premise Thread Grid appliance integration, see Firepower Management Center Configuration Guide, Version 7.0 - Dynamic Analysis On-Premises Appliance (Cisco Threat Grid) .