

FMC 6.6.1+ - Tipps für Vor- und nach einem Upgrade

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Wichtigste Schritte vor dem FMC-Upgrade](#)

[Wählen Sie die FMC-Zielsoftware-Version aus](#)

[Überprüfen des aktuellen FMC-Modells und der aktuellen Softwareversion](#)

[Planung des Upgrade-Pfades](#)

[Upgrade-Pakete hochladen](#)

[Erstellen der FMC-Sicherung](#)

[NTP-Synchronisierung überprüfen](#)

[Überprüfen des Festplattenspeichers](#)

[Bereitstellen aller ausstehenden Richtlinienänderungen](#)

[Führen Sie FirePOWER-Software-Bereitschaftsprüfungen durch.](#)

[Wichtigste Maßnahmen nach dem FMC-Upgrade](#)

[Bereitstellen aller ausstehenden Richtlinienänderungen](#)

[Überprüfen Sie, ob die aktuelle Schwachstellen- und Fingerabdruckdatenbank installiert ist.](#)

[Überprüfen der aktuellen Version von Snort Rule und Lightweight Security Package](#)

[Überprüfen der aktuellen Version des Standortaktualisierungsvorgangs](#)

[Automatisieren der Aktualisierung der URL-Filterung-Datenbank mit geplanter Aufgabe](#)

[Konfigurieren Sie regelmäßige Sicherungen.](#)

[Stellen Sie sicher, dass die Smart License registriert ist.](#)

[Überprüfen der Konfiguration der Variablensätze](#)

[Überprüfen der Cloud Services Enablement](#)

[URL-Filterung](#)

[AMP für Netzwerke](#)

[Cisco Cloud-Region](#)

[Konfiguration von Cisco Cloud-Ereignissen](#)

[Aktivieren der SecureX-Integration](#)

[Integration der SecureX-Multifunktionsleiste](#)

[Verbindungsereignisse an SecureX senden](#)

[Integration von sicheren Endgeräten \(AMP für Endgeräte\)](#)

[Integration sicherer Malware-Analysen \(Threat Grid\)](#)

Einleitung

Dieses Dokument beschreibt die Best Practices für die Überprüfung und Konfiguration, die vor und nach dem Upgrade von Cisco Secure Firewall Management Center (FMC) auf Version 6.6.1+

durchgeführt werden müssen.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Hardware: Cisco FMC 1000
- Software: Version 7.0.0 (Build 94)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Wichtigste Schritte vor dem FMC-Upgrade

Wählen Sie die FMC-Zielsoftware-Version aus

Lesen Sie die [Versionshinweise](#) für [Firepower](#) für die Zielversion, und machen Sie sich mit folgenden Themen vertraut:

- Kompatibilität
- Funktionen und Merkmale
- Behebte Probleme
- Bekannte Probleme

Überprüfen des aktuellen FMC-Modells und der aktuellen Softwareversion

Überprüfen Sie das aktuelle FMC-Modell und die aktuelle Softwareversion:

1. Navigieren Sie zu **Hilfe > Info**.
2. Überprüfen Sie das **Modell** und die **Softwareversion**.

The screenshot shows the Cisco FMC 'About' page. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a search icon. The user is logged in as 'admin'. The main content area displays system details:

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 (build 174)
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

A help menu is open, listing options such as 'Page-level Help', 'How-Tos', 'Documentation on Cisco.com', 'What's New in This Release', 'Software Download', 'Secure Firewall YouTube', 'Secure Firewall on Cisco.com', 'Firepower Migration Tool', 'Partner Ecosystem', 'Ask a Question', 'TAC Support Cases', and 'About'.

Planung des Upgrade-Pfades

Je nach aktueller und angestrebter FMC-Softwareversion ist möglicherweise ein vorläufiges Upgrade erforderlich. Lesen Sie im [Cisco FirePOWER Management Center Upgrade Guide](#) den **Upgrade Path**: Abschnitt **FirePOWER Management Center** und Planung des Upgrade-Pfades.

Upgrade-Pakete hochladen

Gehen Sie wie folgt vor, um das Upgrade-Paket auf das Gerät hochzuladen:

1. Laden Sie das Upgrade-Paket von der [Software Download](#)-Seite herunter.
2. Navigieren Sie im FMC zu **System > Updates**.
3. Wählen Sie das **Upload Update** aus.
4. Klicken Sie auf das Optionsfeld **Lokales Softwareaktualisierungspaket hochladen**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie das Paket aus.
6. Klicken Sie auf **Hochladen**.

The screenshot shows the 'Product Updates' page in the FMC. The current software version is 7.0.0. The 'Updates' dialog box is open, showing the following options:

- Action:**
 - Upload local software update package
 - Specify software update source (FTD devices only)
- Package:** Cisco_Firepower_Mgmt_Center_Patch-7.0.0.1-15.sh.REL.tar

Buttons for 'Cancel' and 'Upload' are visible at the bottom of the dialog.

Erstellen der FMC-Sicherung

Die Sicherung ist ein wichtiger Disaster Recovery-Schritt, mit dem die Konfiguration wiederhergestellt werden kann, wenn ein Upgrade katastrophal fehlschlägt.

1. Navigieren Sie zu **System > Tools > Backup/Restore**.
2. Wählen Sie das **FirePOWER Management Backup** aus.

3. Geben Sie im Feld **Name** den Sicherungsnamen ein.
4. Wählen Sie den Speicherstandort und die Informationen aus, die in die Sicherung eingeschlossen werden sollen.
5. Klicken Sie auf **Sicherung starten**.
6. Überwachen Sie **unter Notification > Tasks** den Fortschritt der Erstellung von Backups.

Tipp: Es wird dringend empfohlen, eine Sicherung an einem sicheren Remote-Standort durchzuführen und den Erfolg der Übertragung zu überprüfen. Der Remote-Speicher kann von der Seite "Backup-Management" konfiguriert werden.

The screenshot shows the Cisco FMC Firepower Management Backup interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', 'Intelligence', 'Deploy', and a search icon. The user is logged in as 'admin'. A 'Remote Storage' button is highlighted in the top right. Below the navigation, there are tabs for 'Backup Management' and 'Backup Profiles'. The main content area is titled 'Create Backup' and contains the following fields and options:

- Name:** FMC_Backup
- Storage Location:** /var/sf/backup/
- Back Up Configuration:**
- Back Up Events:**
- Back Up Threat Intelligence Director:**
- Email when complete:**
- Email Address:** (empty text field)
- Copy when complete:**

At the bottom of the form are three buttons: 'Cancel', 'Save As New', and 'Start Backup'.

Weitere Informationen finden Sie unter:

- [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Kapitel: Sichern und Wiederherstellen](#)
- [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Remote Storage Management](#)

NTP-Synchronisierung überprüfen

Für ein erfolgreiches FMC-Upgrade ist eine NTP-Synchronisierung erforderlich. Gehen Sie wie folgt vor, um die NTP-Synchronisierung zu überprüfen:

1. Navigieren Sie zu **System > Configuration > Time**.
2. Überprüfen Sie den **NTP-Status**.

Anmerkung: Status: "Wird verwendet" gibt an, dass die Appliance mit dem NTP-Server synchronisiert ist.

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)

Weitere Informationen finden Sie unter [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Zeit- und Uhrzeitsynchronisierung](#).

Überprüfen des Festplattenspeichers

Abhängig vom FMC-Modell und der Zielversion, stellen Sie sicher, dass genügend freier Speicherplatz verfügbar ist, andernfalls schlägt das Upgrade fehl. Gehen Sie wie folgt vor, um den verfügbaren FMC-Festplattenspeicher zu überprüfen:

1. Navigieren Sie zu **System > Health > Monitor (System > Zustand > Monitor)**.
2. Wählen Sie das FMC aus.
3. Erweitern Sie das Menü, und suchen Sie nach **Datenträgerverwendung**.
4. Die Speicherplatzanforderungen finden Sie unter [Zeittests und Speicherplatzanforderungen](#).

The screenshot shows the Cisco FMC Monitor interface. The 'Health Status' section indicates a 'Warning' status for the selected device. The primary issue is 'Disk Usage', which is using 44% of the available 3.7G space (1.5G used, 2.0G available). A detailed table for 'Local Disk Partition Status' is provided below:

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

Other health items include 'FMC Access Configuration changes on device', which does not apply to this platform.

Bereitstellen aller ausstehenden Richtlinienänderungen

Vor der Update- oder Patch-Installation müssen Änderungen in den Sensoren bereitgestellt werden. Gehen Sie wie folgt vor, um sicherzustellen, dass alle ausstehenden Änderungen bereitgestellt werden:

1. Navigieren Sie zu **Bereitstellen > Bereitstellung**.
2. Wählen Sie alle Geräte in der Liste aus, und **stellen Sie bereit**.

Vorsicht: Die Spalte "Inspect Interruption" gibt eine Unterbrechung des Datenverkehrs an.

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

Führen Sie FirePOWER-Software-Bereitschaftsprüfungen durch.

Bereitschafts-Überprüfungen prüfen, ob eine FirePOWER-Appliance auf ein Software-Upgrade vorbereitet ist.

Gehen Sie wie folgt vor, um die Überprüfung der Softwarebereitschaft durchzuführen:

1. Navigieren Sie zu **System > Updates**.
2. Wählen Sie neben der Zielversion das Symbol **Install (Installieren)** aus.
3. Wählen Sie das FMC aus, und klicken Sie auf **Check Readiness**.
4. Klicken Sie im Pop-up-Fenster auf **OK**.
5. Überwachen Sie den Bereitschafts-Check-Prozess über **Benachrichtigungen > Aufgaben**.

Weitere Informationen finden Sie im [Cisco FirePOWER Management Center Upgrade Guide - FirePOWER Software Readiness Checks](#).

Wichtigste Maßnahmen nach dem FMC-Upgrade

Bereitstellen aller ausstehenden Richtlinienänderungen

Unmittelbar nach jeder Update- oder Patch-Installation müssen Änderungen in den Sensoren implementiert werden. Gehen Sie wie folgt vor, um sicherzustellen, dass alle ausstehenden Änderungen bereitgestellt werden:

1. Navigieren Sie zu **Bereitstellen > Bereitstellung**.
2. Wählen Sie alle Geräte in der Liste aus, und klicken Sie auf **Bereitstellen**.

Vorsicht: Die Spalte "Inspect Interruption" gibt eine Unterbrechung des Datenverkehrs an.

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

Überprüfen Sie, ob die aktuelle Schwachstellen- und Fingerabdruckdatenbank installiert ist.

Gehen Sie wie folgt vor, um die aktuelle Fingerabdruck-Version (VDB) zu überprüfen:

1. Navigieren Sie zu **Hilfe > Info**.
2. Überprüfen Sie die **VDB-Version**.

Um die VDB-Updates direkt von cisco.com herunterladen zu können, ist eine Erreichbarkeit vom FMC auf cisco.com erforderlich.

1. Navigieren Sie zu **System > Updates > Produktaktualisierungen**.
2. Wählen Sie **Updates herunterladen aus**.
3. Installieren Sie die neueste verfügbare Version.
4. Sie müssen die Sensoren später erneut bereitstellen.

Anmerkung: Wenn das FMC keinen Internetzugang hat, kann das VDB-Paket direkt von software.cisco.com heruntergeladen werden.

Es wird empfohlen, Tasks zu planen, um automatische VDB-Paketdownloads und -Installationen durchzuführen.

Als bewährtes Verfahren sollten Sie täglich nach VDB-Updates suchen und diese am Wochenende auf dem FMC installieren.

Gehen Sie wie folgt vor, um die VDB täglich von www.cisco.com zu überprüfen:

1. Navigieren Sie zu **System > Tools > Scheduling**.
2. Klicken Sie auf **Task hinzufügen**.
3. Wählen Sie in der Dropdown-Liste **Job Type (Auftragstyp)** die Option **Letzte Aktualisierung herunterladen**.
4. Zum **Ausführen der Task 'Zeitplan'** klicken Sie auf das Optionsfeld **Recurring (Wiederholt)**..
5. Wiederholen Sie die Aufgabe jeden Tag, und führen Sie sie um 03:00 Uhr oder außerhalb der Geschäftszeiten aus.
6. Für **Aktualisierungselemente** aktivieren Sie das Kontrollkästchen **Schwachstellendatenbank**..

New Task

Job Type

Schedule task to run Once Recurring

Start On Europe/Warsaw

Repeat Every Hours Days Weeks Months

Run At

Job Name

Update Items Software Vulnerability Database

Comment

Email Status To

Um die neueste VDB im FMC zu installieren, legen Sie die periodische Aufgabe wöchentlich fest:

1. Navigieren Sie zu **System > Tools > Scheduling**.
2. Klicken Sie auf **Task hinzufügen**.
3. Wählen Sie in der Dropdown-Liste **Job Type (Auftragstyp)** die Option **Letzte Aktualisierung installieren aus**.
4. Wenn Sie **die Aufgabe planen möchten**, klicken Sie auf das Optionsfeld **Wiederholt**.
5. Wiederholen Sie die Aufgabe alle 1 Woche, und führen Sie sie um 05:00 Uhr oder außerhalb der Geschäftszeiten aus.
6. Für **Aktualisierungselemente** aktivieren Sie das Kontrollkästchen **Schwachstellendatenbank**.

New Task

Job Type

Schedule task to run Once Recurring

Start On Europe/Warsaw

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Update Items Software Vulnerability Database

Device

Comment

Email Status To

Weitere Informationen finden Sie unter [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Update the Vulnerability Database \(VDB\)](#)

Überprüfen der aktuellen Version von Snort Rule und Lightweight Security Package

Gehen Sie wie folgt vor, um die aktuellen Versionen von Snort Rule (SRU), Lightweight Security Package (LSP) und Geolocation zu überprüfen:

1. Navigieren Sie zu **Hilfe > Info**.
2. Überprüfen Sie die **Regelaktualisierungsversion** und die **LSP-Version**.

Um die SRU und den LSP direkt von www.cisco.com herunterzuladen, ist eine Erreichbarkeit vom FMC auf www.cisco.com erforderlich.

1. Navigieren Sie zu **System > Updates > Regelaktualisierungen**.
2. Wählen Sie auf der Registerkarte **Einmaliges Aktualisieren von Regeln/Importieren von Regeln** die Option **Neue Regelaktualisierung von der Support-Site herunterladen aus**.
3. Wählen Sie **Importieren aus**.
4. Implementieren Sie die Konfiguration anschließend auf den Sensoren.

Anmerkung: Wenn das FMC keinen Internetzugang hat, können die SRU- und LSP-Pakete direkt von der Website software.cisco.com heruntergeladen werden.

Aktualisierungen von Angriffsregeln sind kumulativ und es wird empfohlen, immer die neuesten Aktualisierungen zu importieren.

Gehen Sie wie folgt vor, um das wöchentliche Herunterladen und Bereitstellen von Snort Rule Updates (SRU/LSP) zu aktivieren:

1. Navigieren Sie zu **System > Updates > Regelaktualisierungen**.
2. Aktivieren Sie auf der Registerkarte **Imports für Regelaktualisierungen (Recurring Rule Update Imports, wiederkehrende Regelaktualisierungen aktivieren)** das Kontrollkästchen **Importieren von Regelaktualisierungen vom Support-Standort** aktivieren.
3. Wählen Sie die Häufigkeit des Imports als wöchentlich aus, wählen Sie einen Tag der Woche und einen späten Nachmittag für den Download und die Bereitstellung der Richtlinien aus.
4. Klicken Sie auf **Speichern**.

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

Cancel Save

Weitere Informationen finden Sie unter [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Update Intrusion Rules](#).

Überprüfen der aktuellen Version des Standortaktualisierungsvorgangs

Gehen Sie wie folgt vor, um die aktuelle Standortversion zu überprüfen:

1. Navigieren Sie zu **Hilfe > Info**.
2. Überprüfen Sie die **Version der Standortaktualisierung**.

Um Geolocation Updates direkt von www.cisco.com herunterzuladen, ist eine Erreichbarkeit vom FMC auf www.cisco.com erforderlich.

1. Navigieren Sie zu **System > Updates > Geolokations-Updates**.
2. Wählen Sie auf der Registerkarte **One-Time Geolocation Update (Aktualisierung für einmalige Standortbestimmung)** die Option **Geolokations-Update von der Support-Site herunterladen und installieren aus**.
3. Klicken Sie auf **Importieren**.

Anmerkung: Wenn das FMC keinen Internetzugang hat, kann das Geolocation Updates-Paket direkt von software.cisco.com heruntergeladen werden.

Führen Sie die folgenden Schritte aus, um die automatischen Standortaktualisierungen zu aktivieren:

1. Navigieren Sie zu **System > Updates > Geolokations-Updates**.
2. Aktivieren Sie im Abschnitt "Aktualisierte Standorteinstellungen" das Kontrollkästchen **Regelmäßige wöchentliche Updates über die Support-Site aktivieren**.

3. Wählen Sie die Importfrequenz als Wochenzeitraum aus, wählen Sie Montag um Mitternacht aus.
4. Klicken Sie auf **Speichern**.

Recurring Geolocation Updates

Enable Recurring Weekly Updates from the Support Site

Update Start Time Europe/Warsaw

Weitere Informationen finden Sie unter [Firepower Management Center Configuration Guide, Version 7.0 - Update the Geolocation Database \(GeoDB\)](#).

Automatisieren der Aktualisierung der URL-Filterung-Datenbank mit geplanter Aufgabe

Um sicherzustellen, dass die Bedrohungsdaten für die URL-Filterung aktuell sind, muss das System Datenaktualisierungen von der Cisco Collective Security Intelligence (CSI) Cloud beziehen. Führen Sie die folgenden Schritte aus, um diesen Prozess zu automatisieren:

1. Navigieren Sie zu **System > Tools > Scheduling**.
2. Klicken Sie auf **Task hinzufügen**.
3. Wählen Sie in der Dropdown-Liste **Job Type** (Jobtyp) die Option **URL-Filterdatenbank aktualisieren aus**.
4. Um **die Aufgabe Planen auszuführen**, klicken Sie auf das Optionsfeld **Wiederholt**.
5. Wiederholen Sie die Aufgabe jede Woche, und führen Sie sie sonntags oder außerhalb der Geschäftszeiten um 20:00 Uhr aus.
6. Klicken Sie auf **Speichern**.

New Task

Job Type

Schedule task to run Once Recurring

Start On Europe/Warsaw

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Comment

Email Status To

Weitere Informationen finden Sie unter [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Automatisieren von URL-Filterungsaktualisierungen mithilfe eines geplanten Tasks](#).

Konfigurieren Sie regelmäßige Sicherungen.

Im Rahmen des Disaster Recovery-Plans wird empfohlen, regelmäßige Backups durchzuführen.

1. Stellen Sie sicher, dass Sie sich in der **globalen Domäne befinden**.
2. Erstellen Sie das FMC-Sicherungsprofil. Weitere Informationen finden Sie im Abschnitt **Erstellen der FMC-Sicherung**.
3. Navigieren Sie zu **System > Tools > Scheduling**.
4. Klicken Sie auf **Task hinzufügen**.
5. Wählen Sie aus der Dropdown-Liste **Auftragstyp** die Option **Backup aus**.
6. Um **die Aufgabe Planen auszuführen**, klicken Sie auf das Optionsfeld **Wiederholt**.
Die Sicherungshäufigkeit muss an die Anforderungen des Unternehmens angepasst werden. Es wird empfohlen, Backups während eines Wartungsfensters oder zu anderen Zeiten geringer Nutzung zu erstellen.
7. Klicken Sie als **Sicherungsart** auf das Optionsfeld **Management Center**.
8. Wählen Sie aus der Dropdown-Liste **Backup-Profil** das Sicherungsprofil aus.
9. Klicken Sie auf **Speichern**.

New Task

Job Type

Schedule task to run Once Recurring

Start On UTC

Repeat Every Hours Days Weeks Months

Run At

Repeat On Sunday Monday Tuesday Wednesday Thursday Friday Saturday

Job Name

Backup Type Management Center Device

Backup Profile

Comment

Email Status To

Weitere Informationen finden Sie im [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Kapitel: Sichern und Wiederherstellen](#).

Stellen Sie sicher, dass die Smart License registriert ist.

Gehen Sie wie folgt vor, um das Cisco Firewall Management Center beim Cisco Smart Software Manager zu registrieren:

1. Navigieren Sie in <https://software.cisco.com> zu **Smart Software Manager > Lizenzen verwalten**.
2. Navigieren Sie zu **Bestand > Allgemein**, und erstellen Sie ein **neues Token**.
3. Navigieren Sie in der FMC-Benutzeroberfläche zu **System > Licenses > Smart Licenses (System > Lizenzen > Smart Licenses)**.
4. Klicken Sie auf **Registrieren**.
5. Fügen Sie das im Cisco Smart Software-Lizenzierungsportal erstellte Token ein.
6. Stellen Sie sicher, dass **das Cisco Success Network aktiviert ist**.
7. Klicken Sie auf **Änderungen übernehmen**.
8. Überprüfen Sie den Smart-Lizenzstatus.

Smart Licensing Product Registration ?

Product Instance Registration Token:

MGI0ZGJhNTEtOTIxYy00ZGM2LWJjMTctNWE1ZTY5YWUxZGExLTE2NjQwMTUz%0AM
 DQ0OTZ8bTQxTWJDbmJJWlVld3hQMGS4bytHdU4wVzNvRWRZM1pjbk.J4Nkcr%0A!

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.

Weitere Informationen finden Sie unter [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Smart Licenses registrieren](#).

Überprüfen der Konfiguration der Variablensätze

Stellen Sie sicher, dass die Variable HOME_NET nur die internen Netzwerke/Subnetze in der Organisation enthält. Eine unangemessene Definition von Variablen beeinträchtigt die Leistung der Firewall.

1. Navigieren Sie zu **Objekte > Variablensatz**.
2. Bearbeiten Sie den von der Intrusion Policy verwendeten Variablensatz. Es kann eine Variable pro Intrusion Policy mit unterschiedlichen Einstellungen festgelegt werden.
3. Passen Sie die Variablen an Ihre Umgebung an, und klicken Sie auf **Speichern**.

Andere relevante Variablen sind DNS_SERVERS ODER HTTP_SERVER.

Weitere Informationen finden Sie unter [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Variable Sets](#).

Überprüfen der Cloud Services Enablement

Um die Vorteile der verschiedenen Cloud-Services nutzen zu können, Navigieren Sie zu **System > Integration > Cloud-Services**.

URL-Filterung

1. Aktivieren Sie URL-Filterung, und aktivieren Sie die Option Cisco Cloud-Abfrage für unbekannte URLs abrufen.
Ein häufigeres Ablauf von Cache-URLs erfordert mehr Anfragen an die Cloud, was zu einer Verlangsamung der Web-Last führt.
2. **Speichern Sie die Änderungen.**

Tipp: Lassen Sie bei Ablauf des Cache-URL die Standardeinstellung **Never (Nie)**. Wenn eine strengere Web-Reklassifizierung erforderlich ist, kann diese Einstellung entsprechend geändert werden.

AMP für Netzwerke

1. Stellen Sie sicher, dass beide Einstellungen aktiviert sind: **Automatische Updates zur lokalen Malware-Erkennung** und **Freigabe von URIs von Malware-Ereignissen an Cisco**.
2. Deaktivieren Sie in FMC 6.6.X die Verwendung des Legacy-Ports 32137 für AMP für Netzwerke, sodass der verwendete TCP-Port 443 ist.
3. **Speichern Sie die Änderungen.**

Anmerkung: Diese Einstellung ist in FMC 7.0+ nicht mehr verfügbar, und der Port ist immer 443.

Cisco Cloud-Region

1. Die Cloud-Region muss mit der SecureX-Organisationsregion übereinstimmen. Wenn die SecureX-Organisation nicht erstellt wird, wählen Sie die Region aus, die näher an der FMC-Installation liegt: APJ-Region, EU-Region oder US-Region.
2. **Speichern Sie die Änderungen.**

Konfiguration von Cisco Cloud-Ereignissen

Für FMC 6.6.x

1. Stellen Sie alle drei Optionen sicher: **Verbindungsereignisse mit hoher Priorität an die Cloud senden**, **Datei- und Malware-Ereignisse an die Cloud senden** und **Angriffsversuche an die Cloud senden** werden ausgewählt.
2. **Speichern Sie die Änderungen.**

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.

Save

Für FMC 7.0+

1. Stellen Sie sicher, dass beide Optionen ausgewählt sind: **Senden von Angriffsversuchen an die Cloud** und **Senden von Datei- und Malware-Ereignissen an die Cloud**.
2. Wählen Sie für die Art der Verbindungsereignisse **Alle** aus, wenn die Sicherheitsanalytik- und Protokollierungslösung verwendet wird. Wählen Sie für SecureX nur **Security Events** aus.
3. **Speichern Sie die Änderungen.**

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

Save

Aktivieren der SecureX-Integration

Die SecureX-Integration bietet sofortigen Einblick in die Bedrohungslandschaft Ihrer Cisco Security-Produkte. Um SecureX anzuschließen und das Band zu aktivieren, gehen Sie wie folgt vor:

Integration der SecureX-Multifunktionsleiste

Anmerkung: Diese Option ist für FMC Version 7.0+ verfügbar.

1. Melden Sie sich bei SecureX an, und erstellen Sie einen API-Client: Geben Sie im Feld **Client Name (Client-Name)** einen beschreibenden Namen für das FMC ein. Beispiel: FMC 7.0 API-Client. Klicken Sie auf die Registerkarte **OAuth Code Clients**. Wählen Sie in der Dropdown-Liste **Client Preset (Client-Voreinstellung)** die Option **Multifunktionsleiste** aus. Sie

wählt die Bereiche aus: Casebook, Enrich:read, Global Intel:read, Inspect:read, Notification, Orbital, Private Intel, Profile, Response, Telemetrie:write. Fügen Sie die beiden im FMC dargestellten Umleitungs-URLs hinzu:

URL für Umleitung: <FMC_URL>/securex/auth/callback

URL für zweite Umleitung: <FMC_URL>/securex/testcallback

1. Wählen Sie in der Dropdown-Liste **Verfügbarkeit** die Option **Organisation aus**. Klicken Sie auf **Neuen Client hinzufügen**.

Add New Client with 10 scopes ✕

Client Name*

Client Preset
 ✕ ▾

API Clients OAuth Code Clients

Scopes* Select All

🔍

<input checked="" type="checkbox"/>	Response	List and execute response actions using configured modules
<input type="checkbox"/>	SSE	SSE Integration. Manage your Devices.
<input checked="" type="checkbox"/>	Telemetry:write	collect application data for analytics - Write Only
<input type="checkbox"/>	Users	Manage users of your organisation
<input type="checkbox"/>	Webhook	Manage your Webhooks

Redirect URL*

Redirect URL* Delete

Add another Redirect URL

Availability*
 ▾

Description

2. Navigieren Sie vom FMC zu **System > SecureX**.

3. Aktivieren Sie den Umschalter in der oberen rechten Ecke, und überprüfen Sie, ob die angezeigte Region mit der SecureX-Organisation übereinstimmt.

4. Kopieren Sie die **Client-ID** und das **Client-Kennwort** und fügen Sie sie in das FMC ein.

5. Wählen Sie **Testen der Konfiguration** aus.

6. Melden Sie sich bei SecureX an, um den API-Client zu autorisieren.

7. Speichern Sie die Änderungen, und aktualisieren Sie den Browser, damit das Menüband unten angezeigt wird.

8. Erweitern Sie die Multifunktionsleiste, und wählen Sie **Get SecureX aus**. Geben Sie bei Aufforderung die SecureX-Anmeldeinformationen ein.

9. Das SecureX-Band ist jetzt voll funktionsfähig für Ihren FMC-Benutzer.

SecureX Configuration

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

Follow these steps to configure SecureX

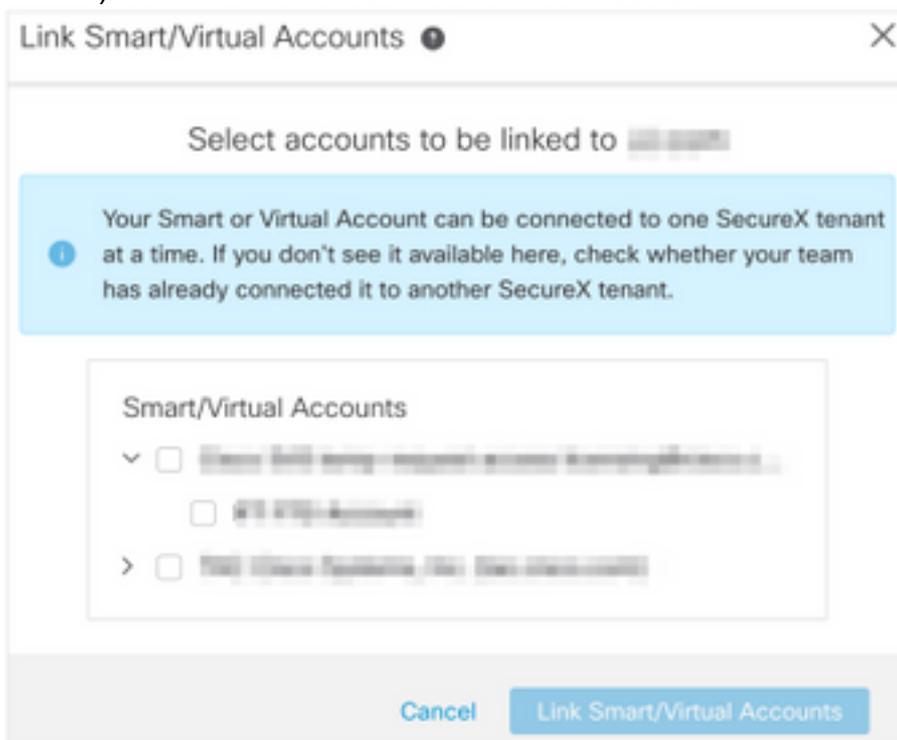
1. Confirm your cloud region
Currently selected region: `api-sse.cisco.com`
To change the cloud region, go to [System / Integration / Cloud Services](#).
2. [Create a SecureX API client](#) 
Copy and paste the URL below into the "Redirect URL" field:
[Copy to Clipboard](#)
`https://10.62.184.21/securex/oauth/callback`
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 Password
 Show Password

5YVPsGdzrkX8q8q0yYI-DitezO6p_17MtH6NATx68fUZ5u9T3qOEq

Anmerkung: Wenn ein anderer FMC-Benutzer Zugriff auf das Band benötigt, muss sich dieser Benutzer mit SecureX-Anmeldeinformationen beim Band anmelden.

Verbindungsereignisse an SecureX senden

1. Navigieren Sie im FMC zu **System > Integration > Cloud Services**, und stellen Sie sicher, dass die **Cisco Cloud Event Configuration** Intrusion, File and Malware Events sendet, wie im Abschnitt **Turn on Cloud Services** erläutert.
2. Stellen Sie sicher, dass das FMC bei einer Smart-Lizenz registriert ist, wie im Abschnitt **"Smart Licenses registrieren"** beschrieben.
3. Notieren Sie sich den Namen des **zugewiesenen virtuellen Kontos**, wie er unter **System > Licenses (System > Lizenzen > Smart Licenses)** im FMC angezeigt wird.
4. Registrieren Sie das FMC in SecureX: Navigieren Sie in SecureX zu **Administration > Devices**. Wählen Sie **Geräte verwalten aus**. Stellen Sie sicher, dass Popup-Fenster im Browser zugelassen sind. Melden Sie sich bei Security Services Exchange (SSE) an. Navigieren Sie zu **Menü Extras > Smart/Virtual Accounts verknüpfen**. Wählen Sie **Weitere Konten verknüpfen aus**. Wählen Sie das dem FMC zugewiesene virtuelle Konto aus (Schritt 3). Wählen Sie **Link Smart/Virtual Accounts**.



- Stellen Sie sicher, dass das FMC-Gerät in den Geräten aufgeführt ist.
 - Navigieren Sie zur Registerkarte **Cloud-Services**, und aktivieren Sie die Funktionen **Cisco SecureX Threat Response** und **Event**.
 - Wählen Sie die **zusätzlichen Serviceeinstellungen** (Zahnrad-Symbol) neben der Eventing-Funktion aus.
 - Wählen Sie auf der Registerkarte Allgemein die Option **Ereignisdaten für Talos freigeben aus**.
 - Wählen Sie auf der Registerkarte Auto-Promote Events (Veranstaltungen automatisch fördern) im Abschnitt By Event Type (Ereignistyp) alle verfügbaren Ereignistypen aus, und **Save (Speichern)**.
5. Navigieren Sie im SecureX-Hauptportal zu **Integration Modules > FirePOWER**, und fügen Sie das FirePOWER-Integrationsmodul hinzu.
 6. Erstellen Sie ein neues Dashboard.
 7. Fügen Sie die FirePOWER-Kacheln hinzu.

Integration von sicheren Endgeräten (AMP für Endgeräte)

Führen Sie die folgenden Schritte aus, um die Integration von Secure Endpoint (AMP für Endgeräte) in Ihre FirePOWER-Bereitstellung zu aktivieren:

1. Navigieren Sie zu **AMP > AMP Management**.
2. Wählen Sie **AMP-Cloud-Verbindung hinzufügen** aus.
3. Wählen Sie die Cloud aus, und **registrieren Sie sich**.

Anmerkung: Der Status **Aktiviert** bedeutet, dass die Verbindung zur Cloud hergestellt wird.

Integrieren Sichere Malware-Analysen (Threat Grid)

Standardmäßig kann das FirePOWER Management Center eine Verbindung zur öffentlichen Cisco Threat Grid-Cloud herstellen, um Dateien zu senden und Berichte abzurufen. Es ist nicht möglich, diese Verbindung zu löschen. Es wird jedoch empfohlen, die Cloud-Umgebung auszuwählen, die Ihrer Bereitstellung am nächsten liegt:

1. Navigieren Sie zu **AMP > Dynamic Analysis Connections**.
2. Klicken Sie im Bereich Aktion auf **Bearbeiten** (Bleistiftsymbol).
3. Wählen Sie den richtigen Cloud-Namen aus.
4. Um dem Threat Grid-Konto detaillierte Berichterstattungs- und erweiterte Sandbox-Funktionen zuzuordnen, klicken Sie auf das **Associate**-Symbol.

Weitere Informationen finden Sie unter [Konfigurationsleitfaden für das FirePOWER Management Center, Version 7.0 - Aktivieren des Zugriffs auf dynamische Analyseergebnisse in der Public Cloud](#).

Informationen zur Integration von Thread Grid-Appliances vor Ort finden Sie im [FirePOWER Management Center Configuration Guide, Version 7.0 - Dynamic Analysis On-Premises Appliance \(Cisco Threat Grid\)](#).