Configure Automatic Update of CA Bundles for FMC and FDM

Contents

Introduction

This document describes the use of the Automatic update of Cisco CA Bundles for Secure Firewall Management Center and Secure Firewall Device Manager.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Cisco Secure Firewall Management Center (formerly known as Firepower Management Center) and Secure Firewall Device Manager (formerly known as Firepower Device Manager).
- Secure Firewall Appliance (formerly known as Firepower) knowledge.

Components Used

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

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600, and virtual) running software version 7.0.5 and above.
- Cisco Secure Firewall Management Center (FMC 1600, 2600,4600, and virtual) running software version 7.1.0-3 and above.
- Cisco Secure Firewall Management Center (FMC 1600, 2600,4600, and virtual) running software version 7.2.4 and above.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000, and virtual) running software version 7.0.5 and above, managed by Secure Firewall Device Manager.

- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000, and virtual) running software version 7.1.0-3 and above, managed by Secure Firewall Device Manager.
- Cisco Secure Firewall (FPR 1000, 2100, 3100, 4100, 9300, ISA3000, and virtual) running software version 7.2.4 and above, managed by Secure Firewall Device Manager.

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.

Background Information

Uses for Cisco CA Bundles

Cisco Secure Firewall (Previously known as Firepower) devices use Local CA bundles that contain certificates to access several Cisco Services (Smart Licensing, Software, VDB, SRU, and Geolocation Updates). The System now automatically queries Cisco for new CA certificates at a daily system-defined time. Previously, you had to upgrade the software to update CA Certificates.

Note: This feature is not supported in Version 7.0.0 to 7.0.4, 7.1.0 to 7.1.0-2, or 7.2.0 to 7.2.3. If you upgrade from a supported version to an unsupported version, the feature is temporarily disabled and the system stops contacting Cisco.

Configure Automatic update for CA Bundles on SFMC and SFDM

Enable Automatic update for CA Bundles

To enable Automatic Update for CA Bundles on Secure Firewall Management Center and Secure Firewall Device Manager:

1. Access SFMC or SFDM over CLI using SSH or Console.
2. Run the **configure cert-update auto-update enable** command on CLI:

<#root>

```
> configure cert-update auto-update enable

Autoupdate is enabled and set for every day at 18:06 UTC
```

3. To test if the CA bundle update is capable to auto-update, run the **configure cert-update test** command:

<#root>

```
> configure cert-update test

Test succeeded, certs can safely be updated or are already up to date.
```

Run the update for CA Bundles Manually

To Manually run the Update for CA Bundles on Secure Firewall Management Center and Secure Firewall Device Manager:

1. Access SFMC or SFDM over CLI using SSH or Console.
2. Run the **configure cert-update run-now** command on CLI:

<#root>

```
> configure cert-update run-now

Certs have been replaced or was already up to date.
```

Verify

Validate the Automatic update for CA Bundles

To validate the configuration for the Automatic Update for CA Bundles on Secure Firewall Management Center and Secure Firewall Device Manager:

1. Access SFMC or SFDM over CLI using SSH or Console.
2. Run the **show cert-update** command on CLI:

<#root>

```
> show cert-update


Autoupdate is enabled and set for every day at 18:06 UTC
CA bundle was last modified 'Wed Jul 19 03:11:31 2023'
```

Troubleshoot

Update Error

Recommended steps:

1. Validate your current DNS configuration.
2. Validate the internet and proxy configuration for the Management Interface.
3. Confirm that you have connectivity with tools.cisco.com using ICMP and curl with the command in expert mode:
   sudo curl -vvk https://tools.cisco.com