Configure Mgmt Access for SSH and HTTPS on FTD via FDM or CLISH

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- FDM Steps
- CLISH Steps

Verify

References

Introduction

This document describes the process to configure and verify the management access-list for SSH and HTTPS on FTD managed locally or remote.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

- Cisco Secure Firewall Threat Defense running version 7.4.1 managed by FDM.

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.

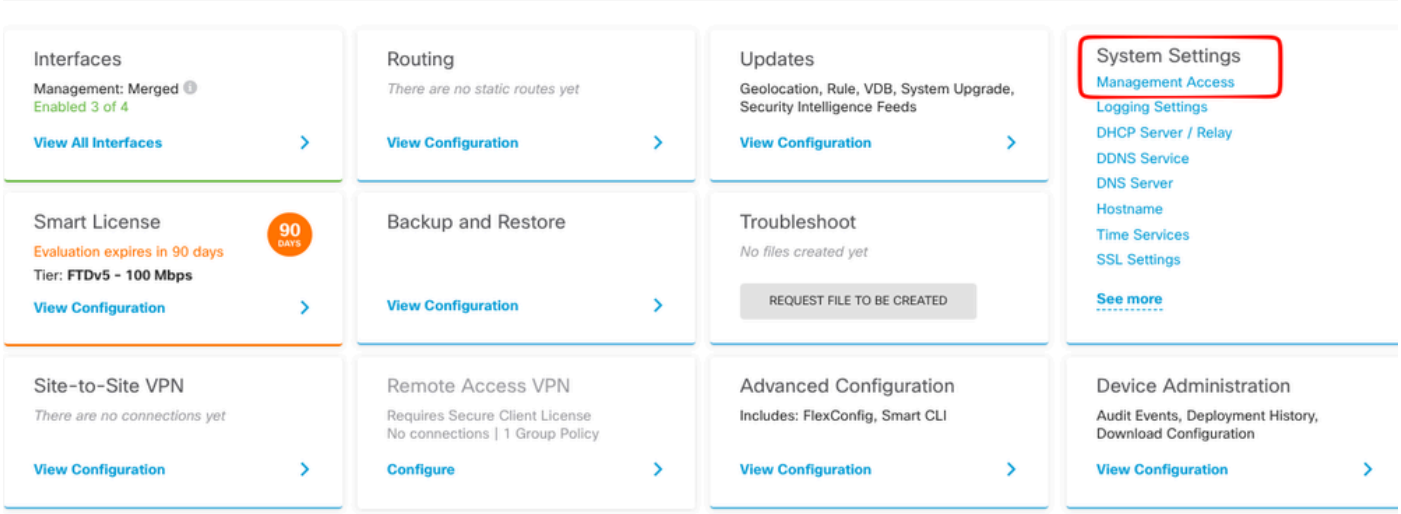
Configure

FTD can be managed locally using FDM or via FMC. The main focus of this document is management access via FDM and CLI. Using CLI, you can make changes for both FDM and FMC.

⚠ **Caution**: Configure SSH or HTTPS access lists one at a time to avoid session lockout. First, update and deploy one protocol, verify access, then proceed with the other.

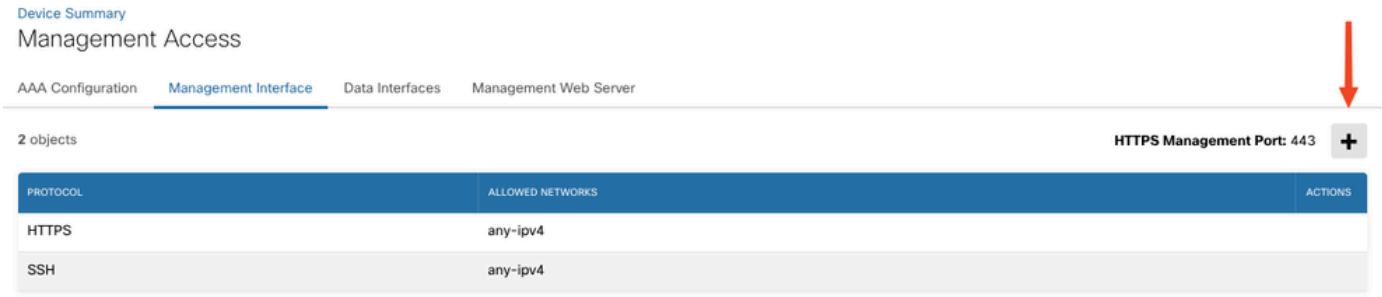
FDM Steps

1. Log in to the Firepower Device Manager (FDM) and navigate to **System Settings** > **Management Access** > **Management Interface**.



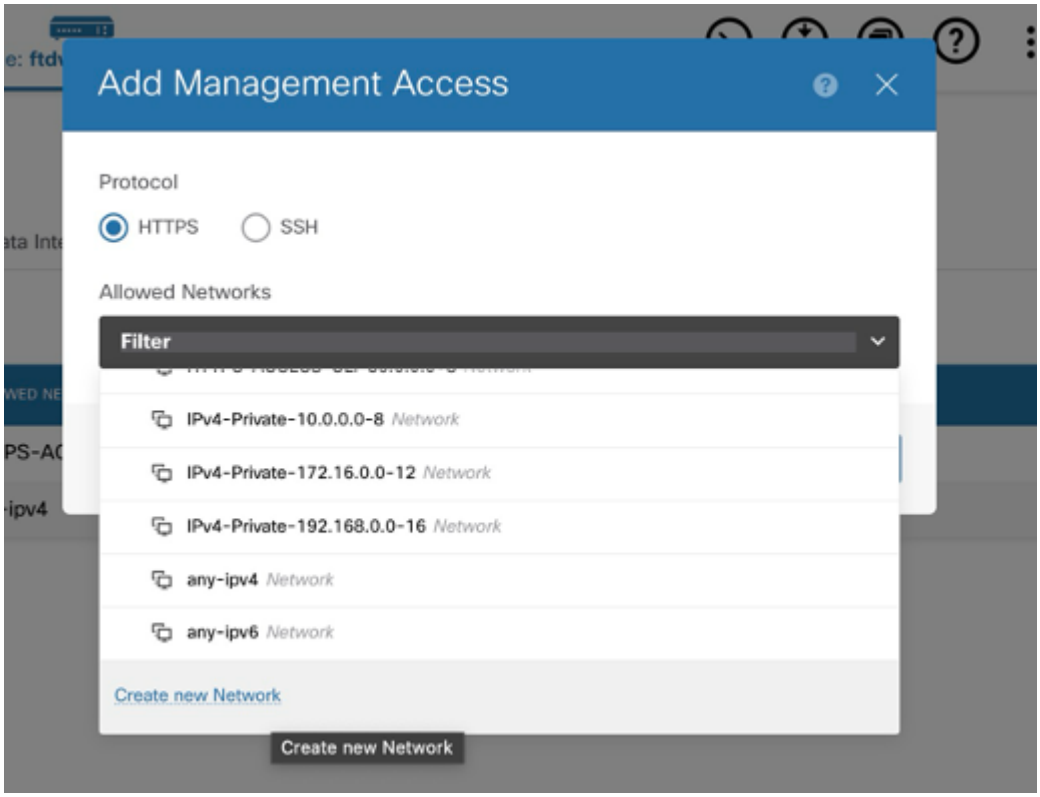
---

2. Click the + icon to open the window for adding the network.



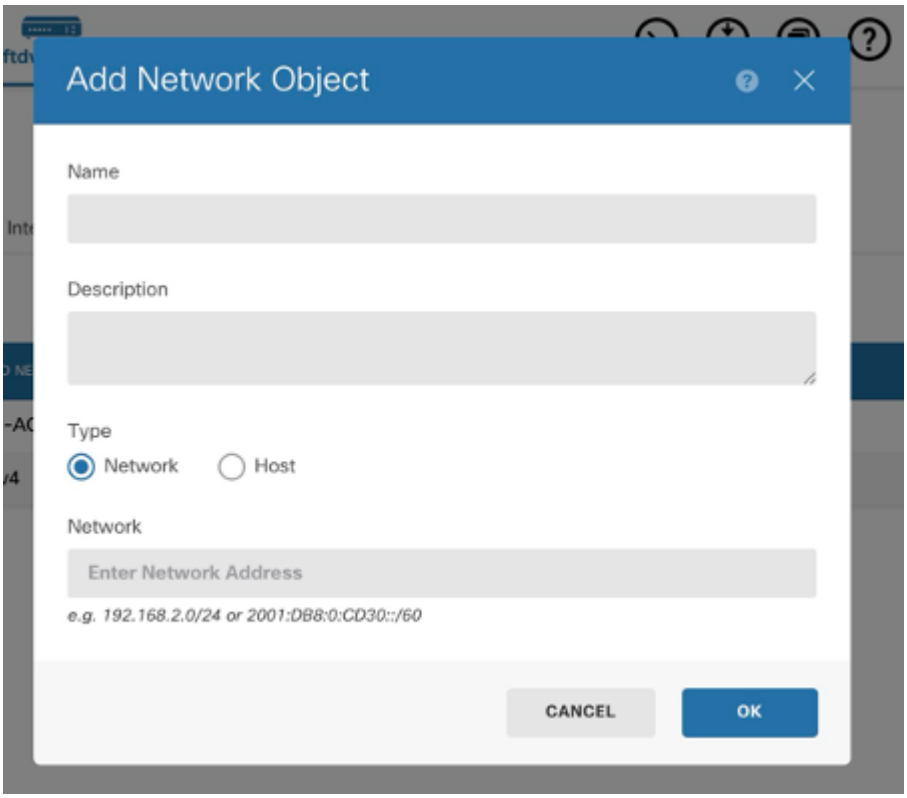
---

3. Add the network object to access SSH or HTTPS. If you must create a new network, select the **Create New Network** option. You can add multiple entries for networks or hosts in the management access section.



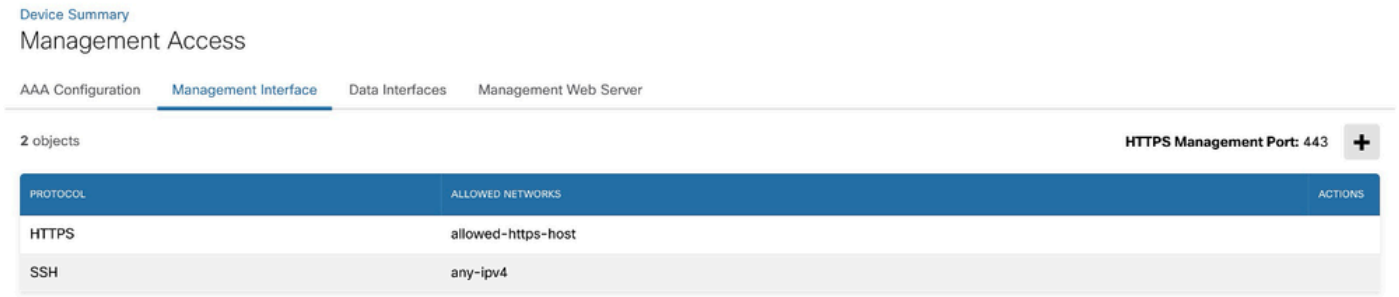
---

4. **Optional**: Select **Create a New Network** option opens up **Add Network Object** window.



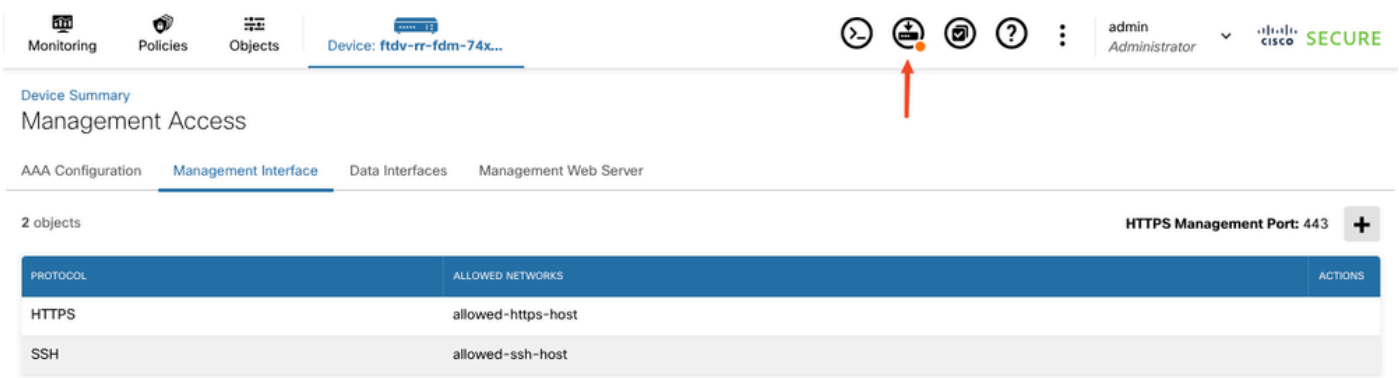
---

5. Verify the changes made and **Deploy**.



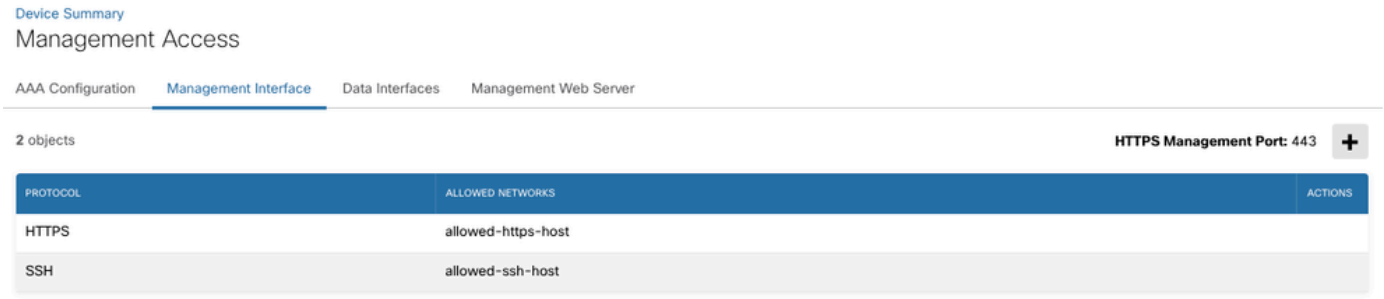
---

6. **Optional**: Once the previous changes for HTTPS are verified, repeat the same for SSH.



---

7. Deploy the changes and verify your access to FTD from the allowed network and host.



CLISH Steps

CLI steps can be used if both FDM or FMC are managed. To configure the device to accept HTTPS or SSH connections from a specified IP address or network, run the **configure https-access-list** or **configure ssh-access-list** command.

- You must include all supported hosts or networks in a single command. Addresses specified in this command overwrite the current contents of the respective access list.
- If the device is a unit in a locally-managed high availability group, your changes overwrite the next time the active unit deploys configuration updates. If this is the active unit, the change propagates to the peer during deployment.

```
> configure https-access-list x.x.x.x/x,y.y.y.y/y

The https access list was changed successfully.

> show https-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:https
ACCEPT     tcp  --  y.y.y.y/y            anywhere             state NEW tcp dpt:https
```

Note: x.x.x.x/x and y.y.y.y/y represents IPv4 address with CIDR notation. To specify all IPv4 hosts, enter 0.0.0.0/0. To specify all IPv6 hosts, specify ::/0.

For SSH connections run **configure ssh-access-list** command.

```
> configure ssh-access-list x.x.x.x/x

The ssh access list was changed successfully.
```

```
> show ssh-access-list
ACCEPT     tcp  --  x.x.x.x/x            anywhere             state NEW tcp dpt:ssh
```



Note: You can run commands **configure disable-https-access** or **configure disable-ssh-access** to disable HTTPS or SSH access respectively. Ensure you are aware of these changes as this can lock you out of the session.

You can also configure multiple entries in a single command with a comma separated for values of ipaddress/CIDR.

Verify

To verify from CLISH you can run commands:

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh

> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
```

The sample output shows the f2b-ssh entry. After 10 consecutive failed SSH attempts, the system automatically adds a f2b-sshd entry to run the **show ssh-access-list** command output.

```
> show ssh-access-list
f2b-sshd   tcp  --  anywhere             anywhere             tcp dpt:ssh
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
Chain f2b-sshd (1 references)
```

Refer to f2b in the references section.

References

- Cisco Secure Firewall Threat Defense Command Reference
- Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager