



Managing TrustSec

This chapter contains the following sections:

- [About Cisco Trustsec, page 1](#)
- [Refreshing TrustSec, page 1](#)

About Cisco Trustsec

Cisco TrustSec provides an access-control solution that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. In the Cisco TrustSec solution, enforcement devices utilize a combination of user attributes and endpoint attributes to make role-based and identity-based access control decisions. The availability and propagation of this information is used to apply security solutions across networks at the access, distribution, and core layers of the network.

In Cisco UCS Director, you can manage Cisco Trustsec on the following Cisco network devices:

- Cisco ASA 5500 Series firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)

Refreshing TrustSec

-
- Step 1** Choose **Physical > Network**.
 - Step 2** On the **Network** page, choose the pod.
 - Step 3** Select the network device to be configured.
The summary of the device is displayed.
 - Step 4** Click **TrustSec Refresh**.
 - Step 5** In the **TrustSec Refresh** screen, complete the following field:

| Name | Description |
|---|---|
| Copy Running configuration to Startup configuration check box field | Check the check box to copy the running configuration to the startup configuration. |

Step 6 Click **Submit**.
