Secure Network Services Using Trustsec

Overview of Cisco TrustSec

Cisco TrustSec technology uses software-defined segmentation to simplify the provisioning of security policies, to accelerate security operations, and to consistently enforce policy anywhere in the network. TrustSec is embedded technology in Cisco switches, routers, wireless, and security devices. It is a secure network architecture that extends security across the network from campus to branch to data center. TrustSec is the foundation for using the Network as an Enforcer and mitigates risk by reducing attack surface through better segmentation, whilst also increasing operational efficiency and making compliance goals easier to achieve.

In Cisco Prime Infrastructure, the TrustSec network service design enables you to choose preferred options for provisioning configurations to TrustSec-capable devices to enable 802.1X and other TrustSec functionality. You can configure wired 802_1x devices by creating TrustSec model-based configuration templates and choosing any one of the following navigation paths:

- **Services > TrustSec**
- **Configuration > Templates > Features & Technologies > Security > TrustSec > Wired 802_1x**

Note For the TrustSec 5.3 platform support list, see the Cisco TrustSec Release 5.3 System Bulletin.

For more details about configuring TrustSec model-based configuration templates, see Create a New Features and Technologies Template Using an Existing Template.

Related Topics

Generate a Trustsec Readiness Assessment Report, on page 1

Generate a Trustsec Readiness Assessment Report

TrustSec Readiness Assessment displays TrustSec-based device details such as TrustSec Feature classification.

The devices are categorized as:

- Classification is the process of assigning a security group tags based on identity or context (dynamically with 802.1x or MAB or web auth or statically mapped to IP, subnet, VLAN or interface). These security group tags are transmitted to the devices using inline tagging or security group tag exchange protocol (SXP).
- Enforcement is the process of enforcing traffic policy based on the security group tags via a secure group ACL (SGACL on switches and routers) or security group firewall (SGFW).
- TrustSec Incapable are devices with no classification, propagation or enforcement capabilities.

To generate a TrustSec Readiness Assessment report, follow these steps:

Step 1 Choose **Services > TrustSec > Readiness Assessment**.

Step 2 Click **TrustSec Readiness** tab. The TrustSec table appears with the following types of devices:

- Classification Devices
- Enforcement Devices
- TrustSec Incapable Devices

Step 3 Click the various device categories to view the details of the selected TrustSec-based device type. Each category displays the number of devices in percentage in a color coded circle. The color codes for each category are:

Classification, Enforcement and TrustSec Incapable Devices:

- Red — Number of TrustSec incapable devices.
- Light Green—Number of classification capable devices
- Dark Green—Number of enforcement capable devices.

Step 4 Choose the appropriate filter from the **Show** drop-down list to filter the devices in each category.

Step 5 Click the Export icon to download the device details as CSV or PDF file.