Controller Security

FIPS, CC, and UCAPL

This section contains the following subsections:

FIPS

Federal Information Processing Standard (FIPS) 140-2 is a security standard used to validate cryptographic modules. The cryptographic modules are produced by the private sector for use by the U.S. government and other regulated industries (such as financial and healthcare institutions) that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information.

Note Cisco TrustSec (CTS) is not supported when the controller is in FIPS mode.

For more information about FIPS, see

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html.

FIPS Self-Tests

A cryptographic module must perform power-up self-tests and conditional self-tests to ensure that it is functional.

Power-up self-tests run automatically after the device powers up. A device goes into FIPS mode only after all self-tests are successfully completed. If any self-test fails, the device logs a system message and moves into an error state. Also, if the power-up self test fails, the device fails to boot.

Using a known-answer test (KAT), a cryptographic algorithm is run on data for which the correct output is already known, and then the calculated output is compared to the previously generated output. If the calculated output does not equal the known answer, the known-answer test fails.

Power-up self-tests include the following:

- Software integrity
- Algorithm tests

Conditional self-tests must be run when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

The device uses a cryptographic algorithm known-answer test (KAT) to test FIPS mode for each FIPS 140-2-approved cryptographic function (encryption, decryption, authentication, and random number generation) implemented on the device. The device applies the algorithm to data for which the correct output is already known. It then compares the calculated output to the previously generated output. If the calculated output does not equal the known answer, the KAT fails.

Conditional self-tests run automatically when an applicable security function or operation is invoked. Unlike the power-up self-tests, conditional self-tests are executed each time their associated function is accessed.

Conditional self-tests include the following:

- Pair-wise consistency test—This test is run when a public or private key-pair is generated.
- Continuous random number generator test—This test is run when a random number is generated.
- Bypass
- Software load

Information About CC

Common Criteria (CC) is a testing standard to verify that a product provides security functions that are claimed by its developer. CC evaluation is against a created protection profile (PP) or security target (ST).

The four security levels in FIPS 140–2 do not map directly to specific CC EALs or CC functional requirements. For more information about CC, see Common Criteria Portal and CC evaluation and validation scheme.

To configure the controller into CC mode of operation, refer the *Admin Guidance Document* published on the Certified Product page of the Common Criteria Portal website.

After providing CC for the controller, the controller series name is listed in the Common Criteria Portal. Click the **Security Documents** tab to view the list of documented available for the controller.

Information About UCAPL

The US Department of Defense (DoD) Unified Capabilities Approved Product List (APL) certification process is the responsibility of the Defense Information Systems Agency (DISA) Unified Capabilities Certification Office (UCCO). Certifications are performed by approved distributed testing centers including the Joint Interoperability Test Command (JITC).

DoD customers can only purchase unified capabilities related equipment, both hardware and software, that has been certified. Certified equipment is listed on the DoD UC APL. UC APL certifications verify the system complies with and is configured consistent with the DISA Field Security Office (FSO) Security Technical Implementation Guides (STIG).

For more information about the UC APL process, see Defense Information System Agency.

Guidelines on UCAPL

- In UCAPL web authentication login, multifactor authentication, which includes client (browser) certificate validation and user authentication, is performed; Certificate validation prior to user authentication is mandatory. Certificate validation is part of DTLS handshake, which is performed only once for a session till its lifetime (default session lifetime is 5 minutes). When a user tries to login again, certificate validation is not performed because the old session is not yet flushed and user authentication is not performed without certificate validation. For more information, see https://tools.ietf.org/html/rfc5246.
- UCAPL certification requires a maximum of three unsuccessful login attempts to SSH. With some SSH clients, fourth attempts are also observed; however, controller does not accept the fourth attempt even if the credentials are correct.

Configuring FIPS (CLI)

Procedure

Step 1 Configure FIPS on the controller by entering this command:

config switchconfig fips-prerequisite {**enable** | **disable** }

Step 2 View the FIPS configuration by entering this command:

show switchconfig

Information similar to the following appears:

```
802.3x Flow Control Mode........................ Disable
FIPS prerequisite features...................... Enabled
WLANCC prerequisite features.................... Enabled
UCAPL prerequisite features..................... Disabled
secret obfuscation.............................. Enabled
```

Configuring CC (CLI)

Before you begin

FIPS must be enabled on the controller.

Procedure

Step 1 Configure FIPS on the controller by entering this command:

config switchconfig wlancc {**enable** | **disable** }

Step 2 View the FIPS configuration by entering this command:

show switchconfig

Information similar to the following appears:

```
802.3x Flow Control Mode......................... Disable
FIPS prerequisite features....................... Enabled
WLANCC prerequisite features..................... Enabled
UCAPL prerequisite features...................... Disabled
secret obfuscation............................... Enabled
```

Configuring UCAPL (CLI)

Before you begin

FIPS and WLAN CC must be enabled on the controller.

Procedure

Step 1 Configure UCAPL on the controller by entering this command:

config switchconfig ucapl {**enable** | **disable** }

Step 2 View the FIPS configuration by entering this command:

show switchconfig

Information similar to the following appears:

```
802.3x Flow Control Mode......................... Disable
FIPS prerequisite features....................... Enabled
WLANCC prerequisite features..................... Enabled
UCAPL prerequisite features...................... Enabled
secret obfuscation............................... Enabled
```

Preparing Controller in FIPS Mode for Management in Cisco Prime Infrastructure (CLI)

This is an update to the existing FIPS feature function. As per this update, when the controller is in FIPS mode or when the Cisco Prime Infrastructure (PI) is used for SNMP management, SNMP trap logger, and as a syslog server with IPsec, you must add the Cisco PI IP address in the controller before adding the controller IP address in the PI configuration.

Procedure

Step 1 Enable FIPS mode in controller

Note Do not execute the optional steps (b, c) when using Cisco 3702E AP in the network.

Cisco Wave 1 APs (AP3702/AP2702/AP1702) support FIPS DTLS 1.0 with AES128-SHA1 or AES256-SHA256 only. WLAN Common Criteria (WLAN CC) requires DTLS 1.2 with Ephemeral Diffie-Hellman (DHE) cipher suite. Hence, these APs cannot join the controller with WLANCC enabled.

a) Configure FIPS on the controller by entering this command:

   config switchconfig fips-prerequisite {**enable** | **disable**}

b) [Optional] Configure WLAN Common Criteria on the controller by entering this command:

   config switchconfig wlancc {**enable** | **disable**}

c) [Optional] Configure UCAPL on the controller by entering this command:

   config switchconfig ucapl {**enable** | **disable**}

d) Save the current configuration to the NVRAM by entering this command:

   save config

e) Reboot the controller by entering this command:

   reset system

Step 2 Configure the Cisco PI IP address to manage the controller by entering this command:

config snmp pi-ip-address *ip-address* {**add** | **delete**}

Note The IP address is the Cisco PI eth0 interface IP address.

Step 3 Configure the IPSec profile.

a) Create the IPSec profile by entering this command:

   config ipsec-profile {**create** | **delete** } *profile-name*

b) Configure the IPSec profile encryption by entering this command:

   config ipsec-profile encryption {**aes-128-cbc** | **aes-256-cbc** | **aes-128-gcm** | **aes-256-gcm** } *profile-name*

c) Configure the IPSec profile authentication by entering this command:

   config ipsec-profile authentication {**hmac-sha256** | **hmac-sha384** } *profile-name*

d) Configure the IPSec life time in seconds by entering this command:

   config ipsec-profile life-time-ipsec *life-time-ipsec seconds profile-name*

   The valid range is between 1800 and 28800 seconds. Default is 1800 seconds.

e) Configure Internet Key Exchange (IKE) lifetime in seconds by entering this command:

   config ipsec-profile life-time-ike *life-time-ipsec seconds profile-name*

   The valid range is between 1800 and 86400 seconds. Default is 28800 seconds.

f) Configure the IPSec profile Internet Key Exchange (IKE) version by entering this command:

   config ipsec-profile ike version {**1** | **2** } *profile-name*

   Note Currently only IKE version 1 is supported.

g) Configure the IKE authentication method by entering this command:

config ipsec-profile ike auth-mode certificate *profile-name*

h) Attach the IPSec profile to SNMP by entering this command:

config snmp community ipsec profile *profile-name*

i) Enable IPSec for SNMP by entering this command:

config snmp community ipsec enable

Step 4 Configure SNMP Trap Receiver.

a) Configure the IPSec profile to the Trap receiver by entering this command:

config snmp trapreceiver ipsec profile *profile-name trap-receiver-name*

b) Enable SNMP Traps over IPSec by entering this command:

config snmp trapreceiver ipsec enable *trap-receiver-name*

Step 5 Configure Syslog.

a) Configure the host IP for the syslog by entering this command:

config logging syslog host *ip address*

You can add up to three syslog servers to the controller.

b) Assign an IPSec profile to syslog by entering this command:

config logging syslog ipsec profile *profile-name*

c) Enable logging messages to syslog over IPSEC by entering this command:

config logging syslog ipsec enable

d) Deleting syslog server IP address by entering this command:

config logging syslog host *ip address* **delete**

Step 6 Disabling and unlinking the IPSec profile prior to editing the IPSec profile.

- SNMP
  a. Disable—**config snmp community ipsec disable**

  b. Unlink—**config snmp community ipsec none**

- Trap Receiver
  a. Disable—**config snmp trapreceiver ipsec disable** *trapreceiver-name*

  b. Unlink—**config snmp trapreciver ipsec profile none** *trapreceiver-name*

- Syslog
  a. Disable—**config logging syslog ipsec disable**

  b. Unlink—**config logging syslog ipsec profile none**

Step 7 View the active IPSec tunnel details by entering this command:

```
show ipsec status
```

Cisco TrustSec

Cisco TrustSec enables organizations to secure their networks and services through identity-based access control to anyone, anywhere, anytime. The solution also offers data integrity and confidentiality services, policy-based governance, and centralized monitoring, troubleshooting, and reporting services. You can combine Cisco TrustSec with personalized, professional service offerings to simplify the solution deployment and management, and is a foundational security component to Cisco Borderless Networks.

The Cisco TrustSec security architecture helps build secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between the devices in the domain is secured with a combination of encryption, message integrity check, and data path replay protection mechanisms. Cisco TrustSec uses a device and user credentials that are acquired during authentication for classifying the packets by security groups (SGs), as they enter the network. This packet classification is maintained by tagging packets on an ingress to the Cisco TrustSec network. This is because they can be correctly identified to apply security and other policy criteria along the data path. The tag, called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. Note that the Cisco TrustSec security group tag is applied only when you enable AAA override on a WLAN.

One of the components of Cisco TrustSec architecture is the security group-based access control. In the security group-based access control component, access policies in the Cisco TrustSec domain are topology-independent, based on the roles (as indicated by the security group number) of source and destination devices rather than on network addresses. Individual packets are tagged with the security group number of the source.

The Cisco TrustSec solution is implemented across the following three distinct phases:

- Client classification at ingress by a centralized policy database (Cisco ISE) and assigning unique SGT to clients based on client identity attributes such as the role and so on.
- Propagation of IP-to-SGT binding to neighboring devices using the SGT Exchange Protocol (SXP) or inline tagging methods or both.
- Security Group Access Control List (SGACL) policy enforcement. Cisco AP is the enforcement point for central or local switching (central authentication).

For more information about deploying the Cisco TrustSec solution, see the *Wireless TrustSec Deployment Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-4/b_wireless_trustsec_deployment_guide.html.

SGT Exchange Protocol

Cisco devices use the SGT Exchange Protocol (SXP) to propagate SGTs across network devices that do not have any hardware support for Cisco TrustSec. The SXP is the software solution to eliminate the need for upgrade of Cisco TrustSec hardware on all Cisco switches. Controller supports the SXP as part of the Cisco TrustSec architecture. The SXP sends SGT information to the Cisco TrustSec-enabled switches so that appropriate role-based access control lists (RBAC lists) can be activated. This depends on the role information present in the SGT. To implement the SXP on a network, only the egress distribution switch has to be Cisco TrustSec-enabled. All the other switches can be non-Cisco TrustSec-capable switches.

The SXP runs between the access layer and the distribution switch or between two distribution switches. The SXP uses TCP as the transport layer. Cisco TrustSec authentication is performed for the host (client) joining the network on the access layer switch. This is similar to an access switch with the hardware that is enabled with Cisco TrustSec. The access layer switch is not Cisco TrustSec hardware enabled. Therefore, data traffic is not encrypted or cryptographically authenticated when it passes through the access layer switch. The SXP is used to pass the IP address of the authenticated device, which is a wireless client and the corresponding SGT up to the distribution switch. If the distribution switch is a hardware that is enabled with Cisco TrustSec, the switch inserts the SGT into the packet on behalf of the access layer switch. If the distribution switch is not a hardware that is enabled with Cisco TrustSec, the SXP on the distribution switch passes the IP-SGT mapping to all the distribution switches that have the Cisco TrustSec hardware. On the egress side, the enforcement of the RBAC lists occurs at the egress L3 interface on the distribution switch.

The following are some guidelines for Cisco TrustSec SXP:

- The SXP is supported only on the following security policies:
  - WPA2-dot1x
  - WPA-dot1x
  - MAC filtering using RADIUS servers
  - Web authentication using RADIUS servers for user authentication
- The SXP is supported for both IPv4 and IPv6 clients.
- By default, the controller always works in the Speaker mode.
- From Release 8.3, the SXP on the controller is supported for both centrally and locally switched networks.
- It is possible to do IP-SGT mapping on the WLANs as well for clients that are not authenticated by Cisco ISE.

For more information about Cisco TrustSec, see
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html.

Guidelines and Restrictions on Cisco TrustSec

- SXP is supported only in centrally switched networks that have central authentication.
- By default, SXP is supported for APs that work only in local mode.
- The configuration of the default password should be consistent for both the controller and the switch.
- Fault tolerance is not supported because fault tolerance requires local switching on APs.
- Static IP-SGT mapping for local authentication of users is not supported.
- IP-SGT mapping requires authentication with external Cisco ISE servers.
- In auto-anchor/guest-anchor mobility, the SGT information that is passed by the RADIUS server to a foreign controller can be communicated to the anchor controller through the EoIP/CAPWAP mobility tunnel. The anchor controller can then build the SGT-IP mapping and communicate it to another peer via SXP.

- In a local web authentication with AAA override scenario, if a client tries to login after logging out, SGT from WLAN is not applied again and the client retains the AAA overridden SGT.
- It is possible to change the interface management IP address even if you have Cisco TrustSec SXP in enabled state.
- Cisco TrustSec (CTS) is not supported when the controller is in FIPS mode.

Configuring Cisco TrustSec

Configuring Cisco TrustSec on Controller (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **General**.
The **General** page is displayed.

Step 2 Check the **CTS** check box to enable Cisco TrustSec. By default, Cisco TrustSec is in disabled state.

Step 3 Save the configuration.

Configuring Cisco TrustSec on Cisco WLC (CLI)

Procedure

- Enable Cisco TrustSec on the controller by entering this command:

  config cts enable

Note If you enable Cisco TrustSec, the SGACL is also enabled in the controller. Also, you will need to manually enable inline tagging.

SXP

Configuring SXP on Cisco WLC (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **SXP Config**.

The **SXP Configuration** page is displayed with the following SXP configuration details:

- **Total SXP Connections**—Number of SXP connections that are configured.
- **SXP State**—Status of SXP connections as either disabled or enabled.

- **SXP Mode**—SXP mode of the Cisco WLC. The Cisco WLC is always set to Speaker mode for SXP connections.
- **Default Password**—Password for MD5 authentication of SXP messages. We recommend that the password contain a minimum of 6 characters.
- **Default Source IP**—IP address of the management interface. SXP uses the default source IP address for all new TCP connections.
- **Retry Period**—SXP retry timer. The default value is 120 seconds (2 minutes). The valid range is 0 to 64000 seconds. The SXP retry period determines how often the controller retries for an SXP connection. When an SXP connection is not successfully set up, the controller makes a new attempt to set up the connection after the SXP retry period timer expires. Setting the SXP retry period to 0 seconds disables the timer and retries are not attempted.

This page also displays the following information about SXP connections:

- **Peer IP Address**—The IP address of the peer, that is, the IP address of the next-hop switch to which the Cisco WLC is connected. There is no effect on the existing TCP connections when you configure a new peer connection.
- **Source IP Address**—The IP address of the source, that is, the management IP address of the Cisco WLC.
- **Connection Status**—Status of the SXP connection.

Step 2 From the **SXP State** drop-down list, choose **Enabled** to enable SXP.

Step 3 Enter the default password that should be used to make an SXP connection. We recommend that the password contain a minimum of 6 characters.

Step 4 In the **Retry Period** field, enter the time, in seconds, that determines how often the Cisco TrustSec software retries for an SXP connection.

Step 5 Click **Apply** to commit your changes.

Configuring SXP on Cisco WLC (CLI)

Procedure

- Enable or disable the SXP on the controller by entering this command:

  config cts sxp {**enable** | **disable**}

- Configure the default password for MD5 authentication of SXP messages by entering this command:

  config cts sxp default password *password*

- Configure the IP address of the next-hop switch with which the controller is connected by entering this command:

  config cts sxp connection peer *ip-address*

- Configure the interval between connection attempts by entering this command:

  config cts sxp retry period *time-in-seconds*

- Remove an SXP connection by entering this command:

config cts sxp connection delete *ip-address*

- See a summary of the SXP configuration by entering this command:

  show cts sxp summary

  The following is a sample output of this command:

  ```
  SXP State....................................... Enable
  SXP Mode........................................ Speaker
  Default Password................................ ****
  Default Source IP............................... 209.165.200.224
  Connection retry open period ................... 120
  ```

- See the list of SXP connections that are configured by entering this command:

  show cts sxp connections

  The following is a sample output of this command:

  ```
  Total num of SXP Connections.................... 1
  SXP State....................................... Enable
  Peer IP            Source IP           Connection Status
  ---------------    ---------------     -----------------
  209.165.200.229   209.165.200.224             On
  ```

- Establish connection between the controller and a Cisco Nexus 7000 Series switch by following either of these steps:

  - Enter the following commands:

    1. **config cts sxp version sxp version 1 or 2** *1*

    2. **config cts sxp disable**

    3. **config cts sxp enable**

  - If SXP version 2 is used on the controller and version 1 is used on the Cisco Nexus 7000 Series switch, an amount of retry period is required to establish the connection. We recommend that you initially have less interval between connection attempts. The default is 120 seconds.