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.

From Release 8.4, SXPv4 is supported in FlexConnect mode APs.

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

Environment Data

Cisco TrustSec environment data is a set of information or attributes that helps controller to perform Cisco TrustSec-related functions.

The controller acquires the environment data from the authentication server (Cisco ISE) when the controller first joins a Cisco TrustSec domain by sending a secure RADIUS Access request. The authentication server returns a RADIUS Access-Accept message with attributes, including environment expiry timeout attributes. This is the time interval that controls how often the Cisco TrustSec device must refresh its environment data.

Security Group Access Control List Policy Download

A Security Group is a group of users, endpoint devices, and resources that share access control policies. Security groups are defined by the administrator in the Cisco ISE. As new users and devices are added to the Cisco TrustSec domain, the authentication server assigns these new entities to the appropriate security groups. Cisco TrustSec assigns each of the security group a unique 16-bit number whose scope is global in a Cisco

TrustSec domain. The number of security groups in a wireless device is limited to the number of authenticated network entities. You do not have to manually configure the security group numbers.

After a device is authenticated, the Cisco TrustSec tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT everywhere in the network, in the Cisco TrustSec header.

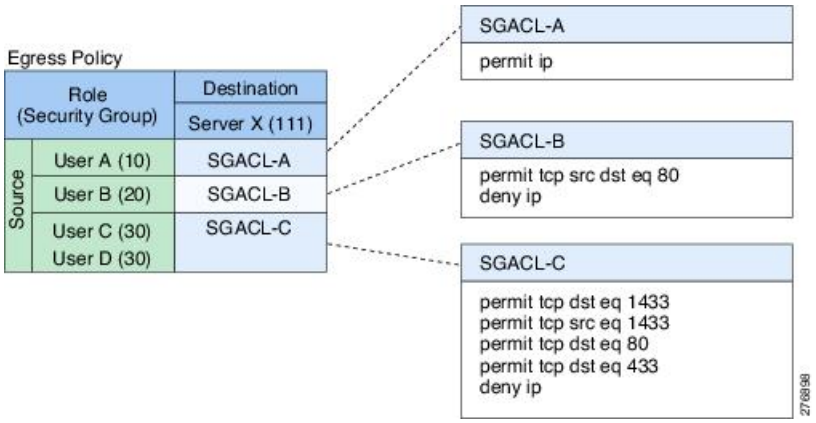
As the SGT contains the security group of the source, the tag can be referred to as the source SGT (S-SGT). The destination device is also assigned to a security group (destination SG) that can be referred to as the destination SGT (D-SGT), although the Cisco TrustSec packet does not contain the security group number of the destination device.

You can control the operations that users can perform based on the security group assignments of users and destination resources, using the Security Group Access Control Lists (SGACLs). Policy enforcement in a Cisco TrustSec domain is represented by a permission matrix, with the source security group on one axis and destination security group numbers on the other axis. Each cell in the matrix body contains an ordered list of SGACLs, which specifies the permissions that must be applied to packets originating from the source security group and destined for the destination security group. When a wireless client is authenticated, it downloads all the SGACLs in the matrix cells.

When a wireless client connects to the network, the client pushes all the ACLs to the controller.

This figure shows an example of a Cisco TrustSec permission matrix with three defined user roles, one defined destination resource, and three SGACL policies that control access to the destination server based on the user roles.

Figure 1: Example of an SGACL Policy Matrix



Cisco TrustSec achieves role-based topology-independent access control in a network by assigning users and devices in the network to security groups and applying access control between the security groups. The SGACLs define access control policies based on the device identities. As long as the roles and permissions remain the same, changes to the network topology do not change the security policy. When a user is added to the wireless group, you simply assign the user to an appropriate security group and the user immediately receives permissions to that group.

The size of ACLs is reduced and their maintenance is simplified with the use of role-based permissions. With Cisco TrustSec, the number of Access Control Entities (ACEs) configured is determined by the number of permissions that are specified, resulting in a much smaller number of ACEs.

Note By default, the following predefined SGACL policies are downloaded:

- Default policy—This is applied when source and destination SGTs are available, but SGACLs are not defined for a cell or column.
- Unknown policy—This is applied when the source SGT is unknown. You can use the session group named Unknown and apply the unknown policy on that traffic.

The following are examples of SGACLs that are on Cisco ISE and downloaded on a controller and tested:

Generic SGACL

- **Web_SGACL**

  permit tcp dst eq 80

  permit tcp dst eq 443

  deny ip
- **PCI_Servers_SGACL**

  deny tcp dst eq 4444

  deny tcp dst eq 4446

  deny tcp dst eq 443

  permit ip
- **PCI_Zone_SGACL**

  deny tcp dst eq 4444

  deny tcp dst eq 4446

  deny tcp dst eq 443

  permit ip
- **Deny_SSH_RDP_Telnet_SGACL**

  deny tcp dst eq 23

  deny tcp dst eq 23

  deny tcp dst eq 3389

  permit ip
- **Deny_JumpHost_Protocols**

  deny tcp dst eq 23

  deny tcp dst eq 23

  deny tcp dst eq 3389

  permit ip

Anti-Malware SGACLs

- **Anti-Malware-ACL**

deny icmp

deny udp src dst eq domain

deny tcp src dst eq 3389

deny tcp src dst eq 1433

deny tcp src dst eq 1521

deny tcp src dst eq 445

deny tcp src dst eq 137

deny tcp src dst eq 138

deny tcp src dst eq 139

deny udp src dst eq snmp

deny tcp src dst eq telnet

deny tcp src dst eq www

deny tcp src dst eq 443

deny tcp src dst eq 22

deny tcp src dst eq pop3

deny tcp src dst eq 123

deny tcp match-all -ack +fin -psh -rst -syn -urg

deny tcp match-all +fin +psh +urg

permit tcp match-any +ack +syn

Collaboration SGACLs

- **rbacl:Gateway_sig**

  permit udp dst eq 5060 log

  permit tcp dst eq 5060 log

  permit tcp dst eq 5061 log

  permit udp dst range 32768 61000

  permit tcp dst range 32768 61000

  deny ip log

- **rbacl:Intra_Jabber**

  permit udp dst range 16384 32767 log

  permit tcp dst range 49152 65535 log

  permit tcp dest eq 37200 log

  deny ip log

- **rbacl:Jabber_sig**

  permit tcp dst eq 6970 log

permit tcp dst eq 6972 log

permit tcp dst eq 3804 log

permit tcp dst eq 8443 log

permit tcp dst eq 8191 log

permit tcp dst eq 5222 log

permit tcp dst eq 37200 log

permit tcp dst eq 443 log

permit tcp dst eq 2748 log

permit tcp dst eq 5060 log

permit tcp dst eq 5061 log

permit tcp dst range 30000 39999 log

permit udp dst range 5070 6070 log

deny ip log

- **rbacl:Phone_sig**

  permit udp dst eq 69 log

  permit tcp dst eq 8080 log

  permit tcp dst eq 2445 log

  permit tcp dst eq 3804 log

  permit tcp dst eq 5060 log

  permit udp dst eq 5060 log

  permit tcp dst eq 5061 log

  permit tcp dst eq 6970 log

  deny ip log

- **rbacl:UC_endpoint_media**

  permit udp dst range 16384 32767 log

  deny ip log

Inline Tagging

Inline tagging is a transport mechanism using which a controller or a Cisco AP understands the source SGT. Transport mechanism is of two types:

- Central switching—For centrally switched packets, controller performs inline tagging for all the packets that are sourced from wireless clients that are associated with the controller by tagging it with the Cisco Meta Data (CMD) tag. For packets inbound from the Distribution System, inline tagging also involves controller stripping off the CMD header from the packet to learn the S-SGT tag. Controller thereafter forwards the packet including the S-SGT for SGACL enforcement.
- Local switching—To transmit locally switched traffic, Cisco AP performs inline tagging for packets that are associated with the Cisco AP and sourced from clients. To receive traffic, Cisco AP handles both

locally switched packets and centrally switched packets, uses an S-SGT tag for packets, and applies the SGACL policy.

With wireless Cisco TrustSec enabled on the controller, the choice of enabling and configuring SXP to exchange tags with the switches is optional. Both wireless Cisco TrustSec and SXP modes are supported; however, there is no use case to have both wireless Cisco TrustSec on AP and SXP to be in the enabled state concurrently.

Policy Enforcement

Cisco TrustSec access control is implemented using ingress tagging and egress enforcement. At the ingress point to the Cisco TrustSec domain, the traffic from the source is tagged with an SGT containing the security group number of the source entity. The SGT is propagated across the domain with the traffic. At the egress point of the Cisco TrustSec domain, an egress device uses the source SGT (S-SGT) and the security group of the destination entity (D-SGT) to determine the access policy to apply from the SGACL policy matrix.

You can apply policy enforcement to both central and local switched traffic on an AP. If wired clients communicate with wireless clients, the Cisco AP enforces the downstream traffic. If wireless clients communicate with wired clients, the Cisco AP enforces the upstream traffic. This way, the Cisco AP enforces traffic in both downstream and wireless-to-wireless traffic. You require S-SGT, D-SGT, and ACLs for enforcement to work. Cisco APs get the SGT information for all wireless clients from the information available on the Cisco ISE server.

Note A Cisco AP must be in either Listener or Both (Listener and Speaker) mode to enforce traffic as the Listener mode maintains the complete set of IP-SGT bindings. After you enable enforcement on a Cisco AP, the corresponding policies are downloaded and pushed to the Cisco AP.

Guidelines and Restrictions on Cisco TrustSec

- The configuration of the default password should be consistent for both the controller and the switch.
- 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.
- Cisco TrustSec is not supported in L3 and Guest Access deployments.
- Cisco TrustSec in Monitor mode is not supported.
- Device or Multicast SGT and server list as part of environment data is not supported.

- Change of Authorization (CoA) for policy and environment data refresh is not supported.
- In a High Availability (HA) setup, environment data, and SGACLs are not synchronized with standby controllers. The PAC information and device ID and password are synchronized. Upon a controller failover, environment data and SGACLs are downloaded from Cisco ISE.

Note In an HA setup, when a client connects to an AP that is associated with the active controller, the AP-SGT information is updated in the standby controller. This AP-SGT mapping is used to download the SGT policy after an HA switchover. The policy is not synchronized with the standby controller. However, the AP-SGT information is used to initiate the policy download after the HA switchover.

Only the active controller can set create an SXP socket connection to the peer; The standby controller does not establish the SXP socket connection. Therefore, the SXP status in the standby controller is 'OFF'.

- When a controller running Release 8.4 or a later release becomes nonoperational, an AP associated with the WLC might switch to another controller running Release 8.3 or an earlier release and download the image. Then, the AP cannot communicate with the controller because Release 8.3 and older releases do not support inline tagging. In this case, we recommend that you disable Cisco TrustSec manual configuration mode (**cts manual**) on the AP switchport so that the AP can download the image.
- The **policy static sgt** *tag* **trusted** command, in the Cisco TrustSec manual configuration mode, is used in an inline tagging enabled setup, when the AP switch port is required to trust the SGT tag set by the peer. In case of untagged traffic, the switch port tags all the packets with the value that is configured in this command. Therefore, this configuration must not be used when inline tagging is disabled.
- Static SGACL policy is not supported on controller.
- Policy enforcement is not applied to multicast traffic.
- Inline and SXPv4 are not supported in a FlexConnect split tunneling scenario.
- In a mixed-mode deployment scenario, if a Cisco AP is configured with two SXP peer connections, the password of one peer connection is set to *default* and the password of the other peer connection is set to *none*. In such a scenario, the peer connection with the password set to *none* will not be operational. However, if all the SXP peer connections are configured with the password *none*, the SXP peer connections are operational.
- Cisco TrustSec is not supported for Guest LAN clients.
- Cisco TrustSec is not supported on Outdoor and Industrial Wireless mesh APs.
- Cisco TrustSec is not supported in Cisco Wave 2 APs that are in Flex+Bridge mode.
- PAC provisioning is not supported on these Cisco WLCs: 5508, WiSM2, 8510, 7510, and vWLC.
- PAC provisioning is not supported on a IPv6 server.
- Inline tagging and SGACL download and enforcement are not supported on these Cisco WLCs: 5508, WiSM2, 8510, 7510, and vWLC.
- SXPv4 Listener and Both modes are not supported in FlexConnect deployments with these Cisco WLCs: 5508, WiSM2, 8510, 7510, and vWLC.

- Inline tagging is not supported in Cisco Wave 2 APs that are in Flex+Bridge mode.
- We recommend that you do not use SXPv4 for a NAT scenario (FlexConnect Central DHCP).
- If you encounter the `CTS CORE: AAA-3-AUTH_REQUEST_QUEUE_FAILED` system message, no action is required. This is an expected error log after every controller reboot. This system message is displayed because the Cisco TrustSec core is initialized before AAA.

Cisco TrustSec Feature Support Matrix

Table 1: Cisco TrustSec Feature Support Matrix

AP Mode	SXPv4 Support	Inline Tagging Support	Enforcement Support	Cisco Aironet AP Series	Remarks
Local	No	No	Yes	1700, 2700, 3700	NA
				18*xx*, 38*xx*, 28*xx*	
FlexConnect	Yes	Yes	Yes	1700, 2700, 3700	NA
				18*xx*, 38*xx*, 28*xx*	
Flex+Bridge	Yes	No	Yes	1700, 2700, 3700	NA
	No	No	No	18*xx*, 38*xx*, 28*xx*	Flex+Bridge mode is not supported on these APs.
Mesh	No	No	Yes (Online for indoor mesh)	1700, 2700, 3700	No support for outdoor mesh
	No	No	No	18*xx*, 38*xx*, 28*xx*	Mesh mode is not supported.

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.

Configuring Cisco TrustSec Override for an Access Point (CLI)

Procedure

- Enable or disable override of global Cisco TrustSec configuration on a specific AP by entering this command:

  config cts ap override {**enable** | **disable**} *cisco-ap*

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.

Configuring SXP on Cisco Access Points (GUI)

This configuration is applicable to only FlexConnect, Flex+Bridge, Mesh, and Local mode APs.

Procedure

Step 1 Choose **Wireless** > **Access Points** > **All APs** and the name of the desired access point.

Step 2 Click the **Advanced** tab.

Step 3 In the **Trusted Security** area, click **TrustSec Config**.
The **All APs** > **<ap-name>** > **Trusted Security** page is displayed.

Step 4 In the **Trusted Security** area, check the **SGACL Enforcement** check box.

Step 5 Save the configuration.

Configuring SXP on Cisco Access Points (CLI)

This configuration is applicable to only FlexConnect, Flex+Bridge, Mesh, and Local mode APs.

Procedure

- Enable or disable the SXP for an access point or all access points by entering this command:

  config cts sxp ap {**enable** | **disable**} {*ap_name* | **all**}

- Configure the default password for the SXP connection by entering this command:

config cts sxp ap default password *password* {*ap-name* | **all**}

- Configure the SXP peer IP address with which a Cisco AP is connected by entering this command:

  config cts sxp ap connection peer *ip-address* **password** {**default** | **none**} **mode** {**both** | **listener** | **speaker**} {*ap-name* | **all**}

- Configure the minimum and maximum time intervals for the SXP connection to be alive by entering this command:

  config cts sxp ap listener hold-time *min max* {*ap-name* | **all**}

- Configure the reconciliation time interval on a Cisco AP by entering this command:

  config cts sxp ap reconciliation period *time-in-seconds* {*ap-name* | **all**}

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

  config cts sxp ap retry period *time-in-seconds* {*ap-name* | **all**}

- Configure the connection hold time by entering this command:

  config cts sxp ap speaker hold-time *hold-time-in-seconds* {*ap-name* | **all**}

Note If a Cisco AP with a DHCP IP is rebooted, associates with the Cisco WLC after the reboot, and has a different IP address, the SXP connection fails. To overcome this, perform either of the following tasks:

- Define a reserved set of IP addresses in DHCP for the Cisco AP.
- Configure a static IP address for the Cisco AP.

Cisco TrustSec Credentials

Configuring Cisco TrustSec Credentials (GUI)

Procedure

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

Step 2 In the **Device ID** field, enter the Cisco TrustSec device ID.

Step 3 In the **Password** field, enter the Cisco TrustSec device password.

Step 4 Check or uncheck the **Inline Tagging** check box to enable or disable inline tagging.

Step 5 In the **Environment Data** area, the following information is displayed:

- **Current State**—Shows whether the environment data is complete or not.
- **Last Status**—Shows the last state of the environment data.

Step 6 Click **Apply** to commit your changes.

Step 7 Click **Refresh Env Data** to refresh the environment data.

Configuring Cisco TrustSec Credentials (CLI)

Procedure

- Configure a Cisco TrustSec device ID and password by entering this command:

  config cts device-id *device-id* **password** *password*

Configuring a RADIUS AAA Server (GUI)

You can configure multiple RADIUS accounting and authentication servers. For example, you may want to have one central RADIUS authentication server but several RADIUS accounting servers in different regions. If you configure multiple servers of the same type and the first one fails or becomes unreachable, the controller automatically tries the second one, then the third one if necessary, and so on.

Configuring RADIUS AAA Server (CLI)

Procedure

Configure a RADIUS authentication server to enable RADIUS PAC by entering the command:

config radius auth pac *srv-index* **enable**

Here *srv-index* specifies the RADIUS server index between 1 and 32.

Monitoring Environment Data

Monitoring Environment Data (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **General**.
The **General** page is displayed with the following details as part of Environment data: **Current State** and **Last Status**.

Step 2 To view the updated information, click **Refresh Env Data**.

Monitoring Environment Data (CLI)

Procedure

- View Cisco TrustSec environment data by entering this command:

  show cts environment-data

- Refresh Cisco TrustSec environment data by entering this command:

  config cts refresh environment-data

Note You must manually refresh the environment data from Cisco ISE because CoA is not supported in Cisco Wireless Release 8.4.

Configuring a Static Security Group Tag on a WLAN

Configuring a Static Security Group Tag on a WLAN (GUI)

Procedure

Step 1 Choose **WLANs** to open the WLANs page.

Step 2 Click the WLAN ID.

Step 3 On the **WLANs** > **Edit** page, click the **Advanced** tab.

Step 4 Under the **TrustSec** area, in the **Security Group Tag** field, enter a value between 0 and 65533.

Step 5 Save the configuration.

Configuring a Static Security Group Tag on a WLAN (CLI)

Procedure

- Configure a static Security Group Tag (SGT) on a WLAN by entering this command:

  config wlan security sgt *value wlan-id*

  The valid range for *value* is between 0 and 65533.

Note This command is applicable for local and web authentication of clients in Cisco WLC. The SGT also applies to clients that are connected to WLANs with AAA override disabled.

Configuring Inline Tagging

Configuring Inline Tagging in Cisco WLC (GUI)

Procedure

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

Step 2 Check the **Inline Tagging** check box to enable inline tagging. By default, inline tagging is in disabled state.

Step 3 Save the configuration.

Configuring Inline Tagging in Cisco WLC (CLI)

Procedure

- Enable or disable inline tagging in the controller by entering this command:

  config cts inline-tag {**enable** | **disable**}

Note Controllerperforms the task of inline tagging for central switching packets.

Configuring Inline Tagging in Cisco Access Points (GUI)

Before you begin

1. Inline tagging is supported only on APs in FlexConnect mode.
2. By default, inline tagging is in disabled state.

Procedure

Step 1 To configure inline tagging on all APs:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.
The **Global Configuration** page is displayed.
b) Under the **TrustSec** area, click **TrustSec Config**.
The **All APs Trusted Security** page is displayed.
c) To enable inline tagging, check the **Inline Tagging** check box.
d) Click **Apply**.

Step 2 To configure inline tagging on a specific AP:

a) Choose **Wireless** > **Access Points** > **All APs**.
b) Click the name of the AP.
The **All APs > Details for <ap-name>** page is displayed.
c) Click the **Advanced** tab.
d) Under the **TrustSec** area, click **TrustSec Config**.
e) In the **Trusted Security** area, check the **Inline Tagging** check box to enable inline tagging.
f) Click **Apply**.

Configuring Inline Tagging in Cisco Access Points (CLI)

Before you begin

1. Inline tagging is supported only on APs in FlexConnect mode.

2. By default, inline tagging is in disabled state.

Procedure

- Enable or disable inline tagging on a specific AP or all APs by entering this command:

  config cts ap inline-tagging {*enable* | *disable*} {*Cisco AP* | **all**}

- See if a configuration is applied to a specific AP by entering this command:

  show ap config general {*Cisco AP*}

- See the status of inline tagging on all FlexConnect APs by entering this command:

  show cts ap summary

Note APs perform the task of inline tagging for local switching packets.

Verifying SGACL Policy Download

Verifying SGACL Policy Download in Cisco WLC (GUI)

Procedure

Step 1 Choose **Security** > **TrustSec** > **Policy**.

Step 2 Click a D-SGT.
The **SGT Detail** page is displayed with details of the SGT including the SGACL policy name.

Step 3 Click **Refresh** to refresh the SGT information.

Note CoA is not supported. Therefore, we recommend that you manually refresh the SGACL policy from the Cisco ISE.

Verifying SGACL Policy Download in Cisco WLC (CLI)

Procedure

- View all or specific SGT policy information by entering this command:

  show cts policy {**all** | *sgt_tag*}

- View all or specific SGACL information by entering this command:

  show cts sgacl {**all** | *sgacl name*}

- Check if the SGACL is enabled or disabled for a specific AP by entering this command:

  show ap config general *cisco-ap*

- View the SGACL policy enabled globally by entering this command:

show cts ap summary

- Refresh all SGTs by entering this command:

  config cts refresh policy sgt all

- Refresh a specific SGT by entering this command:

  config cts refresh policy sgt *sgt-tag*

Note CoA is not supported. Therefore, we recommend that you manually refresh the SGACL policy from Cisco ISE.

Configuring Policy Enforcement

Configuring Policy Enforcement (GUI)

Before you begin

SGACL enforcement is supported only on Cisco 5520 and 8540 Wireless Controllers.

Procedure

Step 1 To configure policy enforcement in a specific Cisco AP:

a) Choose **Wireless** > **Access Points** > **All APs** to open the **All APs** page.
b) Click the AP name.
The **All APs > Details for <ap-name>** page is displayed.
c) Click the **Advanced** tab.
d) In the **Trusted Security** area, click **TrustSec Config**.
The **All APs > <ap-name> > Trusted Security** page is displayed.
e) In the **Trusted Security** area, check the **SGACL Enforcement** check box to enforce SGACL policies on the AP.

By default, SGACL enforcement is in disabled state.

f) Click **Apply**.

Step 2 To configure policy enforcement in all Cisco APs:

a) Choose **Wireless** > **Access Points** > **Global Configuration**.
b) In the **TrustSec** area, click **TrustSec Config**.
The **All APs Trusted Security** page is displayed.
c) Check the **SGACL Enforcement** check box to enforce SGACL policies on all APs.
d) Click **Apply**.

Configuring Policy Enforcement (CLI)

Procedure

- Enable the SGACL enforcement for a specific AP or all APs by entering this command:

  config cts ap sgacl-enforcement enable {*ap-name* | **all**}

Note If you enable SGACL enforcement for all APs, the configuration is applied on all APs, except the ones for which CTS override is enabled.

Debugging Cisco TrustSec in Cisco WLC (CLI)

Procedure

- Configure the debug options for Cisco TrustSec AAA by entering this command:

  debug cts aaa {**all** | **errors** | **events**} {**enable** | **disable**}

- Configure the debug options Cisco TrustSec authorization by entering this command:

  debug cts authz {**all** | **errors** | **events** | **aaa**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec policy download over CAPWAP messages by entering this command:

  debug cts capwap {**all** | **errors** | **events** | **messages**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec environment data by entering this command:

  debug cts env-data {**all** | **errors** | **events**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec HA by entering this command:

  debug cts ha {**all** | **errors** | **events**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec key store by entering this command:

  debug cts key-store {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec PAC provisioning by entering this command:

  debug cts provisioning {**all** | **errors** | **events** | **packets**} {**enable** | **disable**}

- Configure the debug options for Cisco TrustSec SXP by entering this command:

  debug cts sxp {**all** | **errors** | **events** | **framework** | **message**} {**enable** | **disable**}

- Configure SGT debugging for up to 10 SGTs by entering this command::

  debug cts sgt *sgt-1…sgt-10*

- Display all the AP-SGT information by entering this command:

  show cts ap sgt-info

Cisco TrustSec Commands on Lightweight APs

Enter these commands in a lightweight AP console:

Procedure

- Show commands:
  a) Check the SXP connection status by entering this command:
     - On Cisco Aironet 1700, 2700, and 3700 Series APs: **show cts sxp connections brief**
     - On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs: **show cts sxp connections**

  b) Check SXP bindings by entering this command:
     - On Cisco Aironet 1700, 2700, and 3700 Series APs: **show cts sxp sgt-map brief**
     - On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs: **show cts sxp sgt-map**

  c) Check IP-SGT binding by entering this command:
     - On Cisco Aironet 1700, 2700, and 3700 Series APs for local switching only: **show cts role-based sgt-map all**
     - On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs for local switching and central switching only: **show cts role-based sgt-map all**

  d) Check SGT for central switching clients by entering this command:

     show controllers {*dot11Radio0|1* | **begin** *SGT*}

  e) Check SGACLs for S-SGT and D-SGT by entering this command:

     show cts role-based permissions [**default** | **from** | **ipv4** | **ipv6** | **to** | *cr*]

  f) Check counter for given source and destination SGT by entering this command:

     show cts role-based counters [**default** | **from** | **ipv4** | **ipv6** | **to** | *cr*]

  g) Check ACEs for a given SGACL by entering this command:

     show access-lists *access-list-name*

- Debug commands:
  a) Debug Cisco TrustSec enforcement by entering this command:

     On Cisco Aironet 18*xx*, 28*xx*, and 38*xx* Series APs: **debug cts enforcement**

  b) Debug enforcement related issues, for both central and local switched data traffic. by entering this command:

     On Cisco Aironet 1700, 2700, and 3700 Series APs: **debug rbm dp packets**

IPSec Profile

Configuring an IPSec Profile (GUI)

Procedure

Step 1 Choose **Management** > **IPSec** to navigate to the **IPSec Profile Name** page.

Step 2 Click **New** and enter a name for the IPSec profile.

Step 3 In the **IPSec Profile Name** listing, click the newly created IPSec profile name to configure the profile parameters.

Step 4 Enter the **IKE Version**. Supported Internet Key Exchange (IKE) versions are 1 and 2.

Step 5 From the **Encryption** drop-down list, choose from the following encryption types:

- **aes-128-cbc**
- **aes-256-cbc**
- **aes-128-gcm**
- **aes-256-gcm**

Note The encryption type choices are of either 128 or 256 key lengths and either Cipher Block Chaining mode or Galois/Counter mode.

Step 6 From the **Authentication** drop-down list, choose from the following hash-based message authentication code (HMAC) secure hash algorithm (SHA) options:

- **HMAC SHA1**
- **HMAC SHA256**
- **HMAC SHA384**

Step 7 From the **IKE DH Group** drop-down list, choose from the following Diffie-Hellman groups:

- **Group 14** (2048 bits)
- **Group 19** (256-bit elliptic curve)
- **Group 20** (384-bit elliptic curve)

Step 8 In the **IKE Lifetime (1800-86400)** field, enter a value (in seconds) to specify the timeout interval for IKE. The valid range is 1800 to 86400 seconds, and the default value is 28,800 seconds.

Step 9 In the **IPSec Lifetime (1800-28800)** field, enter a value (in seconds) to specify the timeout interval for IPSec. The valid range is 1800 to 28800 seconds, and the default value is 1800 seconds.

Step 10 From the **IKE Phase 1** drop-down list, choose one of the following options to specify the IKE protocol:

- **Main**
- **Aggressive**

IKE Phase 1 is used to negotiate how IKE should be protected. Aggressive mode passes more information in fewer packets with the benefit of slightly faster connection establishment at the cost of transmitting the identities of the security gateways in the clear.

Step 11 From the **IKE Peer Identification** drop-down list, choose from the following options to be used:

- **FQDN**
- **User FQDN**
- **CN**
- **IP**

Step 12 In the **IKE Peer Value** field, enter the peer value for IKE.

Step 13 From the **IKE Authentication Mode** drop-down list, choose from the following options:

- **PSK**
- **Certificate**

Step 14 From the **Shared Secret Format** drop-down list, choose **ASCII** or **Hex** to specify the format of the shared secret key to be used between the controller and the RADIUS server. The default value is ASCII.

Step 15 In the **Shared Secret** and **Confirm Shared Secret** fields, enter the shared secret key to be used for authentication between the controller and the server.

Note The shared secret key must be the same on both the server and the controller.

Step 16

Step 17 In the **Shared Secret** and **Confirm Shared Secret** fields, enter the shared secret key to be used for authentication between the controller and the server.

Note The shared secret key must be the same on both the server and the controller.

Step 18 Save the configuration.

Configuring an IPSec Profile (CLI)

Procedure

Step 1 Create the IPSec profile by entering this command:

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

Step 2 Configure the IPSec profile Internet Key Exchange (IKE) version by entering this command:

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

Step 3 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*

Step 4 Configure the IPSec profile authentication by entering this command:

config ipsec-profile authentication {**hmac-sha1** |**hmac-sha256** | **hmac-sha384** } *profile-name*

Step 5 Configure the IKE Diffie-Hellman group by entering this command:

config ipsec-profile ike dh-group {**group-14** |**group-19** | **group-20** } *profile-name*

Step 6 Configure the IKE lifetime by entering this command:

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

The valid range is 1800 to 86400 seconds, and the default value is 28,800 seconds.

Step 7 Configure the IPSec lifetime by entering this command:

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

The valid range is 1800 to 28800 seconds, and the default value is 1800 seconds.

Step 8 Configure IKE Phase1 mode by entering this command:

config ipsec-profile ike phase1 {**aggressive** |**main** } *profile-name*

Step 9 Configure the peer identification mode by entering this command:

config ipsec-profile ike peer-identification {**fqdn** |**user-fqdn** | **dn** | **ip** } *profile-name*

Step 10 Configure the IKE authentication method and the shared secret by entering this command:

config ipsec-profile ike auth-mode {{**pre-shared-key** *profile-name* {*ascii* | *hex*} *shared-secret*} | {**certificate** *profile-name*}}

Step 11 Save the configuration.