Security Features

Device Security

Security features protect against several threats, including threats to the identity of the device and to data. These features establish and maintain authenticated communication streams between the device and the Cisco Unified Communications Manager server, and ensure that the device uses only digitally signed files.

Cisco Unified Communications Manager Release 8.5(1) and later includes Security by Default, which provides the following security features for devices without the need to run the CTL client:

- Signing of the configuration files
- Configuration file encryption
- HTTPS with Tomcat and other web services

Note Secure signaling and media features require a CTL file.

A Locally Significant Certificate (LSC) installs on devices after you perform the necessary tasks that are associated with the Certificate Authority Proxy Function (CAPF). You can use Cisco Unified Communications Manager Administration to configure an LSC, as described in the *Cisco Unified Communications Manager Security Guide*.

Alternatively, you can initiate the installation of an LSC from the Settings application on the device. This Settings application also lets you update or remove an LSC.

Overview of Security Features

Implementation of security in the Cisco Unified Communications Manager system prevents identity theft of the device and Cisco Unified Communications Manager server, prevents data tampering, and prevents call-signaling and media-stream tampering.

To alleviate these threats, the Cisco IP telephony network establishes and maintains secure (encrypted) communication streams between a device and the server, digitally signs files before they are transferred to a device, and encrypts media streams and call signaling between devices.

Cisco DX Series devices use the device security profile, which defines whether the device is nonsecure or secure. For information about applying the security profile to the device, see the *Cisco Unified Communications Manager Security Guide*.

If you configure security-related settings in Cisco Unified Communications Manager Administration, the configuration file contains sensitive information. To ensure the privacy of a configuration file, you must configure it for encryption. For detailed information, see the "Encrypted Phone Configuration File Setup" chapter in the *Cisco Unified Communications Manager Security Guide*.

The following table provides an overview of the security features that the device supports.

Table 1: Overview of Security Features

Feature	Description
Image authentication	Signed binary files (with the extension .sbn) and encrypted binary files (with the extension .sebn) prevent tampering with the firmware image before the image is loaded on a device. Tampering with the image causes a device to fail the authentication process and reject the new image.
Customer-site certificate installation	Each device requires a unique certificate for device authentication. Devices include a manufacturing installed certificate (MIC), but for additional security, you can specify in Cisco Unified Communications Manager Administration that a certificate be installed through use of the Certificate Authority Proxy Function (CAPF). Alternatively, you can install a Locally Significant Certificate (LSC) from the Enterprise security menu on the device.
Device authentication	Occurs between the Cisco Unified Communications Manager server and the device when each entity accepts the certificate of the other entity. Determines whether a secure connection between the device and a Cisco Unified Communications Manager should occur; if necessary, creates a secure signaling path between the entities through TLS protocol. Cisco Unified Communications Manager does not register devices unless it can authenticate them.
File authentication	Validates digitally signed files that the device downloads. The device validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to flash memory on the device. The device rejects such files without further processing.
File encryption	Encryption prevents disclosure of sensitive information while the file is in transit to the device. In addition, the device validates the signature to make sure that file tampering did not occur after file creation. Files that fail authentication are not written to flash memory on the device. The device rejects such files without further processing.
Signaling authentication	Uses the TLS protocol to validate that no tampering to signaling packets has occurred during transmission.
Manufacturing installed certificate	Each device contains a unique manufacturing installed certificate (MIC), which is used for device authentication. The MIC provides permanent unique proof of identity for the device and allows Cisco Unified Communications Manager to authenticate the device.

Feature	Description
Media encryption	Uses SRTP to ensure that media streams between supported devices prove secure and that only the intended device receives and reads the data. Includes creation of a media master key pair for the devices, delivery of the keys to the devices, and securing the delivery of the keys while the keys are in transport.
CAPF (Certificate Authority Proxy Function)	Implements parts of the certificate generation procedure that are too processing-intensive for the device, and interacts with the device for key generation and certificate installation. The CAPF can be configured to request certificates from customer-specified certificate authorities on behalf of the device, or it can be configured to generate certificates locally.
Security profile	Defines whether the device is nonsecure, authenticated, encrypted, or protected. Other entries in this table describe security features. For more information about these features, see the *Cisco Unified Communications Manager Security Guide*.
Encrypted configuration files	Lets you ensure the privacy of device configuration files.
Optional web server disabling for a phone	For security purposes, you can prevent access to the web pages for a device (which display a variety of operational statistics for the device).
Phone hardening	Additional security options, which you control from Cisco Unified Communications Manager Administration: • Disable PC port • Disable Gratuitous ARP (GARP) • Disable PC Voice VLAN access • Provide restricted access to the web applications • Disable Bluetooth Accessory Port • Disable access to web pages for a device • Require a screen lock • Control access to Google Play™ • Control access to installation of applications from unknown sources
802.1X Authentication	The device can use 802.1X authentication to request and gain access to the network.
Secure SIP Failover for SRST	After you configure a Survivable Remote Site Telephony (SRST) reference for security and then reset the dependent devices in Cisco Unified Communications Manager Administration, the TFTP server adds the SRST certificate to the device cnf.xml file and sends the file to the device. A secure device then uses a TLS connection to interact with the SRST-enabled router.
Signaling encryption	Ensures that all SIP signaling messages that are sent between the device and the Cisco Unified Communications Manager server are encrypted.

Security Profiles

Cisco DX Series devices use a security profile, which defines whether the device is nonsecure, authenticated, or encrypted. For information about configuration of the security profile and application of the profile to the device, see the *Cisco Unified Communications Manager Security Guide*.

To view the security mode that is set for the device, view the Security menu in the Settings application.

SE Android

The Security Enhancements for Android™ (SE Android) feature enhances device security. SE Android protects against malicious applications through prevention of attempts to execute unauthorized or dangerous code on the device. SE Android does the following:

- Can prevent privilege escalation by processes
- Can prevent misuse and limit damage if privileged process, such as root, is compromised
- Provides centralized, enforced, analyzable policy
- Protects from undiscovered vulnerabilities

The device contains a policy that specifies the data that an application, process, or user can access. SE Android supports two modes:

- Permissive
- Enforcing

Anything that violates the policy is logged. If the mode is enforcing, the action is denied. No user nor administrator control exists over the policy or the mode.

Upgrades and SE Android

Upon upgrade to Release 10.2(2), Cisco DX650 remains in permissive mode because it must work with existing field units, which require a factory reset before enforcing mode can be enabled. In permissive mode, SE Android has no impact on the endpoint operation.

After a Cisco DX650 has been factory reset, the mode switches automatically to enforcing mode. This action activates SE Android protection and starts denial of actions that violate the policy.

Enforcing mode remains in effect unless the device is downgraded to a firmware release below 10.2(2). Upon upgrade to Release 10.2(2) or later, the device returns to permissive mode until factory reset is performed.

Cisco DX70 and Cisco DX80 devices are always in enforcing mode from the factory. Cisco DX70 and Cisco DX80 devices cannot be placed in permissive mode.

SE Android Troubleshooting

Policy is tuned to the expectation of what an application should be allowed to do. However, policy may prevent an operation that should be allowed. Symptoms of policy errors may include:

- Third-party or other app shows error on launch or while executing.

- App or feature works on endpoint that is in permissive mode, such as Cisco DX650, but not on a similarly configured device in enforcing mode.
- SE Android is an always-on feature and is not under administrator control. Field problems should be diagnosed and reported as defects.

Diagnose SE Android Policy Issues

Procedure

Step 1 Determine the SE Android mode:
a) From the Settings application, tap **About device** > **SELinux status**.
b) From Debugsh, enter command **show selinux status**.
If the mode is permissive, the problem is not SE Android related.

Step 2 If mode is enforcing, retest on a device that is in permissive mode.
If the problem is not reproducible in permissive mode, the problem is most likely SE Android related.

Step 3 If problem is SE Android related or cannot be determined, collect logs and report.

ADB Shell Limitations

When the endpoint is in enforcing mode, the Android Debug Bridge (adb) shell is limited. Commands such as **ls** and **ps** may not show full results.

Use debugsh commands for full results. For example, use debugsh **show process** instead of **ps** from the shell.

Enforcing mode also prevents you from freely browsing the file system, as many directories are off limits in enforcing mode.

SE Android Log Collection

To report an issue, collect this information:

- Brief description of the issue, including time of occurrence
- Screenshot of the problem if possible
- Output of debugsh **show selinux all** command
- Output of Problem Reporting Tool (PRT)

Set Up Locally Significant Certificate

Before You Begin

Make sure that the appropriate Cisco Unified Communications Manager and the Certificate Authority Proxy Function (CAPF) security configurations are complete:

- The CTL or ITL file has a CAPF certificate.

- In Cisco Unified Communications Operating System Administration, verify that the CAPF certificate is installed.
- The CAPF is running and configured.

See the *Cisco Unified Communications Manager Security Guide* for more information.

Procedure

Step 1 Obtain the CAPF authentication code that was set after the CAPF was configured.

Step 2 In the Settings application, choose **Security** > **Enterprise security settings**.

Step 3 Tap **LSC**.
The device prompts for an authentication string.

Step 4 Enter the authentication string and tap **Submit**.
The device begins to install, update, or remove the LSC, depending on how the CAPF was configured. During the procedure, a series of messages appear so you can monitor progress.

Note The LSC installation, update, or removal process can take a long time to complete. You can stop the process at any time by tapping **Cancel**.

After the installation procedure is completed successfully, the device indicates `Installed`. If the device indicates `Not Installed`, the authorization string may be incorrect or the device may not enabled for upgrade. If the CAPF operation deletes the LSC, the device indicates `Not Installed` to indicate that the operation was successful. See error messages that are generated on the CAPF server and take appropriate actions.

Note The device restarts after LSC is installed, upgraded, or deleted.

SHA-256 Manufacturing Installed Certificate

Cisco DX70 and Cisco DX80 use a manufacturing installed certificate (MIC) with the signature algorithm of SHA-256 with an RSA 2048 key. The signature algorithm requires Cisco Unified Communications Manager, Cisco Secure Access Control Server (ACS), and Secure SRST support.

The SHA-256 MIC feature has the following support requirements:

- Cisco Unified Communications Manager Release 9.1(2) and later
- ACS Release 5.2 and later.

Note ACS 5.2 and later do not support EAP-FAST with EAP-TLS inner method. Use EAP-TLS or migrate to ISE for EAP-FAST with EAP-TLS inner method.

- IOS 12.4(15)T1 and later
- Cisco Identity Service Engine release is 1.1 and later. The EAP-FAST with EAP-TLS inner method is supported starting from ISE release 1.2 and later.

The Cisco certificate authority issuing the MIC for this series of phones can be obtained from the following links if separate applications are used and these applications need to authenticate MIC from the phone:

- http://www.cisco.com/security/pki/certs/cmca2.cer
- http://www.cisco.com/security/pki/certs/crcam2.cer

These Cisco certificate authorities must be imported into applications in order for the applications to authenticate MIC for Cisco DX Series devices.

Secure Phone Calls

To implement security for Cisco DX Series devices, enable the Protected Device parameter from the **Phone Configuration** window in Cisco Unified Communications Manager Administration. When security is implemented, the presence of the Secure Call icon in the Call application indicates secure phone calls.

In a secure call, all call signaling and media streams are encrypted. A secure call offers a high level of security and provides integrity and privacy to the call. When a call in progress is being encrypted, the Security Mode status on **Enterprise security** in the Settings application indicates Encrypted.

Note If the call is routed through non-IP call legs, for example, PSTN, the call may be nonsecure even though it is encrypted within the IP network and has a lock icon associated with it.

In a secure call, a 2-second tone notifies the users when a call is encrypted and both devices are configured as protected devices, and if secure tone features are enabled on Cisco Unified Communications Manager. The tone plays for both parties when the call is answered. The tone does not play unless both devices are protected and the call occurs over encrypted media. If the system determines that the call is not encrypted, the device plays a nonsecure indication tone (6 beeps) to alert the user that the call is not protected. For a detailed description of the Secure Indication Tone feature and the configuration requirements, see the *Cisco Unified Communications Manager Security Guide*.

Note Video is transmitted as nonsecure. So, even if both devices are secure, the **Encrypted** lock icon is not displayed for video calls.

Secure Phone Call Identification

A secure call is established when a Cisco DX Series device and a device on the other end are configured for secure calling. Both devices can be in the same Cisco IP network, or on a network outside the IP network. A secure conference call is established through this process:

1. A user initiates the call from a secured device (Encrypted security mode).
2. The device indicates the Encrypted status on Enterprise security in the Settings application. This status indicates that the device is configured for secure calls, but does not mean that the other connected phone is also secured.
3. A security tone plays if the call connects to another secured device, which indicates that both ends of the conversation are encrypted and secured. Otherwise, nonsecure tone plays.

Note Secure tone plays only when it is enabled on Cisco Unified Communications Manager. If secure tone is disabled, no secure tone plays even the call is secure. For more information, see the "Secure and Nonsecure Indication Tone Setup" chapter of the *Cisco Unified Communications Manager Security Guide*.

Secure Conference Call Identification

You can initiate a secure conference call and monitor the security level of participants. A secure conference call is established through this process:

1. A user initiates the conference from a secure device.
2. Cisco Unified Communications Manager assigns a secure conference bridge to the call.
3. As participants are added, Cisco Unified Communications Manager verifies the security mode of each device and maintains the secure level for the conference.
4. The device indicates the security level of the conference call.

Note Various interactions, restrictions, and limitations affect the security level of the conference call, as determined by the security mode of the participant devices and the availability of secure conference bridges. Cisco DX Series devices support secure audio conference calls only; video will not be secure.

Call Security Interactions and Restrictions

Cisco Unified Communications Manager checks the device security status when conferences are established and changes the security indication for the conference or blocks the completion of the call to maintain integrity and security in the system. The following table provides information about changes to call security levels with the Barge feature.

Table 2: Call Security Interactions with the Barge Feature

Initiator Phone Security Level	Feature Used	Call Security Level	Results of Action
Nonsecure	Barge	Encrypted call	The call is barged and identified as nonsecure call
Secure	Barge	Encrypted call	The call is barged and identified as secure call

The following table provides information about changes to conference security levels as determined by the initiator phone security level, the security levels of participants, and the availability of secure conference bridges.

Table 3: Security Restrictions with Conference Calls

Initiator Phone Security Level	Feature Used	Security Level of Participants	Results of Action
Nonsecure	Conference	Secure	Nonsecure conference bridge Nonsecure conference
Secure	Conference	At least one member is nonsecure.	Secure conference bridge Nonsecure conference
Secure	Conference	Secure	Secure conference bridge Secure encrypted level conference
Nonsecure	Meet Me	Minimum security level is encrypted.	Initiator receives message `Does not meet Security Level, call rejected`.
Secure	Meet Me	Minimum security level is nonsecure.	Secure conference bridge Conference accepts all calls.

When secure video is in use over VPN and Cisco Virtualization Experience Client (VXC) VPN, the maximum supported bandwidth is 320 kpbs.

When the device calls Cisco TelePresence, the maximum bandwidth is 320 kbps.

Check Device Security Information Remotely

Procedure

Step 1 To check device security information remotely, the device must be, or previously have been, registered to the Cisco Unified Communications Manager server, and Web Access must be enabled on the device configuration page.

Step 2 In a web browser, go to http://<device ip>/SecurityInformation to view device security information, or http://<device ip>/SecurityInformationX to view device security information in an XML format.

Encryption for Barge

A user cannot barge into an encrypted call if the device that is used to barge is not configured for encryption. When barge fails in this case, a reorder (fast busy) tone plays on the device on which the barge was initiated.

If the initiator device is configured for encryption, the barge initiator can barge into a nonsecure call from the encrypted device. After the barge occurs, Cisco Unified Communications Manager classifies the call as nonsecure.

If the initiator device is configured for encryption, the barge initiator can barge into an encrypted call, and the device indicates that the call is encrypted.

802.1X Authentication Support

Cisco DX Series devices and Cisco Catalyst switches traditionally use Cisco Discovery Protocol (CDP) to identify each other and determine parameters such as VLAN allocation and inline power requirements. CDP does not identify locally attached workstations. Cisco DX Series devices provide an EAPOL pass-through mechanism. This mechanism allows a workstation that is attached to the device to pass EAPOL messages to the 802.1X authenticator at the LAN switch. The pass-through mechanism ensures that the device does not act as the LAN switch to authenticate a data endpoint before the device accesses the network.

Cisco DX Series devices also provide a proxy EAPOL Logoff mechanism. In the event that the locally attached PC disconnects from the device, the LAN switch does not see the physical link fail, because the link between the LAN switch and the device is maintained. To maintain network integrity, the device sends an EAPOL-Logoff message to the switch on behalf of the downstream PC, which triggers the LAN switch to clear the authentication entry for the downstream PC.

Cisco DX Series devices also contain an 802.1X supplicant. This supplicant allows network administrators to control the connectivity of devices to the LAN switch ports. The current release of the device 802.1X supplicant uses the EAP-FAST and EAP-TLS options for network authentication.

Required Network Components

Support for 802.1X authentication on Cisco DX Series devices requires several components. These include:

- The device itself, which acts as the 802.1X supplicant, which initiates the request to access the network.
- Cisco Secure Access Control Server (ACS) (or other third-party authentication server). The authentication server must be configured with a shared secret that authenticates the device.
- Cisco Catalyst Switch (or other third-party switch). The switch must support 802.1X, so it can act as the authenticator and pass the messages between the device and the authentication server. After the exchange completes, the switch grants or denies the device access to the network.

Best Practices

The following list describes requirements and recommendations for 802.1X configuration.

- Enable 802.1X Authentication: If you want to use the 802.1X standard to authenticate Cisco DX Series devices, be sure that you properly configure the other components before you enable authentication on the device.
- Configure PC Port: The 802.1X standard does not take into account the use of VLANs and thus recommends that only a single device should be authenticated to a specific switch port. However, some switches (including Cisco Catalyst switches) support multidomain authentication. The switch configuration determines whether you can connect a PC to the PC port of the device.
    - Enabled: If you are using a switch that supports multidomain authentication, you can enable the PC port and connect a PC to it. In this case, the devices support proxy EAPOL-Logoff to monitor the authentication exchanges between the switch and the attached PC. For more information about

IEEE 802.1X support on the Cisco Catalyst switches, see the Cisco Catalyst switch configuration guides at:

http://www.cisco.com/c/en/us/support/switches/catalyst-6500-series-switches/tsd-products-support-series-home.html

- Disabled: If the switch does not support multiple 802.1X-compliant devices on the same port, you should disable the PC Port when 802.1X authentication is enabled. If you do not disable this port and subsequently attempt to attach a PC to it, the switch denies network access to both the device and the PC.

- Configure Voice VLAN: Because the 802.1X standard does not account for VLANs, you should configure this setting based on the switch support.
  - Enabled: If you are using a switch that supports multidomain authentication, you can continue to use the voice VLAN.
  - Disabled: If the switch does not support multidomain authentication, disable the Voice VLAN and consider assignment of the port to the native VLAN.

Screen Lock and Automatic Lock Setup

The Screen Lock Timeout value controls the normal device idle timeout when the screen turns off and the screen lock is activated. The variable is configurable within a range of 1 to 60 minutes.

The Automatic Lock controls how long the display will stay on before it dims or goes off. If the device is in the Always On mode, the device will dim. If the device is in the Nightlight mode, it will turn off completely. The Automatic Lock value can be configured to a maximum value of 10 minutes. To configure the Automatic Lock value, go to **Settings** > **Security** > **Automatically lock**.

The following table shows the relationship of the Screen Lock Timeout value and Automatic Lock value.

Table 4: Screen Lock Timeout and Automatic Lock Value Relationship

Condition	Outcome
Screen Lock Timeout value is lower than Automatic Lock value	When the Screen Lock Timeout value is reached, screen stays at full brightness; locked screen displays.
Automatic Lock value is lower than Screen Lock Timeout value	When the Automatic Lock value is reached, two outcomes are possible: • If the device is in Always On mode, the device dims when the Automatic Lock value is reached. When the Screen Lock Timeout value is reached, the device locks and remains dimmed. • If the device is in Nightlight mode, the device locks and turns off when the Automatic Lock value is reached. When the Screen Lock Timeout value is reached, no additional changes occur.

Condition	Outcome
Screen Lock Timeout value the same as the Automatic Lock value	When the value is reached, screen stays at full brightness; locked screen displays.

Set Up Screen Unlock/Password Reset

This feature allows the user to reset the PIN/password that is used to unlock the screen. The user can reset the PIN/password through use of Cisco Unified Communications Manager or configured Google™ account credentials. Use the following procedure to reset the PIN/password with Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.

Step 2 Click **Add New**.

Step 3 Enter required user information.

Step 4 In the **Device Information** window, choose the device with which you want to associate the user.

Step 5 Click **Save**.

Step 6 In the **Permissions Information** window, assign the user Cisco Unified Communications Manager Administration permissions.

Step 7 In the **Permissions Information** window, choose **Standard CCM End Users**.

Step 8 Click **Save** and **Apply Config**. After the device reregisters, the user is configured to the device.