ECDSA Support for Common Criteria Certified Solutions

ECDSA Support for Common Criteria for Certified Solutions

Unified Communications Manager supports Elliptic Curve Digital Signature Algorithm (ECDSA) certificates. These certificates are stronger than the RSA-based certificates and are required for products that have Common Criteria (CC) certifications. The US government Commercial Solutions for Classified Systems (CSfC) program requires the CC certification and so, it is included in Unified Communications Manager.

The ECDSA certificates are available along with the existing RSA certificates in the following areas—Certificate Manager, SIP, Certificate Authority Proxy Function (CAPF), Transport Layer Security (TLS) Tracing, Entropy, HTTP, and computer telephony integration (CTI) Manager.

Note ECDSA is supported only for Unified Communications Manager and Tomcat.

Certificate Manager ECDSA Support

In Unified Communications Manager Release 11.0, the certificate manager supports both generation of self-signed ECDSA certificates and the ECDSA certificate signing request (CSR). Earlier releases of Unified Communications Manager supported **RSA** certificate only. However, Unified Communications Manager Release 11.0 onwards, **CallManager-ECDSA** certificate has been added along with the existing **RSA** certificate.

Both the **CallManager** and **CallManager-ECDSA** certificates share the common certificate trust store—CallManager-Trust. Unified Communications Manager uploads these certificates to this trust store.

The certificate manager supports generation of ECDSA certificates having different values of key length.

When you update or install Unified Communications Manager, the self-signed certificate is generated. Unified Communications Manager Release 11.0 always has an ECDSA certificate and uses that certificate in its SIP interface. The secure Computer Telephony Integration (CTI) Manager interface also supports ECDSA certificates. As both the CTI Manager and SIP server use the same server certificate, both the interfaces work in synchronization.

SIP ECDSA Support

Unified Communications Manager Release 11.0 includes ECDSA support for SIP lines and SIP trunk interfaces. The connection between Unified Communications Manager and an endpoint phone or video device is a SIP line connection whereas the connection between two Unified Communications Managers is a SIP trunk connection. All SIP connections support the ECDSA ciphers and use ECDSA certificates.

Following are the scenarios when SIP makes (Transport Layer Security) TLS connections:

- When SIP acts as a TLS server—When the SIP trunk interface of Unified Communications Manager acts as a TLS server for incoming secure SIP connection, the SIP trunk interface determines if the CallManager-ECDSA certificate exists on disk. If the certificate exists on the disk, the SIP trunk interface uses the CallManager-ECDSA certificate if the selected cipher suite is **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** or **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**. The SIP trunk interface continues to support RSA TLS cipher suites for connections from clients that do not support ECDSA cipher suites. The **TLS Ciphers** drop-down list contains options that permit configuration of the supported cipher suites when Unified Communications Manager acts as a TLS server.
- When SIP acts as a TLS client—When the SIP trunk interface acts as a TLS client, the SIP trunk interface sends a list of requested cipher suites to the server based on the **TLS Ciphers** field (which also includes the **ECDSA ciphers** option) in the **Enterprise Parameters** window of Cisco Unified Communications Manager. The **TLS Ciphers**. This configuration determines the TLS client cipher suite list and the supported cipher suites in order of preference.

Note If you establish a TLS connection with an earlier release of the Unified Communications Manager that does not support ECDSA client certificate, the connection uses an RSA cipher suite. The client certificate sent in the TLS connection is not bound to the TLS Cipher you that you choose. Earlier releases of Unified Communications Manager also support that TLS servers receive and handle ECDSA client certificates.

Devices that use an ECDSA cipher to make a connection to Unified Communications Manager must have the CallManager-ECDSA certificate in their Identity Trust List (ITL) file. Then, the devices must incorporate the CallManager-ECDSA certificate into their local certificate store to trust the connection that is secured by the CallManager-ECDSA certificate.

CAPF ECDSA Support

Certificate Authority Proxy Function (CAPF) is a Cisco proprietary method for exchanging certificates between Cisco endpoints and Unified Communications Manager. Only Cisco endpoints use CAPF. To accomplish common criteria requirements, CAPF is updated to CAPF version 3 so that a client can be provided with ECDSA Locally Significant Certificate (LSC). A customer creates LSC locally. An LSC is an alternative to manufacturer installed certificate (MIC) that the manufacturer creates.

Use CAPF version 3 to allow Unified Communications Manager server to direct phone, CTI applications, and Jabber clients to generate EC keys to be used in their LSCs. After the EC Keys are generated, Unified Communications Manager either generates an ECDSA LSC and sends it to the Cisco endpoint or generates an ECDSA CSR.

In case the endpoint does not have CAPF version 3 support, you can configure the required EC key size and RSA key size and choose **EC Key Preferred, RSA Backup** option in **Phone Configuration** window from Cisco Unified CM Administration as a backup. This backup option is useful when CAPF server tries to send a request to EC key pair and the phone communicates to the server that it does not support EC key, the server sends the request to generate an RSA key pair instead of the EC key pair.

Note If Cisco endpoint supports CAPF version 3, and you choose **EC Preferred, RSA Backup** option in **Phone Configuration** without enabling **Endpoint Advanced Encryption Algorithm Support** parameter, then the ECDSA or RSA-based LSCs are not issued. If Cisco endpoint does not support CAPF version 3, and you enable or disable **Endpoint Advanced Encryption Algorithm Support** parameter then the RSA-based LSCs are issued.

Note The **Endpoint Advanced Encryption Algorithms Support** parameter indicates that phones download the TFTP configuration files using advanced TLS ciphers. By default, EC ciphers have the highest priority. This solution is only supported for an on-premises deployment without MRA.

Entropy

To have strong encryption, a robust source of entropy is required. Entropy is a measure of randomness of data and helps in determining the minimum threshold for common criteria requirements. Data conversion techniques, such as cryptography and encryption, rely on a good source of entropy for their effectiveness. If a strong encryption algorithm, such as ECDSA, uses a weak source of entropy, the encryption can be easily broken.

In Unified Communications Manager Release 11.0, the entropy source for Unified Communications Manager is improved. Entropy Monitoring Daemon is a built-in feature that does not require configuration. However, you can turn it off through the Unified Communications Manager CLI.

Use the following CLI commands to control the `Entropy Monitoring Daemon` service:

CLI Command	Description
utils service start Entropy Monitoring Daemon	Starts the `Entropy Monitoring Daemon` service.
utils service stop Entropy Monitoring Daemon	Stops the `Entropy Monitoring Daemon` service.
utils service active Entropy Monitoring Daemon	Activates the `Entropy Monitoring Daemon` service, which further loads the kernel module.
utils service deactive Entropy Monitoring Daemon	Deactivates the `Entropy Monitoring Daemon` service, which further unloads the kernel module.

HTTPS Support for Configuration Download

For secure configuration download, Unified Communications Manager Release 11.0 is enhanced to support HTTPS in addition to the HTTP and TFTP interfaces that were used in the earlier releases. Both client and server use mutual authentication, if required. Clients that are enrolled with ECDSA LSCs and Encrypted TFTP configurations are required to present their LSC.

The HTTPS interface uses both the CallManager and the CallManager-ECDSA certificates as the server certificates.

Note When you update CallManager, CallManager ECDSA, or Tomcat certificates, you must deactivate and reactivate the TFTP service. Port 6971 is used for authentication of the CallManager and CallManager-ECDSA certificates whereas port 6972 is used for the authentication of the Tomcat certificates.

CTI Manager Support

The computer telephony integration (CTI) interface is enhanced to support four new ciphers. The ciphers suites are **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256**, **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384**, **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** and **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384**. By supporting these cipher suites, the CTI Manager interface needs to have the **CallManager-ECDSA** certificate, if it exists in Unified Communications Manager. Similar to the SIP interface, the Enterprise Parameter **TLS Ciphers** option in Unified Communications Manager is used to configure the TLS ciphers that are supported on the CTI Manager secure interface.