Solution Security

- Security, on page 1
- Transport Layer Security, on page 2
- Cross-Origin Resource Sharing (CORS), on page 3
- Gadget Source Allowed List, on page 3
- Secure Real-Time Protocol (Secure RTP or SRTP), on page 3
- Federal Information Processing Standards 140-2 Level 1, on page 4

Security

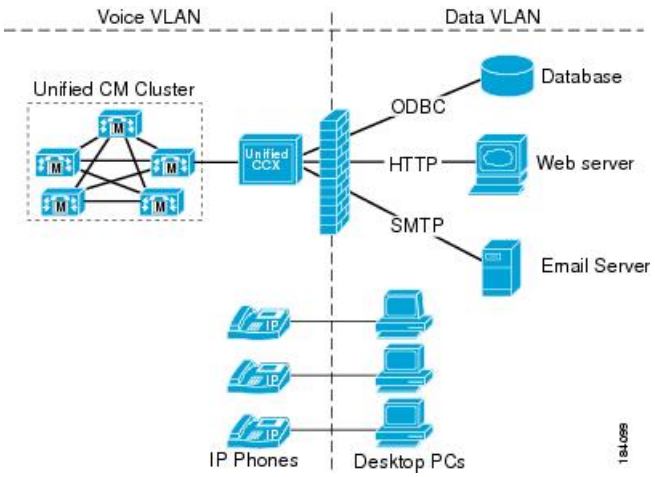
Security can be implemented on many levels. Applications security is dependent upon security implemented at the infrastructure level. For more details on security at the network infrastructure level, refer to the security design considerations in the *Cisco IP Telephony Solution Reference Network Design* documentation, available here:

http://www.cisco.com/warp/public/779/largeent/it/ese/srnd.html

Corporate Data Access

In addition to call routing, Unified CCX or Cisco Unified IP IVR scripts often process enterprise data from existing corporate data stores such as a database or a corporate directory server for functions such as account authentication and order status. These data stores often already exist and share data with other enterprise applications. This figure shows an example of a network where voice and data components reside in separate VLANs and are separated by a firewall.

Figure 1: Unified CCX Accessing Data Stores



Unified CCX can communicate with these external sources through its subsystems, provided that Network Address Translation (NAT) is not used.

SSL HTTPS Connection

The certificates uploaded using the Cisco Unified OS Administration interface to the Tomcat trust store is available to secure all HTTP connections made during script execution. The following can be secured:

- Document steps
- VoiceXML script
- Custom java code that provides web services

Enhanced Security API (ESAPI)

A new security filter is added to the Application Administration component. This filter identifies malicious user input and protects the application against XSS attacks.

If the Application Administration users find any user activity that was allowed earlier is now blocked by the security filter, then disable the security filter using a CLI command.

Transport Layer Security

The Cisco Unified Contact Centre Express supports the TLS version 1.2. The following command line interface commands can be used to show and set the TLS minimum version in the server and the client applications:

- show tls server min-version
- show tls client min-version
- set tls server min-version
- set tls client min-version

Note

- You must relaunch Cisco Unified CCX Editor and Cisco Unified Real-Time Monitoring Tool after the upgrade of Unified CCX.
- Ensure that the Unified CCX server and the client application is restarted for the changes to take effect.

Cross-Origin Resource Sharing (CORS)

Finesse supports CORS requests and allows the customization of the domains which are allowed to make CORS requests to the Finesse desktop. Once CORS is enabled via the CLI **utils finesse cors enable**, the CORS origin request from external domains is blocked by the browser. To enable specific domains to access Finesse desktop via CORS, the domains need to be added to the CORS origin allowed list using the CLI **utils finesse cors allowed_origin add**. For more information on the CORS CLIs, see *Cisco Finesse CLI*.

Gadget Source Allowed List

Shindig proxies requests from the Finesse desktop to external servers and this introduces the possibility of server side request forgery (SSRF). To prevent SSRF, you can choose to restrict outgoing connections requested by the gadgets to specific URIs by enabling shindig allowed list CLIs and adding the required URIs to the allowed list. For more information on Gadget Source Allowed List CLIs, see *Cisco Finesse CLIs*.

Secure Real-Time Protocol (Secure RTP or SRTP)

Secure Real-Time Transport Protocol (SRTP) provides authentication and encryption to secure privacy and confidentiality for voice conversation and other media. It also provides protection against replay attacks. Signaling authentication validates that no tampering has occurred to signaling packets during transmission. The confidentiality of the media is protected with cryptographic procedures as defined in IETF RFC 3711.

Voice security feature supports the following capabilities between voice gateway and IP phones:

- Media encryption and authentication of voice RTP streams using SRTP.
- Exchange of RTP Control Protocol (RTCP) information using SRTP.
- SRTP to RTP fallback for calls between secure and non-secure endpoints.
- When SRTP is enabled, a secure JTAPI connection is established between the following subsystems and Unified CM:
  - Unified CM Telephony
  - RmCm

SRTP Considerations

Before enabling SRTP in your Unified CCX deployment, ensure the following points:

- Voice gateway or the router is secure.
- SIP trunks between CUCM and voice gateway are secure.
- Cluster Security Mode is set to Mixed mode in CUCM.
- CUCM AXL Webservice is running on CUCM AXL Service Provider node.
- CAPF service is running on CUCM Publisher and it is accessible.
- None of the certificates are expired on any of the CUCM nodes.
- Unified CCX Engine is running on all Unified CCX nodes.
- The **Access Control Groups** in CUCM, **Standard CTI Allow Reception of SRTP Key Material** and **Standard CTI Secure Connection** is associated with the application user.
- Agent and Supervisor phones are secure. Supervisors phones must be secure to monitor the agents phones.
- Refer to the Unified CCX Compatibility Matrix for CUCM version that is supported for SRTP.

When SRTP is enabled in FIPS 140-2 mode, if you perform a Unified CCX DRF restore, ensure to re-sync JTAPI and restart Unified CCX Engine on all the nodes.

Note The media leg between Unified CCX and gateway uses SRTP. However, media leg between Unified CCX and Nuance Speech server uses RTP.

SRTP is not applicable for Home Agents with Extend and Connect.

For more information on how to enable SRTP, see *System Parameters* section in *Cisco Unified Contact Center Express Administration and Operations Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

Federal Information Processing Standards 140-2 Level 1

Federal Information Processing Standards (FIPS) 140-2 Level 1 is a U.S. and Canadian government certification standard that defines minimum security requirements for cryptographic modules protecting sensitive information in computer and telecommunications systems. It also defines algorithms that are allowed to be used to encrypt sensitive information. These strictly defined requirements are important for government agencies, hospitals, and other customers, who would require a higher level of security.

Use CLI to enable or disable FIPS 140-2 mode on Unified CCX.

Caution FIPS 140-2 mode is supported only on releases that have been through FIPS compliance.

FIPS 140-2 Level 1 Considerations

For using FIPS 140-2 mode, consider the following points:

- Backup the system before and after enabling FIPS 140-2 mode.

- Ensure that SRTP is disabled before enabling or disabling FIPS 140-2 mode in Unified CCX. You can enable SRTP after enabling or disabling FIPS 140-2 mode in Unified CCX.
- If you upgrade Unified CM when SRTP is enabled in FIPS 140-2 mode, you must resync JTAPI and restart Unified CCX Engine on all the nodes after completing the upgrade.

Note For more information about SRTP, see the previous section in this chapter.

- After enabling or disabling FIPS 140-2 mode, the existing application certificates are re-generated.
  - For third-party CA issued Tomcat certificate:
    - Upload the re-signed certificate to Unified CCX server.
    - Upload the CA root certificate of Unified CCX to CCP.
  - For third-party CA issued IPsec certificates, re-sign the certificates and upload them to the respective nodes.
  - For Self-Signed certificates, you must upload the newly generated Unified CCX certificate to CCP.
- After enabling FIPS 140-2 mode, you may not be able to access any of the Unified CCX applications due to HTTP Strict Transport Security (HSTS) settings in the browser. To add the HSTS exception and access the Unified CCX applications, please refer to the respective browser documentation.
- Ensure that FIPS 140-2 mode is disabled before registering or unregistering Cloud Connect services. You can enable FIPS 140-2 mode after registering or unregistering Cloud Connect services.

For more information on how to enable and disable FIPS 140-2 mode, see *utils fips* section in *Cisco Unified Contact Center Express Administration and Operations Guide* available at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-maintenance-guides-list.html.

FIPS 140-2 Mode Restrictions

Communication with the following interfaces will not operate in FIPS 140-2 mode:

Table 1: FIPS 140-2 Mode Restrictions

Interface	Restrictions
SNMP v3	FIPS mode does not support SNMP v3 with MD5 or DES. When FIPS 140-2 mode is enabled, if you have SNMP v3 configured, you must configure **SHA** as the Authentication Protocol and **AES128** as the Privacy Protocol.
External Database through Unified CCX Scripts	Communication with external database by using Unified CCX engine DB Steps.
CTI Client	Communication with third-party CTI clients.

Interface	Restrictions
Unified CCX Notification Client	Communication to Cisco Unified CCX Notification Service through 5223 or 7443 ports.
Email through Unified CCX Scripts	Email server communication by using scripts with eMail steps.
ASR/TTS	Communication with ASR and TTS Servers.

Supported Ciphers

Cisco Tomcat

The applications **Cisco Unified CCX Administration**, **Cisco Unified Serviceability**, **Cisco Unified CCX Serviceability**, **Cisco Unified OS Administration**, and **Disaster Recovery System** use Cisco Tomcat.

The following are the Ciphers that are supported in FIPS mode:

- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048)`
- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048)`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)`
- `TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)`
- `TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)`

The following are the Ciphers that are supported in Non-FIPS mode:

- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024)`
- `TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 1024)`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)`
- `TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)`
- `TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)`

Cisco Finesse Tomcat, Cisco Identity Service, and Cisco Unified Intelligence Center Reporting Service

All the following Ciphers are supported in both FIPS and Non-FIPS Mode:

- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1)`
- `TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1)`

- TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048)