Solution Security

Security

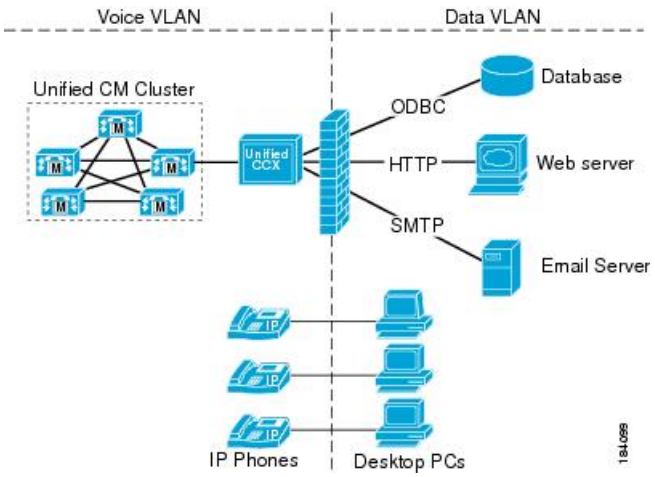
Security can be implemented on many levels. Applications security is dependent upon security implemented at the infrastructure level. For more details on security at the network infrastructure level, refer to the security design considerations in the *Cisco IP Telephony Solution Reference Network Design*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

Data Transfer to Customer Journey Analyzer

Data is transferred or published to Customer Journey Analyzer over a secure HTTPS connection.

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 reinstall 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 whitelist using the CLI **utils finesse cors allowed_origin add**. For more information on the CORS CLIs, see *Cisco Finesse CLIs*.

Gadget Source Whitelisting

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 whitelisting CLIs and adding the required URIs to the whitelist. For more information on Gadget Source Whitelisting CLIs, see *Cisco Finesse CLIs*.