Configurations

Security Configurations

This chapter provides end to end security solutions and references to various security task flows and their brief descriptions.

Table 1: Security Configurations

Steps	Procedure	Description
Step 1	Generate Certificates	Configure and exchange certificates for your system.
Step 2	Configure Certificate Monitoring and Revocation	Configure the system to monitor certificate expiry and to revoke certificates automatically through the Online Certificate Status Protocol (OCSP).
Step 3	Enable Mixed Mode	When mixed mode is enabled, your system uses the Certificate Trust List (CTL) file for security if you're deploying Cisco Unified IP Phone, TelePresence Endpoints, or Jabber without OAuth.
Step 4	Configure Certificate Authority Proxy Function (CAPF)	Configure CAPF to generate LSC certificates for phones.
Step 5	Configure Encrypted TFTP	Configure encrypted TFTP so that the initial phone configuration file sent to the phone is encrypted.
Step 6	Configure Phone Security	Configure Phone Security profiles to include items like TFTP encryption and TLS signaling for your phones.
Step 7	Configure Phone Hardening	Configure optional product-specific configurations to harden the connection to the phone.
Step 8	Configure Secure Trunks	Configure secure trunks to enable TLS and digest authentication on trunks.

Steps	Procedure	Description
Step 9	Enable SIP on Trunks	Configure SIP Trunk for SRTP.
Step 10	Enable SAML SSO	Configure your Identity Management Framework. SAML SSO is recommended for Identity Management. However, you can also use LDAP Authentication or Local authentication.
Step 11	Configure User Access	Assign end users to access control groups to contain roles and access privileges that they need.
Step 12	Configure Credential Policies	Configure default credential policies for user passwords, user PINs, and application user passwords.
Step 13	Configure Contact Search Authentication	Ensure authentication of all directory searches to secure the company directory.
Step 14	Enable TLS	Configure TLS signaling through Phone Security and Trunk Security Profiles.
Step 15	Configure Cipher Management	Customize the list of encryption ciphers that are supported on your system.
Step 16	Configure IPSec Policies	Configure IPSec Policies for your system.
Step 17	Configure Gateway Security	Configure secure gateway for your system.
Step 18	Configure OS Hardening	Configure OS Hardening.
Step 19	Configure FIPS	Configure FIPS mode, Enhanced Security Mode, and Common Criteria Mode to meet compliance guidelines around encryption and data security.
Step 20	Configure Security Features	Configure optional security features, such as: • Secure Monitoring and Recording • Secure Conferencing • Secure Tones and Icons • V.150 • Mobile and Remote Access • AS-SIP