Encryption Support

User and Agent Passwords

When Single Sign-On (SSO) is enabled, it hands off the Agent and Supervisor authentications to a third party Identity Provider (IDP). In such a case, the Agent and Supervisor passwords are not stored in the Unified CCE database.

When SSO is not enabled, the Agent and Supervisor passwords are stored in the configuration database with an MD5 hash. Unified CCE has mechanisms to protect data in transit, and options for protecting data at rest.

Administrator and Configuration user login uses credentials that are stored in Active Directory. These passwords are not stored in the Unified CCE database. The exception is System Inventory, which allows centralized configuration and management of Unified CCE services from a central location via CCE Administration web page. System Inventory requires credentials to manage and get diagnostic information from other sub-systems in the Unified CCE Solution. These passwords are stored with AES 256-bit encryption in the AW database.

CCE Admin web page users are authenticated using the Active Directory credentials.

CUIC reporting users can either use SSO or AD credentials to log on depending on whether SSO is enabled or not. If SSO is not enabled, then Supervisor reporting users use Active Directory authentication to gain access to reporting, and not the local MD5 password stored in the configuration database.

Note Unified CCE cannot read, set, or change user passwords in Active Directory. It is possible and likely that the Supervisor reporting users may use a password (their AD password) to login to CUIC that is different from their agent password set by the configuration administrator.

Call Variables and Extended Call Variables

To protect data sent in call variables or expanded call context (ECC) variables, Unified ICM relies on IPsec and the deployment of IPsec policies between servers running Windows Server 2012 R2.

In a contact center enterprise environment, the establishment of an IPsec channel between the Cisco Unified Communications Manager (Unified CM) and the Peripheral Gateway is also supported. Use SHA-256 as your integrity algorithm and AES with a minimum 256-bit key as your encryption algorithm. For the Internet Key Exchange (IKE) security algorithm, use a minimum of Diffie-Hellman Group 2 for a 2048-bit key.

Internet Script Editor

Unified CCE supports the encryption of traffic for users accessing the Internet Script Editor and Web Setup applications. The traffic encryption protects all user sign-ins and optionally session traffic done from a remote machine from snooping.

Note If you use Unified Contact Center Management Portal (Unified CCMP) or Unified Contact Center Domain Manager (Unified CCDM), you cannot use Transport Layer Security (TLS) v1.0 for Internet Script Editor.

The Internet Script Editor web application uses the TLS v1.2 protocol only which provides encryption using a cipher that the endpoints negotiate. All supervisor sign-ins, user sign-ins, and data exchanged is protected across the network.

For more information about enabling certain Cipher Suites in IIS, see the article https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings.

Related Topics

Cisco SSL Encryption Utility

Cisco Contact Center SNMP Management Service

Unified ICM and Unified CCE include a Simple Network Management Protocol (SNMP v3) agent to support authentication and encryption (privacy) provided by *SNMP Research International.* Our implementation exposes the configuration of the communication with a management station to be authenticated using the SHA-256 digest algorithms. For all SNMP message encryption, our implementation uses one of the following protocols:

- AES-192
- AES-256

For more information, see the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html.

Additional Encryption

In addition to the encryption in the contact center applications, Cisco supports the deployment of the solution across sites running Cisco IOS IPsec in Tunnel Mode with HMAC-SHA1 Authentication (ESP-SHA-HMAC) and 3DES Encryption (ESP-3DES).

Related Topics

IPsec and NAT Support

Unsupported Ciphers

Ciphers become obsolete as encryption algorithms advance. The following ciphers are not supported for use with contact center enterprise solutions:

- DES 56/56
- RC2 128/128
- RC2 40/128
- RC2 56/128
- RC4 128/128
- RC4 40/128
- RC4 56/128
- RC4 64/128
- Triple DES 168/168
- NULL