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

Call context variables in Unified CCE may contain sensitive data depending on how it is configured and scripted in your system Peripheral. Variables between 1 to10 are stored in the Termination Call Detail records, and the Expanded Call Context (ECC) variables are stored in the Termination Call Variable and Router Call Variable records on the Historical Data Server (HDS), if the **Persistent** check box is checked.

These variables are neither encrypted in the memory nor when they are stored in the database. Therefore, be cautious about the data you store in these variables. These variables are typically used for diagnostics and custom reporting only.

Unified CCE has strategies for encrypting the variables during transport and encrypting the drive where they are stored.

For more information, see About IPsec and Manage Secured PII in Transit.

Internet Script Editor

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

Unified CCE Certificate Management Utilities

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.

TLS Encryption Support

External interfaces such as data center interfaces and external components such as Cisco Finesse, Customer Collaboration Platform, CVP, and Application Gateways support encryption using TLS.

Supported Ciphers

The following AES ciphers are used for encryption:

- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

Note This is a mandatory cipher. It's required to support TLS access.

- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA384

Note This is a mandatory cipher. It's required to support TLS access.

- AES128-GCM-SHA256
- AES256-GCM-SHA384
- AES128-SHA256
- AES128-SHA
- AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Cipher Suite Management

You can add or remove the supported ciphers from the following registries for the server and client respectively:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\Cisco SSL
Configuration\ServerCiphers

HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\Cisco SSL
Configuration\ClientCiphers
```