Encryption Support

- User and Agent Passwords, page 1
- Call Variables and Extended Call Variables, page 1
- Internet Script Editor and Agent Re-Skilling, page 1
- CTI OS C++/COM Toolkit, page 2
- Cisco Contact Center SNMP Management Service, page 2
- Additional Encryption, page 3

User and Agent Passwords

Unified ICM/Unified CCE systems are highly distributed applications composed of many node and server applications. The system stores application user and contact center agent passwords in the Logger and the Distributor databases as an RSA Data Security, Inc. MD5 Message-Digest Algorithm hash. When passed from one server node to another, such as from a PG to a Router, The system passes the passwords as MD5 hashes.

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 2008 R2. In a Unified CCE environment, the establishment of an IPsec channel between the Cisco Unified Communications Manager (Unified CM) and the Peripheral Gateway is also supported. Use SHA-1 as your integrity algorithm and 3DES as your encryption algorithm. For the Internet Key Exchange (IKE) security algorithm, use at least a minimum of Diffie-Hellman Group 2 for a 1024-bit key or 2048-bit key if processing power allows it.

Internet Script Editor and Agent Re-Skilling

Unified ICM supports, as a default on Windows Server 2008 R2, the encryption of traffic for users accessing the Unified ICM Internet Script Editor, Web Setup, and Agent Re-skilling applications so that all user logins and optionally session traffic done from a remote machine are protected from snooping. The applications that implement the Transport Layer Security (TLS) v1.0 protocol using the Open SSL libraries are HTTP-based.
The Agent Re-skilling and Internet Script Editor web applications are deployed and enabled for 128-bit SSL encryption in IIS 7 as a default. All supervisor logins, user logins, and data exchanged is protected across the network.

For more information about enabling certain Cipher Suites in IIS, see the article KB 245030.

Related Topics

Cisco SSL Encryption Utility

CTI OS C++/COM Toolkit

The CTI OS (C++/COM toolkit) and CAD agent desktops implement TLS v1.0 protocol using the OpenSSL libraries to protect data exchanged between the agent desktop to the CTI Object Server. A Cipher suite is used for authentication, key exchange, and stream encryption. The Cipher suite is as follows:

- Key exchange: Diffie–Hellman
- Authentication: RSA
- Encryption: AES (128)
- Message digest algorithm: SHA1

When you enable CTI OS Security, agent capacity decreases by 25%.

Important


Cisco Contact Center SNMP Management Service

Unified ICM/Unified CCE includes a Simple Network Management Protocol (SNMP v3) agent to support authentication and encryption (privacy) provided by SNMP Research International. The Cisco implementation exposes the configuration of the communication with a management station to be authenticated using the SHA-1 digest algorithms. For all SNMP messages to be encrypted, the Cisco implementation uses one of the following three protocols:

- 3DES
- AES-192
- AES-256

Additional Encryption

In addition to the application-level encryption provided in the Unified ICM suite of 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