# 暗号化のサポート


- ユーザとエージェントのパスワード （1 ページ）
- コール変数と拡張コール変数 （2 ページ）
- Internet Script Editor （2 ページ）
- Cisco Contact Center の SNMP 管理サービス （2 ページ）
- TLS 暗号化のサポート （3 ページ）


## ユーザとエージェントのパスワード

シングルサインオン（SSO）が有効の場合、エージェントとスーパーバイザの認証をサードパーティのアイデンティティ プロバイダー（IDP）に渡します。このような場合、エージェントパスワードとスーパーバイザパスワードは Unified CCE データベースに保存されません。

SSO が有効になっていない場合、エージェントパスワードとスーパーバイザパスワードは SHA-256 ハッシュを含む設定データベースに保存されます。Unified CCE には、転送中のデータを保護するメカニズムと、保存中のデータを保護するためのオプションがあります。

管理者ユーザと設定ユーザのログインでは、Active Directory に保存されているログイン情報を使用します。これらのパスワードは、Unified CCE データベースには保存されません。例外として、システムインベントリは CCE 管理 Web ページを介して、中央の場所から Unified CCE サービスの中央の設定と管理を可能にするシステムインベントリです。システムインベントリでは、Unified CCE ソリューション内の他のサブシステムを管理し、診断情報を取得するためのログイン情報が必要です。これらのパスワードは、AW データベースに AES 256 ビット暗号化で保存されます。

CCE 管理 Web ページのユーザは、Active Directory のログイン情報を使用して認証されます。

CUIC レポート ユーザは、SSO が有効かどうかに応じて、SSO または AD のログイン情報を使用してログインできます。SSO が有効になっていない場合、スーパーバイザ レポート ユーザは Active Directory 認証を使用してレポートにアクセスし、設定データベースに保存されているローカルの SHA-256 パスワードにはアクセスしません。

（注） Unified CCE では、Active Directory のユーザパスワードの読み取り、設定、または変更ができません。スーパーバイザ レポート ユーザが、設定管理者が設定したエージェントパスワードとは異なる CUIC にログインするために、パスワード（AD パスワード）を使用する可能性があります。

# コール変数と拡張コール変数

Unified CCE のコールコンテキスト変数には、システム周辺機器内の設定とスクリプトの方法に応じて、センシティブデータが含まれている場合があります。終話コール詳細レコードに 1 ~10 の変数が格納され、**[永続（Persistent）]** チェックボックスがオンの場合、拡張コールコンテキスト（ECC）変数は、履歴データサーバ（HDS）の終端コール変数およびルータコール変数のレコードに保存されます。

これらの変数は、メモリ内でも、データベースに保存されている場合でも暗号化されません。したがって、これらの変数に保存するデータについては慎重にしてください。これらの変数は通常、診断とカスタムレポートにのみ使用されます。

Unified CCE は、トランスポート中に変数を暗号化し、格納されているドライブを暗号化するための戦略を持っています。

詳細については、「IPSec の概要」および「転送中の安全な PII」を参照してください。

# Internet Script Editor

インターネット スクリプト エディタ Web アプリケーションは、TLS v1.2 プロトコルのみを使用し、エンドポイントがネゴシエートする暗号を使用して暗号化を行います。スーパーバイザのサインイン、ユーザのサインイン、および交換されたデータは、ネットワーク全体で保護されます。

IIS 内の特定の暗号スイートの有効化の詳細については、https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings にある項目を参照してください。

**関連トピック**

CCE 証明書管理ユーティリティ

# Cisco Contact Center の SNMP 管理サービス

Unified ICM と Unified CCE には、*SNMP* リサーチ インターナショナルによって提供される認証と暗号化（プライバシー）をサポートする簡易ネットワーク管理プロトコル（SNMP v3）エージェントが含まれます。この実装では、管理ステーションとの通信の設定を、SHA-256 ダイジェストアルゴリズムを使用して認証されます。すべての SNMP メッセージの暗号化に対して、この実装では次のいずれかのプロトコルが使用されます。

- aes-192
- AES-256

詳細については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html にある「*Cisco Unified ICM/Contact Center Enterprise SNMP* ガイド」を参照してください。

# TLS 暗号化のサポート

データ センター インターフェイスや、Cisco Finesse、Customer Collaboration Platform、CVP、アプリケーション ゲートウェイなどの外部コンポーネントは、TLS を使用した暗号化をサポートします。

## サポート対象の暗号方式

暗号化に使用される AES 暗号を次に示します。

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

## 暗号スイートの管理

サーバとクライアントについて、サポートされている暗号をそれぞれ次のレジストリから追加または削除できます。

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

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