参照先

セキュリティ証明書

Live Data の証明書

HTTPS を使用して Finesse と Cisco Unified Intelligence Center のセキュリティ証明書をセットアップする必要があります。

次の操作を実行できます。

- Finesse および Cisco Unified Intelligence Center に付属の自己署名証明書を使用します。
- サードパーティ ベンダーから認証局（CA）証明書を入手してインストールします。
- 証明書を内部で作成します。

（注） その他の自己署名証明書を使用する場合、ライブデータ ガジェットを使用する前に、エージェントはサインインの際に Finesse デスクトップでライブ データ証明書を受け入れる必要があります。

ライブ データの自己署名証明書の追加

Finesse および Unified Intelligence Center の両方が、自己署名証明書を使用してインストールされます。独自の CA 証明書を作成したり、サードパーティの証明書ベンダーから CA 証明書を入手するのではなく、これらの自己署名証明書を使用する場合は、最初に Unified Intelligence Center パブリッシャとサブスクライバから証明書をエクスポートする必要があります。次に、証明書を Finesse にインポートする必要があります。パブリッシャの証明書は Finesse プライマリ ノードにインポートし、サブスクライバ証明書は Finesse セカンダリ ノードにインポートします。

その他の自己署名証明書を使用する場合と同様に、ライブデータ ガジェットを使用する前に、エージェントはサインイン時に Finesse デスクトップでライブ データ証明書を受け入れる必要があります。

手順

ステップ 1 Cisco Unified Intelligence Center で Cisco Unified Operating System Administration にサインインします（`https://<Cisco Unified Intelligence Center サーバのホスト名>/cmplatform`）。

ステップ 2 [セキュリティ（Security）] メニューから、[証明書の管理（Certificate Management）] を選択します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 次のいずれかを実行します。

- サーバの tomcat 証明書がリストにない場合は、[新規作成（Generate New）] をクリックします。証明書の作成が完了したら、サーバを再起動します。この手順を再開します。
- サーバの tomcat 証明書がリストにある場合は、その証明書をクリックして選択します。（選択した証明書に、サーバのホスト名が含まれていることを確認します。）

ステップ 5 [.pemファイルのダウンロード（Download .pem file）] をクリックして、ファイルをデスクトップに保存します。

Cisco Unified Intelligence Center パブリッシャと Cisco Unified Intelligence Center サブスクライバのホスト名を含む証明書をダウンロードする必要があります。

ステップ 6 プライマリ Finesse サーバで Cisco Unified Operating System にサインインします（http://*Finesse* サーバのホスト名/cmplatform）。

ステップ 7 **[セキュリティ（Security）]** メニューで **[証明書の管理(Certificate Management)]** を選択します。

ステップ 8 [証明書のアップロード(Upload Certificate)] をクリックします。

ステップ 9 [証明書の名前（Certificate Name）] ドロップダウン リストから、[tomcat-trust] を選択します。

ステップ 10 [参照（Browse）] をクリックし、.pem ファイル（Cisco Unified Intelligence Center パブリッシャとサブスクライバの証明書）の場所を参照します。

ステップ 11 [ファイルのアップロード（Upload File）] をクリックします。

ステップ 12 Finesse サーバで Cisco Finesse Tomcat を再起動します。

サード パーティ ベンダーからのライブ データの CA 証明書の取得およびアップロード

Finesse と Cisco Unified Intelligence Center サーバ間の HTTPS 接続を確立するときには、サードパーティ ベンダーから提供される証明機関（CA）の証明書を使用できます。

https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-enterprise-1101/200286-Unified-CCE-Solution-Procedure-to-Obtai.htmlから入手可能なテクニカルノート『*Procedure to Obtain and Upload CA Certificate from a Third-party Vendor*』の手順に従ってください。

Windows での CA のセットアップ

Windows 2008 R2 での Microsoft Certificate Server のセットアップ

この手順では、導入に Windows Server 2008 R2（Standard）Active Directory サーバが使用されていることを前提とします。Windows 2008 R2（Standard）ドメイン コントローラで Active Directory 証明書サービスの役割を追加するには、以下の手順を実行します。

手順

ステップ 1 [スタート（Start）] をクリックし、[コンピュータ（Computer）] を右クリックして、[管理（Manage）] を選択します。

ステップ 2 左側のペインで **[ロール（Roles）]** をクリックします。

ステップ 3 右側のペインで **[ロールの追加(Add Roles)]** をクリックします。

[ロール ウィザードの追加(Add Roles Wizard)]が開きます。

ステップ 4 [サーバ ロールの選択(Select Server Roles)]画面で、**[ディレクトリ証明書サービスの有効（Active Directory Certificate Services）]** チェック ボックスをオンにし、**[次へ（Next）]** をクリックします。

ステップ 5 [ディレクトリ証明書サービスを有効する紹介（Introduction to Active Directory Certificate Services）] 画面で、**[次へ（Next）]** をクリックします。

ステップ 6 [ロール サービスの選択（Select Role Services）]画面で、**[証明機関（Certification Authority）]** チェック ボックスをオンにし、**[次へ（Next）]** をクリックします。

ステップ 7 [セットアップタイプの指定（Specify Setup Type）]画面で、**[エンタープライズ（Enterprise）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 8 [CA タイプの指定（Specify CA Type）]画面で、**[ルートCA（Root CA）]** を選択し、**[次へ（Next）]** をクリックします。

ステップ 9 [秘密キーのセットアップ（Set Up Private Key）] でCA の暗号化を設定し、[CA の暗号化の構成（Configure Cryptography for CA）]、[CA 名の構成（Configure CA Name]、[有効期間の設定（Set Validity Period）]、および [Configure Certificate Database] の各画面で **[次へ（Next）]** をクリックし、デフォルト値を受け入れます。

ステップ 10 [インストール選択の確認（Confirm Installations Selections）] 画面で、情報を確認し、**[インストール（Install）]** をクリックします。

Windows Server 2012 R2 での Microsoft Certificate Server のセットアップ

この手順では、導入に Windows Server 2012 R2 （Standard）Active Directory サーバが使用されていることを前提とします。Windows Server 2012 R2（Standard）ドメイン コントローラの Active Directory 証明書サービスの役割を追加するには、以下の手順を実行します。

始める前に

開始する前に、Microsoft .Net Framework 3.5 Service Pack 1 をインストールしている必要があります。手順については、Windows Server 2012 のマニュアルを参照してください。

手順

ステップ 1 Windows で [サーバマネージャ（Server Manager）] を開きます。

ステップ 2 **クイックスタート** ウィンドウで **役割と機能の追加** をクリックします。

ステップ 3 **インストールタイプの設定** タブで、**役割ベースまたは機能ベースのインストール** を選択し、**次へ** をクリックします。

ステップ 4 [サーバの選択（Server Selection）] タブで、宛先サーバを選択してから [次へ（Next）] をクリックします。

ステップ 5 **サーバのロール** タブで、**Active Directory証明書サービス** ボックスをオンにして、ポップアップ ウィンドウで **機能の追加** ボタンをクリックします。

ステップ 6 [機能（Features）] タブと [AD CS] タブで、[次へ（Next）] をクリックしてデフォルト値を受け入れます。

ステップ 7 [役割サービス（Role Services）] タブで [証明機関（Certification Authority）] ボックスがオンになっていることを確認し、[次へ（Next）] をクリックします。

ステップ 8 [確認（Confirmation）] タブで [インストール（Install）] をクリックします。

ステップ 9 インストールが完了したら、**対象サーバに Active Directory 証明書サービスを構成する** リンクをクリックします。

ステップ 10 （ドメイン管理者ユーザの）クレデンシャルが正しいことを確認し、[次へ（Next）] をクリックします。

ステップ 11 [役割サービス（Role Services）] タブで [証明機関（Certification Authority）] ボックスをオンにし、[次へ（Next）] をクリックします。

ステップ 12 [セットアップの種類（Setup Type）] タブで [エンタープライズCA（Enterprise CA）] を選択し、[次へ（Next）] をクリックします。

ステップ 13 [CAの種類（CA Type）] タブで [ルートCA（Root CA）] を選択し、[次へ（Next）] をクリックします。

ステップ 14 [秘密キー（Private Key）]、[暗号化（Cryptography）]、[CAの名前（CA Name）]、[有効期間（Validity Period）]、および [証明書データベース（Certificate Database）] の各タブで、[次へ（Next）] をクリックしてデフォルト値を受け入れます。

ステップ 15 [確認（Confirmation）] タブで情報を確認し、[構成（Configure）] をクリックします。

AW マシンに CA 署名付き証明書を生成してインポートする

CA 署名付き証明書を生成し、すべての AW マシンにインポートします。

手順

ステップ 1 AW-HDS-DDS サーバにログインします。

ステップ 2 以下を実行して、既存の証明書を削除します。**%JAVA_HOME%\bin\keytool.exe -delete -keystore -alias tomcatcert ..\lib\security\cacerts**。

ステップ 3 プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 4 以下を実行して選択したキーサイズでエイリアスの新しいキーペアを生成します。**%JAVA_HOME%\bin>keytool.exe -genkeypair -alias tomcatCert -v -keysize 1024 -keyalg RSA -keystore ..\lib\security\cacerts**。

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the AW host name> E.g CCE-AW-1-21
What is the name of your organizational unit?
[Unknown]: <specify OU> E.g. ccbu
What is the name of your organization?
[Unknown]: <specify the name of the org> E.g. cisco
What is the name of your City or Locality?
[Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
[Unknown]: <specify the name of the state/province>  E.g. KA
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code>  E.g. 91
Is CN=CCE-AW-1-21, OU=cisco, O=ccbu, L=BLR, ST=KA, C=91 correct?
[no]: yes
```

ステップ 5 プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 6 以下を実行してエイリアスの CSR 証明書を生成して、ファイルに保存します（例えば、tomcatCert.csr）。**%JAVA_HOME%\bin>keytool.exe -alias tomcatCert -certreq -keystore ..\lib\security\cacerts -file c:\cert\tomcatCert.csr**

ステップ 7 プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 8 ルート CA 証明書と CA 署名証明書を %JAVA_HOME%\bin> にコピーします。

ステップ 9 以下を実行してルート CA 証明書をインストールします。**%JAVA_HOME%\bin\keytool.exe -keystore ..\lib\security\cacerts -import -v -trustcacerts -alias root -file %Path_Of_Root_Cert%\<filename_of_root_cert>**。

ステップ 10 プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 11 以下を実行して証明付き証明書をインストールします。**"%JAVA_HOME%\bin\keytool.exe -keystore ..\lib\security\cacerts -import -v -trustcacerts -alias tomcatcert -file %Path_Of_Root_Cert%\<filename_of_CA_signed_cert>"**。

ステップ 12 [サービス] に移動して、Tomcat を再起動します。

AWマシンで自己署名証明書を生成してインポートする

すべての AW マシンに自己署名証明書を生成してインポートします。

手順

ステップ 1 AW-HDS-DDS サーバにログインします。

ステップ 2 以下を実行して、既存の証明書を削除します。**%JAVA_HOME%\bin\keytool.exe -delete -keystore -alias tomcatcert ..\lib\security\cacerts**。

ステップ 3 プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 4 以下を実行して選択したキーサイズでエイリアスの新しいキーペアを生成します。**%JAVA_HOME%\bin>keytool.exe -genkeypair -alias tomcatCert -v -keysize 1024 -keyalg RSA -keystore ..\lib\security\cacerts**。

```
Enter keystore password: <enter the keystore password>
What is your first and last name?
[Unknown]: <specify the AW host name> E.g CCE-AW-1-21
What is the name of your organizational unit?
[Unknown]: <specify OU> E.g. ccbu
What is the name of your organization?
[Unknown]: <specify the name of the org> E.g. cisco
What is the name of your City or Locality?
[Unknown]: <specify the name of the city/locality>  E.g. BLR
What is the name of your State or Province?
[Unknown]: <specify the name of the state/province>  E.g. KA
What is the two-letter country code for this unit?
[Unknown]: <specify two-letter Country code>  E.g. 91
Is CN=CCE-AW-1-21, OU=cisco, O=ccbu, L=BLR, ST=KA, C=91 correct?
[no]: yes
```

ステップ 5 [サービス] に移動して、Tomcat を再起動します。

ECE Web サーバで自己署名証明書を生成する

手順

ステップ 1 **ECE Web サーバ** にログインします。

ステップ 2 **Internet Information Services (IIS) Manager** を開きます。

ステップ 3 左側のペインの **接続** の下で、設定済みの < ホスト名 > を選択します。

<ホスト名> ホーム ページが開きます。

ステップ 4 **IIS** エリアで、**サーバ証明書** をクリックします。

ステップ 5 右側のペインの **アクション** の下で、**自己署名証明書の作成** をクリックします。

自己署名証明書の作成 ウィンドウが開きます。

ステップ 6 **証明書にフレンドリ名を指定** フィールドに、証明書の名前を入力します。

ステップ 7 **新しい証明書の証明書ストアの選択** ドロップダウンリストから、**Web ホスティング** を選択します。

ステップ 8 [OK] をクリックします。

証明書が生成され、ホームページに表示されます。

ステップ 9 左側のペインで、**接続** の下にある **サイトの** > **デフォルト Web サイト** に移動します。

デフォルトの Web サイトのホーム ページが開きます。

ステップ 10 右側ペインの **アクション** の下で、**バインド** をクリックします。

ステップ 11 [追加（Add）] をクリックします。

サイト バインドの追加 ウィンドウが開きます。

ステップ 12 **タイプ** ドロップダウンリストで **https**を選択します。

ステップ 13 [SSL証明書] ドロップダウンリストから、**<ホスト名>** を選択します。

ステップ 14 [OK] をクリックします。

ステップ 15 右ペインの **Web サイトの管理**で **再起動**をクリックします。

Cisco Unified CVP サーバにプリンシパル AW 証明書を追加します。

プリンシパル AW 証明書をすべての Unified CVP サーバに追加します。

手順

ステップ 1 パッケージ済みの CCE webadmin 自己署名証明書を `%CVP_HOME%\conf\security\` にダウンロードする

ステップ 2 証明書をCVPコールサーバーキーストアにインポートします。`%CVP_HOME%\jre\bin\keytool.exe -import -trustcacerts -keystore %CVP_HOME%\conf\security\.keystore -storetype JCEKS -alias AW_cert -file %CVP_HOME%\conf\security\<AW certificate.pem>`

キーストアのパスワードは、%CVP_HOME%\conf\security.properties にあります。

ソリューション コンポーネントの自己署名証明書を AW マシンに追加する

Finesse 証明書を AW マシンに追加します

CA 証明書を持っていない場合は、Finesse サーバから AW マシンに自己署名入りの証明書をインポートする必要があります。これにより、AW マシンは、セキュアチャネル経由で Finesse と通信することができます。

（注）
- 証明書 CommonName (CN) は、パッケージの CCE Inventory 内の各 Finesse および IdS サーバに指定されている完全修飾ドメイン名 (FQDN) と一致する必要があります。

手順

ステップ 1 プライマリ サーバで Cisco Unified オペレーティング システムシステム管理 にサインインします。（*https://<FQDN of Finesse server>:8443/cmplatform*）。

ステップ 2 [セキュリティ（Security）] メニューで [証明書の管理(Certificate Management)] を選択します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 次のいずれかを実行します。

- サーバの tomcat 証明書がリストにない場合は、**自己署名証明書の生成** をクリックします。証明書の作成が完了したら、サーバを再起動します。
- サーバの tomcat 証明書がリストにある場合は、その証明書をクリックして選択します。（選択した証明書に、サーバのホスト名が含まれていることを確認します。）

ステップ 5 **.PEM ファイルのダウンロード** をクリックして、ファイルをデスクトップに保存します。
プライマリ サーバのホスト名を含む自己署名証明書をダウンロードする必要があります。

ステップ 6 AW マシンの任意の場所に証明書をコピーします。

ステップ 7 AW マシンのターミナルで以下のコマンドを実行します。

- `cd %JAVA_HOME%`
- `keytool -import -file <path where .pem certificate is copied> -alias <FQDN of Finesse Server> -keystore .\lib\security\cacerts`

ステップ 8 [サービス] に移動して、Tomcat を再起動します。

AW マシンに IdS 証明書を追加します

CA 証明書がない場合は、Cisco Identify Service (IdS) から、AW マシンに自己署名証明書をインポートする必要があります。これにより、AW マシンは、セキュリティで保護されたチャネルを介して IdS と通信することができます。

（注）
- 証明書は、IdS パブリッシャとサブスクライバ サーバの両方からダウンロードしてインポートする必要があります。
- 証明書 CommonName (CN) は、パッケージの CCE Inventory 内の各 Finesse および IdS サーバに指定されている完全修飾ドメイン名 (FQDN) と一致する必要があります。

手順

ステップ 1 プライマリ サーバ で Cisco Unified オペレーティング システムシステム管理 にサインインします。（*https://<FQDN of Ids server:8443>/cmplatform*）。

ステップ 2 [セキュリティ（Security）] メニューで [証明書の管理(Certificate Management)] を選択します。

ステップ 3 [検索（Find）] をクリックします。

ステップ 4 次のいずれかを実行します。

- サーバの tomcat 証明書がリストにない場合は、**自己署名証明書の生成** をクリックします。証明書の作成が完了したら、サーバを再起動します。
- サーバの tomcat 証明書がリストにある場合は、その証明書をクリックして選択します。（選択した証明書に、サーバのホスト名が含まれていることを確認します。）

ステップ 5 **.PEM ファイルのダウンロード** をクリックして、ファイルをデスクトップに保存します。
プライマリ サーバのホスト名を含む自己署名証明書をダウンロードする必要があります。

ステップ 6 AW マシンの任意の場所に証明書をコピーします。

ステップ 7 AW マシンのターミナルで以下のコマンドを実行します。

- `cd %JAVA_HOME%`
- `keytool -import -file <path where .pem certificate is copied> -alias <FQDN of IdS Server> -keystore .\lib\security\cacerts`

ステップ 8 [サービス] に移動して、Tomcat を再起動します。

ECE Web サーバ証明書を AW マシンに追加します

CA 証明書を持っていない場合は、ECE Web サーバから AW マシンに自己署名入りの証明書をインポートする必要があります。これにより、 Unified CCE 管理で ECE ガジェットを起動できるようになります。

手順

ステップ 1 ECE Web サーバ（*https://<ECE Web Server>*）で、証明書 **.pem ファイル**をダウンロードして、デスクトップに保存します。

ステップ 2 AW マシンの任意の場所に証明書をコピーします。

ステップ 3 AW マシンのターミナルで以下のコマンドを実行します。

- `cd %JAVA_HOME%`
- `keytool -import -file <path where .pem certificate is copied> -alias <FQDN of ECE Web Server> -keystore .\lib\security\cacerts`

ステップ 4 [サービス] に移動して、Tomcat を再起動します。

CVP レポート サーバ証明書を AW マシンに追加します

（注） この手順は、CA 証明書を持っていない場合にのみ適用されます。

CVP レポート サーバをインストールする場合は、レポート サーバの自己署名証明書を AW マシンにインポートして、ブラウザの警告を解消し、CVP レポート サーバと AW マシン間の https 接続を確立する必要があります。キーツールを使用して自己署名証明書を生成します。

重要 証明書 CommonName（CN）は、Packaged CCE Inventory の CVP レポート サーバに提供された完全修飾ドメイン名（FQDN）と一致する必要があります。

手順

ステップ 1 CVP レポート サーバにログインします。

ステップ 2 コマンド プロンプトで、.keystoreがあるディレクトリに移動します。

次に例を示します。

```
C:\Cisco\CVP\conf\security
```

ステップ 3 以下のコマンドを使用して、CVP キーストアの Tomcat 証明書を表示することができます。

```
C:\Cisco\CVP\jre\bin\keytool.exe -delete -alias wsm_certificate -keystore .keystore
-storetype JCEKS
```

ステップ 4 CVP キーストアのパスワードを入力します。

CVP キーストアのパスワードは、`c:\Cisco\CVP\conf\security.properties` で利用できます。

または

以下のコマンドを実行して、キーストア パスワードを取得します。

```
more c:\Cisco\CVP\conf\security.properties
Security.keystorePW = <Returns the keystore password>
```

ステップ 5 以下のコマンドを実行すると自己署名認証が生成されます。

```
C:\Cisco\CVP\jre\bin\keytool.exe -genkey -keyalg RSA -alias wsm_certificate -keystore
.keystore -storetype JCEKS -keysize 1024
```

ステップ 6 キーストアのパスワードを入力し、組織情報を提供します。最初と最後の名前には、CVP レポート サーバの完全修飾ドメイン名 (FQDN) を入力します。

ステップ 7 Reporting Server を再起動します。

ステップ 8 ブラウザから自己署名入りの証明書 (.pem ファイル) をダウンロードします（*https://FQDN of Reporting Server:8111*）。

ステップ 9 AW マシンの任意の場所に証明書をコピーします。

ステップ 10 AW マシンのターミナルで、以下のコマンドを実行します。

- `cd %JAVA_HOME%`
- `keytool -import -file <path where the certificate (.pem) is copied> -alias <FQDN of CVP Reporting Server> -keystore ..\lib\security\cacerts`

ステップ 11 [サービス] に移動して、Tomcat を再起動します。

コール サーバ / レポート サーバのグレースフル シャットダウン

このセクションでは、CLI から callserver/reportingserver のサービスをシャットダウンする手順について説明します。管理者は、記載されている手順に従ってこのユーティリティを使用することができます。

手順

ステップ 1 [CVP コール サーバ] ボックスにログインします。

ステップ 2 `<CVP-INSTALLED-LOCATION>\Cisco\CVP\bin\ServiceController`に移動します。

ステップ 3 `service-controller.bat` ファイルを実行します。

ステップ 4 プロンプトで詳細を入力します。

```
CALLSERVER-IP-ADDRESS: <IP-Address of the Call Server>
CALLSERVER-USERNAME: <Username of the Call Server>
CALLSERVER-PASSWORD:  <Password of the Call Server>
SERVICE-NAME: <Choose the Service name which you need to shutdown
gracefully(callserver/reportingserver)>
REPORTINGSERVER-IP-ADDRESS: <IP-Address of the REPORTING SERVER>
```

（注）
- レポート サーバが正常にシャットダウンされた場合は、CVP のコール サーバが動作していることを確認します。
- **reportingserver** サービスが選択されている場合は、レポートサーバの IP アドレスを指定する必要があります。