初期設定

Contact Center Enterprise CTI サーバの設定の指定

プライマリ Finesse サーバで管理コンソールにアクセスし、A 側と B 側の CTI サーバを設定します。

（注） Finesse の再起動後、サーバ関連のすべてのサービスが再起動するまでに約 6 分かかる場合があります。 したがって、Finesse 管理コンソールにアクセスを試みる前に、6 分待機する必要があります。

（注） HTTPS を使用する場合は、最初に管理コンソールにアクセスしたときに、ブラウザにセキュリティ警告が表示されます。 サインインするたびにブラウザにセキュリティ警告が表示されないようにするには、Finesse に付属の自己署名証明書を信頼するか、CA 証明書を取得してアップロードします。

手順

ステップ 1 次のプライマリ Finesse サーバの管理コンソールにサインインします。
http://*Finesse* サーバの *FQDN*、ホスト名、または *IP* アドレス/cfadmin

ステップ 2 インストール時に定義したアプリケーション ユーザの資格情報でサインインします。

ステップ 3 次の表に示すように、[Contact Center Enterprise CTI Server Settings] 領域で、CTI サーバの設定を入力します。 必要に応じてコンフィギュレーション ワークシートを参照してください。

フィールド	説明
A Side Host/IP Address	A 側の CTI サーバのホスト名または IP アドレスを入力します。 この値は通常、Peripheral Gateway（PG）の IP アドレスです。CTI サーバが PG で稼働します。
A Side Port	A 側の CTI サーバのポート番号を入力します。 このフィールドの値は、A 側の CTI サーバのセットアップ時に設定されたポートと一致している必要があります。
Peripheral ID	エージェント PG ルーティング クライアント（PIM）の ID を入力します。 Agent PG の Peripheral ID は A 側と B 側の CTI 用サーバで同じ値に設定する必要があります。
B Side Host/IP Address	B 側の CTI サーバのホスト名または IP アドレスを入力します。
B Side Port	B 側の CTI サーバのポート番号を入力します。 このフィールドの値は、B 側の CTI サーバのセットアップ時に設定されたポートと一致している必要があります。

ステップ 4 [Save] をクリックします。

関連トピック

システム アカウント権限
コンフィギュレーション ワークシート

Contact Center Enterprise 管理サーバおよびデータ サーバの設定の指定

Contact Center Enterprise 管理サーバおよびデータ サーバの設定を指定して、Finesse エージェントおよびスーパーバイザ用の認証を有効にします。

手順

ステップ 1 まだサインインしていない場合は、管理コンソールにサインインします。

ステップ 2 次の表に示すように、[Contact Center Enterprise Administration & Data Server Settings] 領域で、管理サーバおよびデータ サーバの設定を入力します。 必要に応じてコンフィギュレーション ワークシートを参照してください。

フィールド	説明
Primary Host/IP Address	Unified CCE Administration & Data Server のホスト名または IP アドレスを入力します。
Backup Host/IP Address	バックアップ Unified CCE Administration & Data Server のホスト名または IP アドレスを入力します。
Database Port	Unified CCE Administration & Data Server のポートを入力します。 （注） Finesse がプライマリとバックアップの管理サーバおよびデータ サーバのポートが同じであると想定しているため、Finesse 管理コンソールには 1 つのポート フィールドだけが表示されます。 プライマリとバックアップの管理サーバおよびデータ サーバでポートが同じであることを確認します。
AW Database Name	AW データベース（AWDB）の名前を入力します（たとえば、*ucceinstance*_awdb）。
ドメイン（Domain）	AWDB のドメインを入力します。

フィールド	説明
Username	AWDB にサインインするために必要なユーザ名を入力します。
パスワード	AWDB にサインインするために必要なパスワードを入力します。

ステップ 3 [Save（保存）] をクリックします。

関連トピック

コンフィギュレーション ワークシート

クラスタ設定の指定

セカンダリ Finesse ノードのクラスタ設定を指定します。 セカンダリ Finesse ノードは、プライマリ サーバがダウンした場合に、エージェントの要求を処理します。

手順

ステップ 1 まだサインインしていない場合、アプリケーション ユーザの資格情報を使用して管理コンソールにサインインします。

ステップ 2 [Cluster Settings] 領域の [Host/IP Address] フィールドに、セカンダリ Finesse サーバのホスト名または IP アドレスを入力します。

ステップ 3 [Save（保存）] をクリックします。

関連トピック

コンフィギュレーション ワークシート

Cisco Tomcat の再起動

Contact Center Enterprise CTI サーバ、Contact Center Enterprise Administration & Data Server、またはクラスタの設定変更後、変更を有効にするために Cisco Tomcat を再起動する必要があります。

手順

ステップ 1 CLI にアクセスし、次のコマンドを実行します。
utils service restart Cisco Tomcat

ステップ 2 Cisco Tomcat サービスをモニタするためのコマンド **utils service list** を入力できます。 Cisco Tomcat が STARTED に変更されたら、パスワードを設定してあるエージェントがデスクトップにサインインできます。

関連トピック

Cisco Finesse CLI
Finesse サービス

複製ステータスの確認

手順

ステップ 1 プライマリ Finesse サーバで CLI にアクセスします。
ステップ 2 インストール時に定義した管理者ユーザの資格情報を使用してサインインします。
ステップ 3 次のコマンドを実行します。
utils dbreplication runtimestate

このコマンドは、プライマリおよびセカンダリ Finesse サーバの両方で複製ステータスを返します。

関連トピック

Cisco Finesse CLI
Replication Status

言語パックのインストール

英語以外の言語で Finesse デスクトップ インターフェイスを使用する場合のみ言語パックをダウンロードしてインストールします。

Finesse の言語パックは単一の Cisco Option Package（COP）ファイルとして提供されます。 ファイルは、Cisco.com からダウンロードして使用でき、すべての言語で単一のインストーラが含まれています。

Finesse の言語パックは次のリンクでからダウンロードできます。

http://software.cisco.com/download/release.html?mdfid=283613135&softwareid=284259728&release=10.5(1)&relind=AVAILABLE&rellifecycle=&reltype=latest

COP ファイルは通常、アクティブで実行中のシステムでインストールできます。COP ファイルは削除したりロールバックすることはできません。

（注） 特定の COP ファイルの ReadMe ファイルが以下の一般的なガイドラインと矛盾する場合は、ファイルの説明に従います。

サポートされる言語の詳細については、『*Cisco Finesse Administration Guide*』（http://www.cisco.com/c/en/us/support/customer-collaboration/finesse/products-user-guide-list.html）を参照してください。

手順

ステップ 1 Cisco Software サイトhttp://software.cisco.com/download/type.html?mdfid=283613135&i=rmから Finesse サーバがアクセスできる SFTP サーバまたはローカル ソースに Finesse COP ファイルをダウンロードします。

ステップ 2 SSH を使用して、プラットフォームの管理アカウントで Finesse システムにログインします。

ステップ 3 CLI を使用して、**utils system upgrade initiate** コマンドを実行します。

ステップ 4 utils system upgrade initiate コマンドの指示に従ってください。

ステップ 5 サーバをリブートします。

ステップ 6 ステップ 2 からステップ 5 をセカンダリ Finesse サーバで繰り返して行ってください。

ステップ 7 両方の Finesse サーバでインストールが完了したら、エージェントとスーパーバイザは、ブラウザのキャッシュとクッキーを消去する必要があります。

エージェントにパスワードがあることの確認

Unified CCE Configuration Manager で定義したパスワードがないエージェントは Finesse にサインインできません。

エージェント パスワードは Unified CCE のオプション フィールドですが、Cisco Finesse では必須です。

パスワードがないエージェントの場合、次の手順を実行する必要があります。

手順

ステップ 1 Unified CCE Configuration Manager を起動します。

ステップ 2 エージェント（[Agent Explorer] > [Agent] タブ）のレコードを検索します。

ステップ 3 パスワードを入力し、レコードを保存します。

エージェントの [Logout non-activity time] 設定の確認

[Logout non- activity time] は、Finesse からログアウトするまでにエージェントが [Not Ready] 状態で非アクティブのままになれる時間の長さを指定します。 エージェントの [Logout non-activity time] を設定するには、次の手順を実行します。

手順

ステップ 1 Unified CCE Configuration Manager を起動します。

ステップ 2 Agent Desk Settings List を起動します（[Tools] > [List Tools]）。

ステップ 3 リストから **[Agent Desktop Settings]** を選択します。

ステップ 4 [Logout non-activity time] フィールドで、システム ソフトウェアがエージェントをログアウトするまでにエージェントが [Not Ready] ステータスで非アクティブになっている秒数を入力します。10 ～ 7200 秒の値を入力できます。

ステップ 5 [Save（保存）] をクリックします。
変更した設定は、これらのエージェントのデスクトップ設定を使用してエージェントすべてに適用されます。

エージェント電話の設定

エージェントが Finesse デスクトップにサインインできるようにするには、エージェント電話を Unified Communications Manager で設定する必要があります。 エージェント電話の設定の詳細については、『Unified Contact Center Enterprise Design Guide』の「“Agent Phones”」の項を参照してください。

Internet Explorer のブラウザ設定

Finesse デスクトップへのアクセスに Internet Explorer を使用している場合、Finesse のすべての機能を正しく動作させるため、ブラウザで特定の設定を行う必要があります。

ポップアップ ブロッカを無効にします。

Finesse は、互換表示をサポートしません。 デスクトップが互換表示で実行されている場合、Internet Explorer はそのバージョンの標準モードで表示します。

次のプライバシーと詳細設定を設定します。

1 ブラウザのメニューから、[Tools] > [Internet Options] を選択します。

2 **[Privacy]** タブをクリックします。

3 **[Sites]** をクリックします。

4 [Address of website] ボックスに A 側 Finesse サーバのドメイン名を入力します。

5 **[Allow]** をクリックします。

6 [Address of website] ボックスに B 側 Finesse サーバのドメイン名を入力します。

7 **[Allow]** をクリックします。

8 **[OK]** をクリックします。

9 [Internet Options] ダイアログボックスで、**[Advanced]** タブをクリックします。

10 [Security] で、**[Warn about certificate address mismatch]** チェック ボックスをオフにします。

11 **[OK]** をクリックします。

ユーザがサインインできるようにするには、次のセキュリティ設定を有効にします。

- Run ActiveX controls and plug-ins
- Script ActiveX controls marked as safe for scripting
- Active scripting

これらの設定を有効にするには：

1 Internet Explorer のブラウザ メニューで、[Tools] > [Internet Options] を選択します。

2 **[Security]** タブをクリックします。

3 **[Custom level]** をクリックします。

4 [ActiveX controls and plug-ins] で、**[Run ActiveX controls and plug-ins]** および **[Script ActiveX controls marked safe for scripting]** で **[Enable]** を選択します。

5 [Scripting] の **[Active Scripting]** で **[Enable]** を選択します。

証明書の設定

Finesse Finesse デスクトップとサーバ間の通信に HTTPS を使用している場合、セキュリティ証明書を設定する必要があります。 使用可能な Finesse で提供される自己署名証明書を使用するか、CA 証明書を用意して使用できます。 サードパーティのベンダーから CA 証明書を取得するか、組織内で生成することができます。

Finesseはワイルドカードの証明書をサポートしていません。 認証局によって署名されたルート証明書をアップロードしたら、自己署名証明書が上書きされます。

Finesse 自己署名証明書を使用する場合、エージェントはデスクトップに初めてサインインしたときに、セキュリティ証明書を受け入れる必要があります。 CA 証明書を使用する場合は、各クライアントのブラウザで受け入れるか、またはグループ ポリシーを使用してルート証明書を導入できます。

サーバ側の証明書管理

デフォルトで、Finesse には自己署名証明書が付属しています。 これらの証明書を使用する場合は、初めてサインインしたときに、証明書を受け入れるように手順を実行する必要があります。エージェントの操作を簡単にするため、CA 証明書を取得してアップロードしたり、独自の証明書を内部的に作成できます。

CA 証明書の取得およびアップロード

（注） この手順は、HTTPS を使用している場合にだけ適用されます。

この手順は任意です。 HTTPS を使用している場合、CA 証明書を取得してアップロードするか、Finesse で提供される自己署名証明書を使用するかを選択できます。

サインインするたびにブラウザにセキュリティ警告が表示されないようにするには、認証局（CA）によって署名されたアプリケーション証明書およびルート証明書を取得します。 Cisco Unified Communications Operating System Administration から証明書管理ユーティリティを使用します。

[Cisco Unified Communications Operating System Administration] を開くには、ブラウザで次の URL を入力します。

https://プライマリ *Finesse* サーバのホスト名/cmplatform

Finesse のインストール時に作成されたアプリケーション ユーザ アカウントのユーザ名とパスワードを使用してサインインします。

（注） 詳細については、*Cisco Unified Communications Operating System Administration* オンライン ヘルプのセキュリティに関するトピックを参照してください。

手順

ステップ 1 CSR を作成します。

a) [Security]>[Certificate Management] > [Generate CSR] を選択します。
b) [Certificate Name] ドロップダウン リストで、**[tomcat]** を選択します。
c) **[Generate CSR]** をクリックします。

ステップ 2 CSR をダウンロードします。

a) [Security] > [Certificate Management] > [Download CSR] を選択します。
b) [Certificate Name] ドロップダウン リストで、***[tomcat]*** を選択します。
c) ***[Download CSR]*** をクリックします。

ステップ 3 セカンダリ Finesse サーバ用の CSR を生成し、ダウンロードします。

セカンダリ サーバに対して Cisco Unified Operating System Administration を開くには、ブラウザのアドレス バーに次の URL を入力します。

https://セカンダリ *Finesse* サーバのホスト名/cmplatform

ステップ 4 CSR を使用して、認証局から CA ルート証明書、中間証明書、署名付きアプリケーション証明書を取得します。

（注） 証明書チェーンを正しく設定するには、次の手順で説明されている順序で証明書をアップロードする必要があります。

ステップ 5 証明書を受け取ったら、[Security]> > [Certificate Management] > [Upload Certificate] を選択します。

ステップ 6 ルート証明書をアップロードします。

a) [Certificate Name] ドロップダウン リストで、**[tomcat-trust]** を選択します。
b) [Upload File] フィールドで **[Browse]** をクリックし、ルート証明書ファイルを参照します。
c) **[Upload File]** をクリックします。

ステップ 7 中間証明書をアップロードします。

a) [Certificate Name] ドロップダウン リストで、**[tomcat-trust]** を選択します。
b) ルート証明書フィールドに、前の手順でアップロードしたルート証明書の名前を入力します。拡張子は記入しないでください（例：TEST Root CA 2048）。
c) [Upload File] フィールドで **[Browse]** をクリックし、中間証明書ファイルを参照します。
d) **[Upload File]** をクリックします。

ステップ 8 アプリケーション証明書をアップロードします。

a) [Certificate Name] ドロップダウン リストで、**[tomcat]** を選択します。
b) ルート証明書フィールドに、前の手順でアップロードした中間証明書の名前を入力します。.pem の拡張子を記入してください（例：TEST-SSL-CA.pem）。
c) [Upload File] フィールドで **[Browse]** をクリックし、アプリケーション証明書ファイルを参照します。
d) **[Upload File]** をクリックします。

ステップ 9 アップロードが完了したら、Finesse からログオフします。

ステップ 10 プライマリ Finesse サーバで CLI にアクセスします。

ステップ 11 utils service restart Cisco Finesse Notification Service コマンドを入力して、Cisco Finesse Notification サービスを再起動します。

ステップ 12 utils service restart Cisco Tomcat コマンドを入力して、Cisco Finesse Tomcat サービスを再起動します。

ステップ 13 アプリケーション証明書をセカンダリ Finesse サーバにアップロードします。
ルート証明書と中間証明書は、セカンダリ Finesse サーバにアップロードする必要はありません。これらの証明書をプライマリ サーバにアップロードしたら、セカンダリ サーバに複製されます。

ステップ 14 セカンダリ Finesse サーバの CLI にアクセスし、Cisco Finesse Notification サービスと Cisco Tomcat サービスを再起動します。

内部的な証明書の作成

Microsoft Certificate Server のセットアップ

この手順では、展開に Windows Server 2008 Active Directory サーバが使用されていることを前提とします。 Windows 2008 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、次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、[役割（**Roles**）] をクリックします。

ステップ 3 右側のペインで、[役割の追加（**Add Roles**）] をクリックします。
[役割の追加（Add Roles）] ウィザードが開きます。

ステップ 4 [サーバの役割の選択（Select Server Roles）] 画面で、[Active Directory 証明書サービス（**Active Directory Certificate Services**）] チェックボックスをオンにして [次へ（**Next**）] を選択します。

ステップ 5 [Active Directory 証明書サービスについて（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 [役割サービスの選択（Select Role Services）] 画面で、[認証局（**Certification Authority**）] チェックボックスをオンにして、[次へ（**Next**）] をクリックします。

ステップ 7 [セットアップの種類の指定（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 の種類の指定（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 [公開キーのセットアップ（Set Up Private Key）]、[CA の暗号化を設定（Configure Cryptography for CA）]、[CA 名の設定（Configure CA Name）]、[有効期間を設定（Set Validity Period）]、および [証明書データベースの設定（Configure Certificate Database）] 画面で [次へ（**Next**）] をクリックして、デフォルトの値を受け入れます。

ステップ 10 [インストール時の選択を確認（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。

CA 証明書のダウンロード

この手順は、Windows 証明書サービスを使用していることを前提としています。 次の手順を実行して、認証局からルート CA 証明書を取得します。 ルート証明書を取得した後、各ユーザは Finesse にアクセスするために使用するブラウザにインストールする必要があります。

手順

ステップ 1 Windows 2008 ドメイン コントローラで、CLI コマンド **ca.cert certutil - ca_name.cer** を実行します。

ステップ 2 ファイルを保存します。 後で検索できるように、ファイルを保存した場所のメモを残しておきます。

クライアント側の証明書の受け入れ

最初のサインイン時にエージェントで証明書を受け入れるために実行しなければならない手順は、証明書の管理方法とエージェントが使用するブラウザによって異なります。

Internet Explorer のルート証明書の導入

グループ ポリシーが Active Directory ドメインによって適用されている環境では、ルート証明書を各ユーザの Internet Explorer に自動的に追加できます。 証明書を自動的に追加すると、設定に関するユーザ要求が簡略化されます。

（注） 証明書の警告を回避するために、各ユーザは Finesse サーバの完全修飾ドメイン名（FQDN）を使用してデスクトップにアクセスする必要があります。

手順

ステップ 1 Windows 2008 ドメイン コントローラで、[スタート（Start）]>[管理ツール（Administrative Tools）] > [グループ ポリシーの管理（Group Policy Management）] をクリックします。

ステップ 2 [デフォルトのドメイン ポリシー（Default Domain Policy）] を右クリックし、[編集（Edit）] を選択します。

ステップ 3 [グループ ポリシー管理コンソール（Group Policy Management Console）] で、[コンピュータ設定（Computer Configuration）] > [ポリシー（Policies）] > [ウィンドウの設定（Window Settings）] > [セキュリティ設定（Security Settings）] > [公開キー ポリシー（Public Key Policies）] に進みます。

ステップ 4 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を右クリックし、[インポート（Import）] を選択します。

ステップ 5 ca_name.cer ファイルをインポートします。

ステップ 6 [コンピュータ設定（Computer Configuration）] > [ポリシー（Policies）] > [Windows 設定（Windows Settings）] > [セキュリティ設定（Security Settings）] > [公開キー ポリシー（Public Key Policies）]

> [証明書サービス クライアント - 自動登録（Certificate Services Client - Auto-Enrollment）] に進みます。

ステップ 7 [設定モデル（Configuration Model）] リストから、[有効（Enabled）] を選択します。

ステップ 8 ドメインに含まれるコンピュータにユーザとしてサインインし、Internet Explorer を開きます。

ステップ 9 ユーザが証明書を持っていない場合は、ユーザのコンピュータ上で **gpupdate.exe/target:computer /force** コマンドを実行します。

Internet Explorer ブラウザの証明書のセットアップ

CA 証明書を取得してアップロードした後、すべてのユーザが証明書を受け入れるか、証明書がグループ ポリシーによって自動的にインストールされる必要があります。

ユーザがドメインに直接ログインしていないか、グループ ポリシーが使用されていない環境では、証明書を受け入れたら、システム内の Internet Explorer のすべてのユーザが次の手順を実行する必要があります。

手順

ステップ 1 Windows Explorer で、ca_name.cer ファイルをダブルクリックし、[開く（**Open**）] をクリックします。

ステップ 2 [Install Certificate] > [Next] > [Place all certificates in the following store] をクリックします。

ステップ 3 **[参照（Browse）]** をクリックし、**[信頼されたルート証明機関（Trusted Root Certification Authorities）]** を選択します。

ステップ 4 **[OK]** をクリックします。

ステップ 5 [次へ（**Next**）] をクリックします。

ステップ 6 [終了（**Finish**）] をクリックします。
認証局（CA）から証明書をインストールしようとしていることを示すメッセージが表示されます。

ステップ 7 [はい（**Yes**）] をクリックします。
インポートが正常に実行されたことを示すメッセージが表示されます。

ステップ 8 証明書がインストールされたことを確認するには、Internet Explorer を開きます。 ブラウザのメニューから、[ツール（Tools）]>[インターネット オプション（Internet Options）] を選択します。

ステップ 9 [コンテンツ（**Content**）] タブをクリックします。

ステップ 10 [証明書（**Certificates**）] をクリックします。

ステップ 11 [信頼されたルート証明機関（**Trusted Root Certification Authorities**）] タブをクリックします。

ステップ 12 新しい証明書がリストに表示されていることを確認します。

Firefox ブラウザの証明書のセットアップ

システム上の Firefox のすべてのユーザは、次の手順を一度実行して、証明書を受け入れる必要があります。

（注） 証明書の警告を回避するために、各ユーザは Finesse サーバの完全修飾ドメイン名（FQDN）を使用してデスクトップにアクセスする必要があります。

手順

ステップ 1 Firefox のブラウザ メニューの [オプション（**Options**）] を選択します。

ステップ 2 [詳細設定（**Advanced**）] をクリックします。

ステップ 3 [証明書（**Certificates**）] タブをクリックします。

ステップ 4 [証明書を表示（**View Certificate**）] をクリックします。

ステップ 5 [インポート（**Import**）] をクリックして、ca_name.cer ファイルを参照します。

セキュリティ証明書の受け入れ

Finesse に付属の自己署名証明書を使用する場合、ユーザが Finesse デスクトップに初めてサインインすると、処理を続行する前に、セキュリティ証明書を受け入れるように促されます。 証明書が削除されない限り、各クライアントで受け入れの操作が必要なのは 1 度のみです。

これらの証明書により、Finesse デスクトップはセキュアな接続で Finesse サーバと通信できます。

（注） Windows ユーザとしてサインインしたエージェントまたはスーパーバイザが Windows クライアントを使用し、Internet Explorer を使用して Finesse デスクトップにアクセスする場合、そのエージェントまたはスーパーバイザはセキュリティ証明書をインストールするために管理者として Internet Explorer を実行する必要があります。

管理者として Internet Explorer を実行するには、[Start] メニューで [Internet Explorer] を右クリックし、[Run as administrator] を選択します。

手順

ステップ 1 ブラウザで Finesse デスクトップの URL を入力します。

ステップ 2 Internet Explorer を使用する場合

a) Web サイトのセキュリティ証明書に問題があることを示すページが表示されます。 [**Continue to this website (not recommended)**] をクリックして Finesse のサインイン ページを開きます。

b) エージェントIDまたはユーザ名、パスワード、および内線番号を入力して、**[Sign In]** をクリックします。
次のメッセージが表示されます。

Establishing encrypted connection...

受け入れる証明書の一覧を示すダイアログボックスが表示されます。

c) ダイアログボックスで **[OK]** をクリックします。
受け入れる必要がある証明書ごとに新しいブラウザ タブが開きます。 証明書エラーは、アドレス バーに表示されます。

（注） ブラウザのセキュリティ設定によっては、ブラウザ タブの代わりに受け入れる必要がある証明書ごとにウィンドウが開くこともあります。

d) [Certificate error] をクリックし、**[View Certificates]** をクリックして [Certificate] ダイアログボックスを開きます。

e) [Certificate] ダイアログボックスで、**[Install Certificate]** をクリックして [Certificate Import Wizard] を開きます。
Windows 8.1 で Internet Explorer 11 を使用している場合、[Install Certificate] オプションは、信頼するサイトに Finesse を追加するまで表示されません。

1. ブラウザのメニューから **[Internet Options]** を選択します。
2. [Security] タブで **[Trusted Sites]** をクリックし、[Sites] をクリックします。
3. **[Add this website to the zone]** フィールドに Finesse デスクトップの URL を入力し、**[Add]** をクリックします。
4. 現在のユーザのみの証明書をインストールする場合、**[Install Certificate]** をクリックしたら、**[Store Location]** で **[Current User]** を選択します。または、このコンピュータを使用するすべての Windows ユーザの証明書をインストールする場合は、[Local Machine] を選択します。

   [Local Machine] を選択すると、ダイアログ ボックスが表示され、Windows ホスト プロセスがこのコンピュータに変更を行えるようにするかどうかが尋ねられます。 [Yes] を選択します。

f) **[Certificate Import Wizard]** で **[Next]** をクリックします。
g) **[Place all certificates in the following store]** を選択し、**[Browse]** をクリックします。
h) **[Trusted Root Certification Authorities]** を選択し、[OK] をクリックします。
i) **[Next]** をクリックします。
j) **[Finish]** をクリックします。
証明書をインストールするかどうかをたずねる **[Security Warning]** ダイアログボックスが表示されます。

k) [Yes] をクリックします。
インポートが正常に実行されたことを示す [Certificate Import] ダイアログボックスが表示されます。

l) **[OK]** をクリックします。

m) **[Certificate]** ダイアログボックスで [OK] をクリックします。
n) ブラウザ タブを閉じます。 別の証明書を受け入れるかをたずねられます。 すべての証明書を受け入れるまで、上記の手順を繰り返して行ってください。
すべての必要な証明書を受け入れたら、サインイン プロセスは終了です。

（注） デスクトップから証明書エラーをなくすため、ブラウザを閉じて再度開く必要があります。

ステップ 3 Firefox を使用している場合

a) この接続が信頼できない状態であることを示すページが表示されます。 **[I Understand the Risks]** をクリックし、**[Add Exception]** をクリックします。
b) [**Permanently store this exception**] チェックボックスがオンになっていることを確認します。
c) **[Confirm Security Exception]** をクリックします。
Finesse のサインイン ページが表示されます。
d) エージェント ID またはユーザ名、パスワード、および内線番号を入力して、**[Sign In]** をクリックします。
次のメッセージが表示されます。

Establishing encrypted connection...

受け入れる証明書の一覧を示すダイアログボックスが表示されます。

e) **[OK]** をクリックします。
受け入れる必要がある証明書ごとにブラウザ タブが開きます。
f) 各タブで、**[I Understand the Risks]** をクリックし、**[Add Exception]** をクリックします。
g) **[Permanently store this exception]** チェックボックスがオンになっていることを確認します。
h) **[Confirm Security Exception]** をクリックします。
各タブは、証明書を受け入れると閉じます。

すべての必要な証明書を受け入れたら、サインイン プロセスは終了です。

エージェントがデスクトップにサインイン可能かの確認

システム管理者が設定を定義して、サービスが再起動されると、パスワードと運用のハンドセットを持つエージェントは Finesse Agent Desktop にサインインできます。

（注） Finesse を再起動すると、すべてのサーバ関連のサービスの再起動に約 6 分かかります。 そのため、6 分待ってからデスクトップにサインインを試みてください。

（注） HTTPS を使用する場合、エージェント デスクトップに初めてアクセスすると、ブラウザにセキュリティ警告が表示されます。 サインインするたびにブラウザにセキュリティ警告が表示されないようにするには、Finesse に付属の自己署名証明書を信頼するか、CA 証明書を取得してアップロードします。

手順

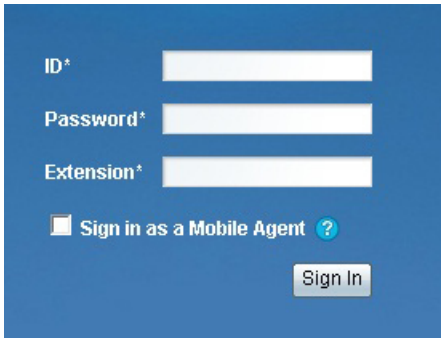
ステップ 1 ブラウザのアドレス バーに次の URL を入力します。
http://*Finesse* サーバの *FQDN*、ホスト名、または *IP* アドレス

ステップ 2 言語パック COP ファイルをインストールする場合は、[Language Selector] ドロップダウン リストからデスクトップに表示する言語を選択できます。 言語パック COP ファイルをインストールしなかった場合は、[Language Selector] ドロップダウン リストは、ユーザ インターフェイスに表示されません。

（注） 言語パック COP ファイルをインストールする場合、URL の一部としてロケールを渡すことによっても、言語を選択できます（たとえば、http://*Finesse* サーバの *FQDN*、ホスト名、または *IP* アドレス/desktop?locale=fr_FR）または、ブラウザで使用する言語を変更しても選択できます。 デフォルトの言語は英語です（en_US）。

ステップ 3 エージェント ID またはユーザ名、パスワード、および内線番号を入力して [Sign In] をクリックします。

図 *1*：デスクトップのサインイン



フェイルオーバー機能の正確な確認

Finesse は、フェールオーバーが正常に動作しているかを確認するための Finesse デスクトップで実行できる診断ツールを提供しています。

（注） このツールで正確な診断を行うには、代替 Finesse サーバがアクセス可能で稼働中である必要があります

手順

ステップ 1 Finesse デスクトップにサインインします。

ステップ 2 ブラウザのアドレス バーに次の URL を入力します。
http://*Finesse* サーバの *FQDN*、ホスト名、または *IP* アドレス/desktop/failover

ツールはフェールオーバーテストのシミュレーションを実行して、結果を表示します。テストに合格した場合、次のメッセージが表示されます。

Test sequence passed for failover to <Finesse alternate server name>. Click OK to test failback by running the test sequence from <Finesse alternate server name>.

ステップ 3 フェールバックをテストするには、[OK] をクリックします。

（注） フェールオーバーテストに失敗すると、サーバはアクセスできない場合があります（たとえば、証明書の例外によりブラウザのアクセスがブロックされることがあります）。そうなっていないことを確認するには、代替 Finesse サーバに直接 FQDN を使用してアクセスし、手動でデスクトップにサインインしてみてください。 サインインが成功すると、特定のブラウザ設定やポリシーが、フェールオーバーの誤動作の原因である可能性があります。 たとえば FQDN ではないホスト名または IP アドレスを持つ Finesse にアクセスした場合、それぞれがサードパーティ製であると見なされるため 2 つのサーバ間でのアクセスにブラウザがクライアント側のセキュリティ制限がかかることがあります。 2 台のサーバが同じドメイン内にあり、FQDN を使用してアクセスされる場合、これらの制限は厳密ではありません。

関連トピック

Internet Explorer のブラウザ設定, （7 ページ）

クライアントでの DNS 設定

（注） この手順は、非階層型 DNS 設定が存在する特殊な環境で必要です。 環境に階層型 DNS 設定がある場合は、この手順を実行する必要はありません。 この手順は、Windows オペレーティング システムを使用するクライアントに適用されます。 Mac クライアントの DNS 設定については、Apple ドキュメント（www.apple.com/mac）を参照してください。

クライアント コンピュータの DNS 設定で、クライアントは、フェイルオーバー時に実行中の Finesse サーバの完全修飾ドメイン名（FQDN）を解決することができます。

手順

ステップ 1 [Control Panel] > [Network and Internet] > [Network and Sharing Center] に進みます。（[Control Panel] を開き、検索バーでネットワーク接続を入力し、[View network connections] をクリックします）。

ステップ 2 適切なネットワーク接続をクリックします。
接続状態を示すダイアログ ボックスが表示されます。

ステップ 3 **[Properties]** をクリックします。

ステップ 4 [Networking] タブで、[Internet protocol version 4 (TCP/IPv4)] を選択し、**[Properties]** をクリックします。

ステップ 5 **[Advanced]** をクリックします。

ステップ 6 [DNS] タブの [DNS server addresses] で使用する順に **[Add]** をクリックします。

ステップ 7 インストール時に入力した DNS サーバの IP アドレスを入力し、**[Add]** をクリックします。

ステップ 8 インストール時にセカンダリ DNS を入力した場合は、ステップ 5 とステップ 6 を繰り返して IP アドレスを追加してください。

初期設定のトラブルシューティング

If	解決策
管理コンソールが初回インストール後にロードされません。	1 ブラウザのキャッシュをクリア（参照履歴およびクッキーを削除）します。 2 問題が続く場合は、Cisco Tomcat サービスを再起動するか、Finesse サーバを再起動します。

If	解決策
新規インストール後に、エージェントでデスクトップにサインインできません。	

If	解決策
	1 エージェント ID とパスワードが正しいかどうかを確認します。 **2** インストール中に有効なドメイン名が設定されているかどうかと、順方向および逆方向 DNS が正常に設定されているかどうかを確認します。 DNS がインストール中に設定されているかどうかを確認するには、次のようにして install.log を確認してください。 InstallWizard|USER_ACTION_BTN_PUSH: Screen = DNS Client Configuration, button pushed = No|<LVL::Info 上のメッセージは、DNS がインストール中に設定されていないことを示します。 Finesse を再インストールして、有効なドメインと DNS を設定します。 **3** エージェントが Unified CCE で設定されていることを確認します。 **4** AWDB が正しく設定されていることを確認します。 **a** 次の行については、realm.log をチェックしてください: "ERROR com.cisco.ccbu.finesse.realms.ccerealm.CCERealmConfig - Cannot connect to any AWDB! Ensure that at least one AWDB is configured properly and running!" この行は、Finesse が AWDB に接続できないことを示しています。 **b** Contact Center Enterprise の Administration & Data Server 設定ガジェットで入力した値が正しいか確認してください。 • 送信されたユーザ名が Windows ドメインユーザであることを確認します。 • ユーザ名がドメインに追加（例：domain\username）されていないことを確認します。 • 設定されているポートが Finesse サーバに開いていることを確認します。 **c** AWDB が正しく設定され実行されていることを確認します。 • AWDB SQL Server では Windows 認証を使用する必要があります。 • AWDB サーバが稼働しており、ディストリビュータサービスが動作していることを確認します。

If	解決策
	5 プライマリおよびセカンダリ Finesse サーバで Cisco Tomcat を再起動します。 6 エージェントのデバイスが Unified Communications Manager に正しく設定されており、アクティブであることを確認します。

関連トピック

ログの収集