Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）

この章では、Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）について説明します。

HTTPS

HTTPS（Hypertext Transfer Protocol over Secure Sockets Layer（SSL））は、Microsoft Windows ユーザ向けにブラウザと Web サーバの間の通信を保護します。HTTPS は証明書を使用して、サーバのアイデンティティを保証し、ブラウザ接続を保護します。HTTPS では、インターネット経由での転送で公開キーを使用してユーザ ログインやパスワードなどのデータを暗号化します。

Unified Communications Manager は、HTTPS 接続の SSL および Transport Layer Security（TLS）をサポートしています。ご使用の Web ブラウザ バージョンが TLS をサポートしている場合、セキュリティ強化のために TLS を使用することを推奨します。セキュアな HTTPS 通信のために TLS を使用するには、Web ブラウザで SSL を無効にします。

HTTPS を有効にするには、接続プロセス中にサーバ識別用の証明書をダウンロードする必要があります。現在のセッションだけにサーバ証明書を使用するか、サーバでの現在のセッションと将来のセッションを保護するために信頼フォルダ（ファイル）に証明書をダウンロードすることができます。信頼フォルダには、すべての信頼済みサイトの証明書が保存されます。

Unified Communications Manager での Cisco Tomcat Web サーバ アプリケーションとの接続について、シスコでは次のブラウザをサポートしています。

- Microsoft Windows XP SP3 上で動作している場合は、Microsoft Internet Explorer（IE）7

- Microsoft Windows XP SP3 または Microsoft Vista SP2 上で動作している場合は、Microsoft Internet Explorer（IE）8
- Microsoft Windows XP SP3、Microsoft Vista SP2 または Apple MAC OS X 上で動作している場合は、Firefox 3.x
- Apple MAC OS X 上で動作している場合は、Safari 4.x

（注） Unified Communications Manager をインストールまたはアップグレードすると、HTTPS 自己署名証明書（Tomcat）が生成されます。この自己署名証明書は、Unified Communications Manager へのアップグレード時に自動的に移行されます。この証明書のコピーは .DER および .PEM 形式で作成されます。

自己署名証明書は、Cisco Unified Communications Operating System GUI を使用して再生成できます。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Unified Communications Manager で Cisco Tomcat との間で HTTPS を使用するアプリケーションを次の表に示します。

表 *1 : Unified Communications Manager HTTPS* アプリケーション

Unified Communications Manager HTTPS アプリケーション	**Web アプリケーション**
ccmadmin	Unified Communications Manager Administration
ccmservice	Cisco Unified Serviceability
cmplatform	オペレーティング システムの管理ページ
cmuser	Cisco Personal Assistant
ast	Real Time Monitoring Tool
RTMTReports	Real Time Monitoring Tool レポート アーカイブ
PktCap	パケット キャプチャに使用される TAC トラブルシューティング ツール
art	Unified Communications Manager CDR Analysis and Reporting
taps	Unified Communications Manager Auto-Register Phone Tool
dna	Dialed Number Analyzer
drf	Disaster Recovery System

Unified Communications Manager HTTPS アプリケーション	Web アプリケーション
SOAP	Unified Communications Manager データベースの読み取り/書き込み用の Simple Object Access Protocol API （注） セキュリティのため、SOAP を使用するすべての Web アプリケーションで HTTPS が必要です。SOAP アプリケーションの場合 HTTP はサポートされていません。HTTP を使用する既存のアプリケーションは実行に失敗します。ディレクトリ変更によって HTTPS に変換することはできません。

Cisco Unified IP Phone サービスの HTTPS

Unified Communications Manager、Cisco IP Phone、および Cisco Unified IP Phone の各サービスでは、HTTPS、暗号化、およびポート 8443 を使用したサーバのセキュアな識別がサポートされています。

TVS（信頼検証サービス）では証明書チェーンは確認されません。TVS が証明書を確認するためには、電話によって TVS に提示されるのと同じ証明書が Tomcat 信頼証明書ストア内に存在する必要があります。

TVS では、ルート証明書や中間証明書は確認されません。アイデンティティ証明書のみ、データベースに存在しない場合に確認されます。ルート証明書および中間証明書が提示された場合でも、検証は失敗します。

HTTPS をサポートする Cisco Unified IP Phone

次の Cisco IP Phone では、HTTPS がサポートされています。

- 6901、6911、6921、6941、6945、6961
- 7811、7821、7832、7841、7861
- 7906、7911、7925、7925-EX、7926、7931、7941、7941G-GE、7942、7945、7961、7962、7961G-GE、7965、7975
- 8811、8821、8831、8832、8841、8845、8851、8851NR、8861、8865、8865NR
- 8941、8945、8961
- 9951、9971

（注） このリストの 69xx 電話は、HTTPS クライアントとして動作可能ですが、HTTPS サーバとしての動作はできません。このリスト内の残りの電話は、HTTPS クライアントまたは HTTPS サーバとして動作可能です。

HTTPS をサポートする機能

次の機能で HTTPS がサポートされています。

- Cisco Extension Mobility（EM）
- Cisco Extension Mobility Cross Cluster（EMCC）
- Cisco Unified Communications Manager Manager Assistant（IPMA）
- Cisco Unified IP Phone サービス
- パーソナル ディレクトリ
- クレデンシャルの変更

Cisco Unified IP Phone サービスの設定

Unified Communications Manager リリース 8.0(1) 以降では、HTTPS をサポートするため、次の表に示すセキュア URL パラメータが電話の設定に含まれるようになりました。

セキュア URL の各パラメータを設定するには、[Unified Communications Manager Administration] から **[Device]** > **[Device Settings]** > **[Phone Services]** を選択します。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

（注） [Cisco Unified Communications Manager Administration] の [Enterprise Parameters] セクションで Secured Phone URL パラメータを削除してリブートすると、デフォルトで URL パラメータが再度読み込まれます。リブートの後、[Secured Phone URL Parameters] セクションに移動し、正しい URL に変更して電話を再起動します。

表 *2:* セキュア *URL* の電話の設定

フィールド	説明
[Secure Service URL]	電話 Web サーバに対する要求を検証するために電話で使用されるセキュア URL を入力します。 （注） セキュア認証 URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルトでは、この URL はインストール中に設定された [Cisco Unified Communications Self Care Portal] ウィンドウにアクセスします。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[Secure Directory URL]	電話のディレクトリ情報の取得元となるサーバの URL を入力します。このパラメータには、ユーザが [Directory] ボタンを押したときにセキュアな Cisco IP Phone が使用する URL を指定します。 （注） セキュア ディレクトリ URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

フィールド	説明
[Secure Idle URL]	電話が [Idle Timer] フィールドで指定された時間アイドルだったときに Cisco IP Phone に表示される情報のセキュア URL を入力します。たとえば、電話が 5 分間使用されなかったときに、LCD にロゴを表示できます。 （注） セキュア アイドル URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[Secure Information URL]	Cisco IP Phone がヘルプ テキストの情報を取得するサーバの場所を示す URL を入力します。この情報は、ユーザが電話の情報ボタン（i）またはヘルプ ボタン（?）ボタンを押したときに表示されます。 （注） セキュア情報 URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

フィールド	説明
[Secure Messages URL]	メッセージ サーバのセキュア URL を入力します。ユーザが [Messages] ボタンを押すと、Cisco IP Phone はこの URL にアクセスします。 （注） セキュア メッセージ URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[Secure Services URL]	Cisco Unified IP Phone サービスのセキュア URL を入力します。これは、ユーザが [Services] ボタンを押したときにセキュア Cisco Unified IP Phone がアクセスする場所になります。 （注） セキュア サービス URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

HTTPS をサポートするためのエンタープライズ パラメータの設定

HTTPS をサポートするため、Unified Communications Manager リリース 8.0(1) 以降では次の新しいエンタープライズ パラメータがサポートされています。

- [Secured Authentication URL]
- [Secured Directory URL]
- [Secured Idle URL]
- [Secured Information URL]
- [Secured Messaged URL]
- [Secured Services URL]

Internet Explorer 8 を使用して証明書を信頼できるフォルダに保存

ブラウザを再起動するたびに証明書をリロードしなくても安全なアクセスが行えるよう、Unified Communications Manager の証明書を Internet Explorer 8 にインポートしてください。Web サイトで証明書に対する警告が表示され、証明書が信頼ストアにない場合、Internet Explorer 8 は現在のセッションの間だけ証明書を記憶します。

サーバ証明書をダウンロードした後も、Internet Explorer 8 ではその Web サイトに対する証明書エラーが引き続き表示されます。このセキュリティの警告は、ブラウザの信頼ルート認証局の信頼できるストアにインポートされた証明書が含まれている場合には無視できます。

次の手順では、Internet Explorer 8 のルート証明書の信頼ストアに Unified Communications Manager の証明書をインポートする方法について説明します。

手順

ステップ 1 Tomcat サーバのアプリケーションを参照します（たとえば、Unified Communications Manager Administration のホスト名、localhost または IP アドレスをブラウザに入力します）。

ブラウザに「Certificate Error: Navigation Blocked」というメッセージが表示されます。これはこの Web サイトは信頼できないことを示しています。

ステップ 2 サーバにアクセスするには、[Continue to this website (not recommended)] をクリックします。

[Unified Communications Manager Administration] ウィンドウが表示され、ブラウザにアドレスバーと証明書のエラーのステータスが赤色で表示されます。

ステップ 3 サーバ証明書をインポートするには、[Certificate Error] ステータス ボックスをクリックして、ステータス レポートを表示します。レポートの [View Certificates] リンクをクリックします。

ステップ 4 証明書の詳細を確認します。

ステップ 5 [Certificate] ウィンドウで [General] タブを選択し、[Install Certificate] をクリックします。

証明書のインポート ウィザードが起動します。

ステップ 6 ウィザードを起動するには、[Next] をクリックします。

[Certificate Store] ウィンドウが表示されます。

ステップ 7 [Automatic] オプションが選択されていることを確認します。これを選択すると、ウィザードでこの証明書タイプの証明書ストアを選択できるようになります。[Next] をクリックします。

ステップ 8 設定を確認し、[Finish] をクリックします。

インポート操作に対してセキュリティ警告が表示されます。

ステップ 9 証明書をインストールするには、[Yes] をクリックします。

インポート ウィザードに「「The import was successful.」」と表示されます。

ステップ 10 [OK] をクリックします。**[View Certificates]** リンクを次にクリックしたときには、[Certificate Path] ウィンドウの **[Certification Path]** タブに「「This certificate is OK.」」と表示されます。

ステップ 11 信頼ストアにインポートした証明書が含まれていることを確認するには、Internet Explorer のツールバーの **[Tools]** > **[Internet Options]** をクリックして、**[Content]** タブを選択します。[Certificates] をクリックして、[Trusted Root Certifications Authorities] タブを選択します。インポートした証明書が見付かるまでリストをスクロールします。

証明書のインポート後、ブラウザには引き続きアドレスバーと証明書エラーのステータスが赤色で表示されます。このステータスは、ホスト名、localhost または IP アドレスを入力したり、ブラウザを更新または再起動した場合でも表示されます。

Internet Explorer 8 証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1 [Certificate Error] ステータス ボックスをクリックします。

ステップ 2 [View Certificate] をクリックします。

ステップ 3 [Details] タブをクリックします。

ステップ 4 [Copy to File] ボタンをクリックします。

ステップ 5 [Certificate Export Wizard] が表示されます。[Next] をクリックします。

ステップ 6 次のリストに、選択可能なファイル形式を定義しています。エクスポートするファイルに使用するファイル形式を選択し、[Next] をクリックします。

a) [DER encoded binary X.509 (.CER)]：エンティティ間の情報転送で DER を使用します。
b) [Base-64 encoded X.509 (.CER)]：バイナリ添付ファイルをインターネット上でセキュアに送信できます。ファイルの文字化けを防ぐため、ASCII テキスト形式を使用します。
c) [Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)]：証明書自体と、選択した PC の認証パスにあるすべての証明書をエクスポートします。

ステップ 7 ファイルのコピーをエクスポートし、ファイル名を設定する場所を参照します。**[Save]** をクリックします。

ステップ 8 ファイル名とパスは [Certificate Export Wizard] ペインに表示されます。[Next] をクリックします。

ステップ 9 ファイルと設定が表示されます。[Finish] をクリックします。

ステップ 10 エクスポートの成功を示すダイアログボックスが表示されたら、[OK] をクリックします。

HTTPS による Firefox での初回の認証

Unified Communications Manager のインストールまたはアップグレード後に、[Unified Communications Manager Administration] またはその他の Unified Communications Manager SSL 対応仮想ディレクトリにユーザがブラウザクライアントから初めてアクセスすると、サーバを信頼するかどうかを尋ねる [Security Alert] ダイアログボックスが表示されます。

このダイアログボックスが表示された場合、次のいずれかの作業を行う必要があります。

- **[I Understand The Risks]** をクリックすると、現在の Web セッションの間だけ証明書を信頼することになります。現在のセッションの間だけ証明書を信頼する場合は、アプリケーションにアクセスするたびに [Security Alert] ダイアログボックスが表示されます。つまり、信頼できるフォルダに証明書をインストールするまでこのダイアログボックスが表示されることになります。
- **[Get Me Out Of Here]** をクリックすると、操作がキャンセルされます。認証が行われないため、Webアプリケーションにアクセスできません。Webアプリケーションにアクセスするには、**[I Understand The Risks]** をクリックする必要があります。

Firefox 3.x を使用して証明書を信頼できるフォルダに保存

ブラウザ クライアントで HTTPS 証明書を信頼できるフォルダに保存するには、次の手順を実行します。

手順

ステップ 1 Tomcat サーバにアクセスします（たとえば、ブラウザに [Cisco Unified Communications Manager Administration] のホスト名、ローカルホスト、または IP アドレスを入力します）。

ステップ 2 [Security Alert] ダイアログボックスが表示されたら、[I Understand The Risks] をクリックします。

ステップ 3 [Add Exception] をクリックします。

[Add Exception] ダイアログボックスが表示されます。

ステップ 4 [Get Certificate] をクリックします。

ステップ 5 [Permanently store this exception] チェックボックスをオンにします。

ステップ 6 [Confirm Security Exception] をクリックします。

ステップ 7 次の手順を実行して証明書の詳細を表示します。

a) Firefox ブラウザで **[Tools]** > **[Options]** をクリックします。

[Options] ダイアログボックスが表示されます。

b) [Advanced] をクリックします。
c) [View Certificate] をクリックします。

[Certificate Manager] ダイアログボックスが表示されます。

d) 表示する証明書を強調表示して [View] をクリックします。

[Certificate Viewer] ダイアログボックスが表示されます。

e) [Details] タブをクリックします。
f) [Certificate Fields] フィールドで、表示するフィールドを強調表示します。

詳細は [Field Values] フィールドに表示されます。

g) [Certificate Viewer] ダイアログボックスで [Close] をクリックします。
h) [Certificate Viewer] ダイアログボックスで [OK] をクリックします。

Firefox 3.x 証明書のファイルへのコピー

証明書をファイルにコピーし、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1 Firefox ブラウザで **[Tools]** > **[Options]** をクリックします。

[Options] ダイアログボックスが表示されます。

ステップ 2 選択されていなければ、[Advanced] をクリックします。

ステップ 3 [Security] タブをクリックし、[View Certificates] をクリックします。

[Certificate Manager] ダイアログボックスが表示されます。

ステップ 4 [Servers] タブをクリックします。

ステップ 5 コピーする証明書を強調表示して [Export] をクリックします。

[Save Certificate to File] ダイアログボックスが表示されます。

ステップ 6 ファイルをコピーする場所に移動します。

ステップ 7 [Save as type] ドロップダウン リストで、ファイル タイプを次のオプションから選択します。

a) [X.509 Certificate (PEM)]：エンティティ間の情報転送で **PEM** を使用します。
b) [X.509 Certificate with chain (PEM)]：証明書チェーンを検証し、エンティティ間で情報を転送するために、プライバシー強化メール（Privacy Enhanced Mail）を使用します。

- [X.509 Certificate (DER)]：エンティティ間の情報転送で **DER** を使用します。

- [X.509 Certificate (PKCS#7)]：PKCS#7 は署名、データ暗号化のための標準規格です。署名されたデータを確認するには証明書が必要であるため、これを SignedData 構造に含めることができます。A .P7C ファイルは、署名するデータを持たない、退化した SignedData 構造です。
- [X.509 Certificate with chain (PKCS#7)]：証明書チェーンを検証し、エンティティ間で情報を転送するために、PKCS#7 を使用します。

ステップ 8 **[保存（Save）]** をクリックします。

ステップ 9 [OK] をクリックします。

HTTPS による Safari での初回の認証

Unified Communications Manager のインストールまたはアップグレード後に、[Unified Communications Manager Administration] またはその他の Unified Communications Manager SSL 対応仮想ディレクトリにユーザがブラウザクライアントから初めてアクセスすると、サーバを信頼するかどうかを尋ねる [Security Alert] ダイアログボックスが表示されます。

このダイアログボックスが表示された場合、次のいずれかの作業を行う必要があります。

- [Yes] をクリックすると、現在の Web セッションの間だけ証明書を信頼することになります。現在のセッションの間だけ証明書を信頼する場合は、アプリケーションにアクセスするたびに [Security Alert] ダイアログボックスが表示されます。つまり、信頼できるフォルダに証明書をインストールするまでこのダイアログボックスが表示されることになります。
- **[Show Certificate]** > **[Install Certificate]** をクリックして、証明書のインストール作業を実行し、証明書を常に信頼することを示します。証明書を信頼できるフォルダにインストールすると、Web アプリケーションにアクセスするごとに [Security Alert] ダイアログボックスが表示されなくなります。
- [No] をクリックすると、操作がキャンセルされます。認証が行われないため、Web アプリケーションにアクセスできません。Web アプリケーションにアクセスするには、[Yes] をクリックするか、または **[Show Certificate]** > **[Install Certificate]** オプションを選択して証明書をインストールする必要があります。

（注） Unified Communications Manager へのアクセスに使用するアドレスは、証明書にある名前と一致する必要があります。一致しない場合は、デフォルトでメッセージが表示されます。信頼できるフォルダに証明書をインストールした後、ローカル ホストまたは IP アドレスを使用してその Web アプリケーションにアクセスすると、セキュリティ証明書の名前とアクセスするサイトの名前が一致しないことを示すセキュリティの警告が表示されます。

Safari 4.x を使用して証明書を信頼できるフォルダに保存

ブラウザ クライアントで HTTPS 証明書を信頼できるフォルダに保存するには、次の手順を実行します。

手順

ステップ 1 Tomcat サーバにアクセスします（たとえば、ブラウザに [Cisco Unified Communications Manager Administration] のホスト名、ローカルホスト、または IP アドレスを入力します）。

ステップ 2 [Security Alert] ダイアログボックスが表示されたら、[Show Certificate] をクリックします。

証明書のデータを確認する場合は、[Details] タブをクリックして、証明書の詳細を表示できます。設定のサブセットを表示するには（使用可能な場合）、次のオプションのいずれか 1 つを選択します。

a) [All]：すべてのオプションが [Details] ペインに表示されます。
b) [Version 1 Fields Only]：[Version]、[Serial Number]、[Signature Algorithm]、[Issuer]、[Valid From]、[Valid To]、[Subject]、および [Public Key] の各オプションが表示されます。
c) [Extensions Only]：[Subject Key Identifier]、[Key Usage]、および [Enhanced Key Usage] の各オプションが表示されます。
d) [Critical Extensions Only]：存在する場合は [Critical Extensions] が表示されます。
e) [Properties Only]：[Thumbprint algorithm] と [Thumbprint] オプションが表示されます。

ステップ 3 [Certificate] ペインの [Install Certificate] をクリックします。

ステップ 4 [Certificate Import Wizard] が表示されたら、[Next] をクリックします。

ステップ 5 [Place all certificates in the following store] オプション ボタンをクリックし、[Browse] をクリックします。

ステップ 6 [Trusted Root Certification Authorities] を参照し、選択して、[OK] をクリックします。

ステップ 7 [次へ（Next）] をクリックします。

ステップ 8 [完了（Finish）] をクリックします。

[Security Warning] ボックスに証明書の拇印が表示されます。

ステップ 9 証明書をインストールするには、[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。[OK] をクリックします。

ステップ 10 ダイアログボックスの右下隅にある [OK] をクリックします。

ステップ 11 証明書を信頼して、ダイアログボックスが今後表示されないようにするには、[Yes] をクリックします。

ヒント [Certificate] ペインの [Certification Path] タブをクリックして、証明書が正常にインストールされたことを確認できます。

ファイルへの Safari 4.x 証明書のコピー

証明書をファイルにコピーし、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1 [Security Alert] ダイアログボックスで、[Show Certificate] をクリックします。

ヒント Safari で、[Certificate Error] ステータス ボックスをクリックして、[Show Certificate] オプションを表示します。

ステップ 2 [Details] タブをクリックします。

ステップ 3 [Copy to File] ボタンをクリックします。

ステップ 4 [Certificate Export Wizard] が表示されます。[Next] をクリックします。

ステップ 5 次のリストに、選択可能なファイル形式を定義しています。エクスポートするファイルに使用するファイル形式を選択し、[Next] をクリックします。

a) [DER encoded binary X.509 (.CER)]：エンティティ間の情報転送で DER を使用します。

b) [Base-64 encoded X.509 (.CER)]：バイナリ添付ファイルをインターネット上でセキュアに送信できます。ファイルの文字化けを防ぐため、ASCII テキスト形式を使用します。

c) [Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)]：証明書自体と、選択した PC の認証パスにあるすべての証明書をエクスポートします。

ステップ 6 ファイルのコピーをエクスポートし、ファイル名を設定する場所を参照します。**[Save]** をクリックします。

ステップ 7 ファイル名とパスは [Certificate Export Wizard] ペインに表示されます。[Next] をクリックします。

ステップ 8 ファイルと設定が表示されます。[Finish] をクリックします。

ステップ 9 エクスポートの成功を示すダイアログボックスが表示されたら、[OK] をクリックします。

HTTPS 設定に関する詳細情報の入手先

関連するシスコのドキュメント

- 『*Cisco Unified Serviceability Administration Guide*』
- 『*Administration Guide for Cisco Unified Communications Manager*』
- HTTPS に関して利用可能な Microsoft のドキュメント