



セキュリティ

この章では、証明書の管理と IPSec の管理について説明し、次のタスクを実行する手順を示します。

- [Internet Explorer のセキュリティ オプションの設定](#)
- [証明書と証明書信頼リストの管理](#)
- [IPSEC の管理](#)

Internet Explorer のセキュリティ オプションの設定

サーバから証明書をダウンロードするには、Internet Explorer のセキュリティ設定値が次のように設定されていることを確認します。

手順

- ステップ 1** Internet Explorer を起動します。
 - ステップ 2** [ツール] > [インターネット オプション] に移動します。
 - ステップ 3** [詳細設定] タブをクリックします。
 - ステップ 4** [詳細設定] タブで、[セキュリティ] セクションまでスクロールダウンします。
 - ステップ 5** 必要に応じて、[暗号化されたページをディスクに保存しない] チェックボックスをオフにします。
 - ステップ 6** [OK] をクリックします。
-

証明書と証明書信頼リストの管理

次の各トピックでは、[証明書の管理 (Certificate Management)] メニューから実行できる機能について説明します。

- [証明書の表示](#)
- [証明書または CTL のダウンロード](#)
- [証明書の削除と再生成](#)
- [証明書または証明書信頼リストのアップロード](#)
- [サードパーティの CA 証明書の使用方法](#)
- [証明書の有効期限の監視](#)



(注)

[セキュリティ (Security)] メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications オペレーティング システムの管理に再度ログインする必要があります。

証明書の表示

既存の証明書を表示するには、次の手順を実行します。

手順

ステップ 1 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 検索条件フィールドを使用して、証明書リストをフィルタリングできます。

ステップ 3 証明書または信頼ストアの詳細を表示するには、そのファイル名をクリックします。

[証明書の設定 (Certificate Configuration)] ウィンドウに、証明書に関する情報が表示されます。

ステップ 4 [証明書の一覧 (Certificate List)] ウィンドウに戻るには、[関連リンク (Related Links)] リストで [検索 / リストに戻る (Back To Find/List)] を選択し、[移動 (Go)] をクリックします。

証明書または CTL のダウンロード

Cisco Unified Communications オペレーティング システムから PC に証明書または CTL をダウンロードするには、次の手順を実行します。

手順

ステップ 1 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 検索条件フィールドを使用して、証明書リストをフィルタリングできます。

ステップ 3 証明書または CTL のファイル名をクリックします。

[証明書の設定 (Certificate Configuration)] ウィンドウが表示されます。

ステップ 4 [ダウンロード (Download)] をクリックします。

ステップ 5 [ファイルのダウンロード] ダイアログボックスで、[保存] をクリックします。

証明書の削除と再生成

次の各項では、証明書の削除と再生成について説明します。

- [証明書の削除](#)
- [証明書の再生成](#)

証明書の削除

trusted certificate を削除するには、次の手順を実行します。



証明書を削除すると、システムの動作に影響する場合があります。

手順

ステップ 1 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 検索条件フィールドを使用して、証明書リストをフィルタリングできます。

ステップ 3 証明書または CTL のファイル名をクリックします。

[証明書の設定 (Certificate Configuration)] ウィンドウが表示されます。

ステップ 4 [削除 (Delete)] をクリックします。

証明書の再生成

証明書を再生成するには、次の手順を実行します。



注意

証明書を再生成すると、システムの動作に影響する場合があります。

手順

ステップ 1 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 [新規作成 (Generate New)] をクリックします。

[証明書の作成 (Generate Certificate)] ダイアログボックスが開きます。

ステップ 3 [証明書の名前 (Certificate Name)] リストから、証明書の名前を選択します。

ステップ 4 [新規作成 (Generate New)] をクリックします。

証明書または証明書信頼リストのアップロード



注意

新しい証明書ファイルまたは Certificate Trust List (CTL; 証明書信頼リスト) ファイルをアップロードすると、システムの動作に影響する場合があります。

次の各項では、CA ルート証明書、アプリケーション証明書、または CTL ファイルをサーバにアップロードする方法について説明します。

- [証明書のアップロード](#)
- [証明書信頼リストのアップロード](#)
- [ディレクトリ信頼証明書のアップロード](#)

証明書のアップロード

手順

ステップ 1 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 [証明書のアップロード (Upload Certificate)] をクリックします。

[証明書のアップロード (Upload Certificate)] ダイアログボックスが開きます。

- ステップ 3** [証明書の名前 (Certificate Name)] リストから、証明書の名前を選択します。
- ステップ 4** サードパーティの CA から発行されたアプリケーション証明書をアップロードする場合は、[ルート証明 (Root Certificate)] テキストボックスに、CA ルート証明書の名前を入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにしておきます。
- ステップ 5** 次のいずれかの手順を実行して、アップロードするファイルを選択します。
- [ファイルのアップロード (Upload File)] テキストボックスに、ファイルへのパスを入力します。
 - [参照] ボタンをクリックし、アップロードするファイルに移動してから、[開く] をクリックします。
- ステップ 6** ファイルをサーバにアップロードするには、[ファイルのアップロード (Upload File)] ボタンをクリックします。
-

証明書信頼リストのアップロード

手順

- ステップ 1** [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。
- [証明書の一覧 (Certificate List)] ウィンドウが表示されます。
- ステップ 2** [CTL のアップロード (Upload CTL)] をクリックします。
- [証明書信頼リストのアップロード (Upload Certificate Trust List)] ダイアログボックスが開きます。
- ステップ 3** [証明書の名前 (Certificate Name)] リストから、証明書の名前を選択します。
- ステップ 4** サードパーティの CA から発行されたアプリケーション証明書をアップロードする場合は、[ルート証明 (Root Certificate)] テキストボックスに、CA ルート証明書の名前を入力します。CA ルート証明書をアップロードする場合は、このテキストボックスを空白のままにしておきます。
- ステップ 5** 次のいずれかの手順を実行して、アップロードするファイルを選択します。
- [ファイルのアップロード (Upload File)] テキストボックスに、ファイルへのパスを入力します。
 - [参照] ボタンをクリックし、アップロードするファイルに移動してから、[開く] をクリックします。
- ステップ 6** ファイルをサーバにアップロードするには、[ファイルのアップロード (Upload File)] ボタンをクリックします。
-

ディレクトリ信頼証明書のアップロード

手順

-
- ステップ 1** [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。
- [証明書の一覧 (Certificate List)] ウィンドウが表示されます。
- ステップ 2** [CTL のアップロード (Upload CTL)] をクリックします。
- [証明書信頼リストのアップロード (Upload Certificate Trust List)] ダイアログボックスが開きます。
- ステップ 3** [証明書の名前 (Certificate Name)] リストから、**directory-trust** を選択します。
- ステップ 4** [ファイルのアップロード (Upload File)] フィールドに、アップロードするファイルを入力します。
- ステップ 5** ファイルをアップロードするには、[ファイルのアップロード (Upload File)] ボタンをクリックします。
- ステップ 6** Cisco Unified Serviceability にログインします。
- ステップ 7** [Tools] > [Control Center - Feature Services] に移動します。
- ステップ 8** サービス **Cisco Dirsync** を再起動します。
- ステップ 9** Cisco Unified Communications オペレーティング システム CLI に管理者としてログインします。
- ステップ 10** コマンド **utils service restart Cisco Tomcat** を入力し、Tomcat サービスを再起動します。
- ステップ 11** サービスを再起動した後、SSL のためのディレクトリ契約を追加できます。
-

サードパーティの CA 証明書の使用方法

Cisco Unified Communications オペレーティング システムは、サードパーティの Certificate Authority (CA; 認証局) が PKCS # 10 Certificate Signing Request (CSR; 証明書署名要求) によって発行する証明書をサポートしています。次の表に、このプロセスの概要と参照先のドキュメントを示します。

| | タスク | 参照先 |
|---------------|----------------------------------|---|
| ステップ 1 | サーバ上で CSR を生成する。 | P.6-7 の「証明書署名要求の生成」 を参照してください。 |
| ステップ 2 | CSR を PC にダウンロードする。 | P.6-8 の「証明書署名要求のダウンロード」 を参照してください。 |
| ステップ 3 | CSR を使用して、CA からアプリケーション証明書を取得する。 | アプリケーション証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、 P.6-8 の「サードパーティの CA 証明書の取得」 を参照してください。 |
| ステップ 4 | CA ルート証明書を取得する。 | ルート証明書の取得に関する情報は、CA から入手してください。その他の注意事項については、 P.6-8 の「サードパーティの CA 証明書の取得」 を参照してください。 |

| | タスク | 参照先 |
|--------|---|--|
| ステップ 5 | CA ルート証明書をサーバにアップロードする。 | P.6-4 の「証明書のアップロード」を参照してください。 |
| ステップ 6 | アプリケーション証明書をサーバにアップロードする。 | P.6-4 の「証明書のアップロード」を参照してください。 |
| ステップ 7 | CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、新しい CTL ファイルを生成する。 | 『Cisco Unified Communications Manager セキュリティ ガイド』を参照してください。 |
| ステップ 8 | 新しい証明書によって影響を受けるサービスを再起動する。 | すべての証明書タイプで、対応するサービスを再起動します (たとえば、Tomcat 証明書を更新した場合は、Tomcat サービスを再起動します)。さらに、CAPF または Cisco Unified Communications Manager の証明書を更新した場合は、TFTP サービスを再起動します。 サービスの再起動については、『Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド』を参照してください。 |

証明書署名要求の生成

証明書署名要求 (CSR) を生成するには、次の手順を実行します。

手順

ステップ 1 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 [CSR の作成 (Generate CSR)] をクリックします。

[証明書署名要求の作成 (Generate Certificate Signing Request)] ダイアログボックスが開きます。

ステップ 3 [証明書の名前 (Certificate Name)] リストから、証明書の名前を選択します。

ステップ 4 [CSR の作成 (Generate CSR)] をクリックします。

証明書署名要求のダウンロード

証明書署名要求をダウンロードするには、次の手順を実行します。

手順

ステップ 1 [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] に移動します。

[証明書の一覧 (Certificate List)] ウィンドウが表示されます。

ステップ 2 [CSR のダウンロード (Download CSR)] をクリックします。

[証明書署名要求のダウンロード (Download Certificate Signing Request)] ダイアログボックスが開きます。

ステップ 3 [証明書の名前 (Certificate Name)] リストから、証明書の名前を選択します。

ステップ 4 [CSR のダウンロード (Download CSR)] をクリックします。

ステップ 5 [ファイルのダウンロード] ダイアログボックスで、[保存] をクリックします。

サードパーティの CA 証明書の取得

サードパーティの CA が発行するアプリケーション証明書を使用するには、CA から署名付きアプリケーション証明書と CA ルート証明書の両方を取得する必要があります。これらの証明書の取得に関する情報は、CA から入手してください。証明書取得プロセスは、CA によって異なります。

CAPF および Cisco Unified Communications Manager の CSR には、CA へのアプリケーション証明書要求に含める必要のある拡張情報が含まれています。CA が ExtensionRequest メカニズムをサポートしていない場合は、CSR 生成プロセスの最後のページに一覧表示される X.509 拡張を有効にする必要があります。

Cisco Unified Communications オペレーティング システムは、証明書を DER および PEM 符号化フォーマットで生成し、CSR を PEM 符号化フォーマットで生成します。また、DER および PEM 符号化フォーマットの証明書を受け入れます。

シスコは、Microsoft、Keon、および Verisign の CA から取得されたサードパーティの証明書を検証済みです。その他の CA からの証明書でも機能する可能性がありますが、未検証です。

証明書の有効期限の監視

証明書が有効期限に近づくと、システムから自動的に電子メールが送信されるようにすることができます。証明書モニタを表示および設定するには、次の手順を実行します。

手順


ステップ 1 Certificate Expiration Monitor の現在の設定を表示するには、[セキュリティ (Security)] > [証明書モニタ (Certificate Monitor)] に移動します。

[証明書モニタ (Certificate Monitor)] ウィンドウが表示されます。

ステップ 2 必要な設定情報を入力します。[証明書モニタ (Certificate Monitor)] の各フィールドの説明については、表 6-1 を参照してください。

ステップ 3 変更内容を保存するには、[保存 (Save)] をクリックします。

表 6-1 [証明書モニタ (Certificate Monitor)] のフィールド説明

| フィールド | 説明 |
|--|--|
| [通知開始時期 (Notification Start Time)] | 証明書が期限切れになる何日前に通知を受け取るかを入力します。 |
| [通知の頻度 (Notification Frequency)] | 通知の頻度を時間単位または日単位で入力します。 |
| [メール通知の有効化 (Enable E-mail Notification)] | このチェックボックスをオンにすると、電子メール通知が有効になります。 |
| [メール ID (Email IDs)] | 通知の送信先となる電子メールアドレスを入力します。 |
| |  <p>(注) システムが通知を送信するためには、SMTP ホストを設定する必要があります。</p> |

IPSEC の管理

次の各トピックでは、[IPSec] メニューから実行できる機能について説明します。

- [新しい IPsec ポリシーの設定](#)
- [既存の IPsec ポリシーの管理](#)

新しい IPsec ポリシーの設定

新しい IPsec ポリシーおよびアソシエーションを設定するには、次の手順を実行します。



(注)

システムのアップグレード中に IPsec ポリシーに対して行った変更は、すべて失われます。そのため、アップグレード中に IPsec ポリシーを修正したり作成したりしないでください。



注意

IPsec は、特に暗号化に関して、システムのパフォーマンスに影響を及ぼします。

手順

- ステップ 1** [セキュリティ (Security)] > [IPSEC 設定 (IPSEC Configuration)] に移動します。
- [IPSEC ポリシーの一覧 (IPSEC Policy List)] ウィンドウが表示されます。
- ステップ 2** [新規追加 (Add New)] をクリックします。
- [IPSEC ポリシーの設定 (IPSEC Policy Configuration)] ウィンドウが表示されます。
- ステップ 3** [IPSEC ポリシーの設定 (IPSEC Policy Configuration)] ウィンドウで、適切な情報を入力します。このウィンドウの各フィールドの説明については、[表 6-2](#) を参照してください。
- ステップ 4** 新しい IPsec ポリシーを設定するには、[保存 (Save)] をクリックします。

表 6-2 IPSEC ポリシーとアソシエーションのフィールド説明

| フィールド | 説明 |
|--------------------------------|---|
| [ポリシー名 (Policy Name)] | IPsec ポリシーの名前を指定します。この名前には、文字、数字、およびハイフンだけを使用できます。 |
| [アソシエーション名 (Association Name)] | 各 IPsec アソシエーションに与えられるアソシエーション名を指定します。この名前には、文字、数字、およびハイフンだけを使用できます。 |
| [認証方式 (Authentication Method)] | 認証方式を指定します。 |
| [共有キー (Preshared Key)] | [認証方式 (Authentication Method)] フィールドで [事前共有キー (Pre-shared Key)] を選択した場合は、事前共有鍵を指定します。 |

表 6-2 IPSEC ポリシーとアソシエーションのフィールド説明 (続き)

| フィールド | 説明 |
|--|---|
| [ピアタイプ (Peer Type)] | ピアが同じタイプであるか異なるタイプであるかを指定します。 |
| [着信先アドレス (Destination Address)] | 宛先の IP アドレスまたは FQDN を指定します。 |
| [着信先ポート (Destination Port)] | 宛先のポート番号を指定します。 |
| [ソースアドレス (Source Address)] | 送信元の IP アドレスまたは FQDN を指定します。 |
| [ソースポート (Source Port)] | 送信元のポート番号を指定します。 |
| [モード (Mode)] | Tunnel モードまたは Transport モードを指定します。 |
| [リモートポート (Remote Port)] | 宛先で使用するポート番号を指定します。 |
| [プロトコル (Protocol)] | 特定のプロトコルまたは [Any] を指定します。 <ul style="list-style-type: none"> • [TCP] • [UDP] • [Any] |
| [暗号化アルゴリズム (Encryption Algorithm)] | ドロップダウン リストから、暗号化アルゴリズムを選択します。選択肢は次のとおりです。 <ul style="list-style-type: none"> • [DES] • [3DES] |
| [ハッシュアルゴリズム (Hash Algorithm)] | ハッシュ アルゴリズムを指定します。 <ul style="list-style-type: none"> • [SHA1]: フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム • [MD5]: フェーズ 1 IKE ネゴシエーションで使用されるハッシュ アルゴリズム |
| [ESP アルゴリズム (ESP Algorithm)] | ドロップダウン リストから、ESP アルゴリズムを選択します。選択肢は次のとおりです。 <ul style="list-style-type: none"> • [NULL_ENC] • [DES] • [3DES] • [BLOWFISH] • [RIJNDAEL] |
| [フェーズ 1 のライフタイム (Phase One Life Time)] | フェーズ 1 IKE ネゴシエーションのライフタイムを秒単位で指定します。 |
| [フェーズ 1 の DH (Phase One DH)] | ドロップダウン リストから、フェーズ 1 の DH 値を選択します。選択肢は [2]、[1]、[5]、[14]、[16]、[17]、および [18] です。 |
| [フェーズ 2 のライフタイム (Phase Two Life Time)] | フェーズ 2 IKE ネゴシエーションのライフタイムを秒単位で指定します。 |
| [フェーズ 2 の DH (Phase Two DH)] | ドロップダウン リストから、フェーズ 2 の DH 値を選択します。選択肢は [2]、[1]、[5]、[14]、[16]、[17]、および [18] です。 |
| [ポリシーの有効化 (Enable Policy)] | このチェックボックスをオンにすると、ポリシーが有効になります。 |

既存の IPsec ポリシーの管理

既存の IPsec ポリシーを表示、有効化、無効化、または削除するには、次の手順を実行します。



(注)

システムのアップグレード中に IPsec ポリシーに対して行った変更は、すべて失われます。そのため、アップグレード中に IPsec ポリシーを修正したり作成したりしないでください。



注意

IPsec は、特に暗号化に関して、システムのパフォーマンスに影響を及ぼします。



注意

既存の IPsec ポリシーに対する変更は、通常の実システム動作に影響する場合があります。

手順

ステップ 1 [セキュリティ (Security)] > [IPSEC 設定 (IPSEC Configuration)] に移動します。



(注)

[セキュリティ (Security)] メニューの項目にアクセスするには、管理者パスワードを使用して Cisco Unified Communications オペレーティング システムの管理に再度ログインする必要があります。

[IPSEC ポリシーの一覧 (IPSEC Policy List)] ウィンドウが表示されます。

ステップ 2 ポリシーを表示、有効化、または無効化するには、次の手順を実行します。

- a. ポリシー名をクリックします。

[IPSEC ポリシーの設定 (IPSEC Policy Configuration)] ウィンドウが表示されます。

- b. ポリシーを有効または無効にするには、[ポリシーの有効化 (Enable Policy)] チェックボックスを使用します。
- c. [保存 (Save)] をクリックします。

ステップ 3 1 つまたは複数のポリシーを削除するには、次の手順を実行します。

- a. 削除するポリシーの隣にあるチェックボックスをオンにします。

[すべてを選択 (Select All)] をクリックしてすべてのポリシーを選択したり、[すべてをクリア (Clear All)] をクリックしてすべてのチェックボックスをオフにしたりすることができます。

- b. [選択項目の削除 (Delete Selected)] をクリックします。