Cisco Emergency Responder の Cisco Unified Operating System の設定

この章の各トピックでは、Cisco Emergency Responder（Emergency Responder）に付属の Cisco Unified Communications Operating System を設定および使用する方法について説明します。

- Cisco Unified Communications Operating System Administration へのアクセス，1 ページ
- 管理者パスワードとセキュリティ パスワードのリセット，2 ページ
- Cisco Unified OS 情報の表示，4 ページ
- Cisco Unified OS 設定の表示と変更，6 ページ
- ソフトウェア バージョンの管理，9 ページ
- Emergency Responder サーバの IP アドレスの変更，10 ページ
- セキュリティ管理，12 ページ
- IPSEC 管理，20 ページ
- ソフトウェア アップグレード，22 ページ
- カスタマイズされたログイン メッセージのアップロード，31 ページ
- Cisco Unified OS のサービス，31 ページ

Cisco Unified Communications Operating System Administration へのアクセス

Cisco Unified Communications Operating System Administration にアクセスしてログインするには、次の手順を実行します。

（注） Cisco Unified Communications Operating System Administration を使用する場合、ブラウザのコントロール（[Back] ボタンなど）は使用しないでください。

手順

ステップ 1 Emergency Responder にログインします。

ステップ 2 [Emergency Responder Administration] ページの右上にある [Navigation] メニューで [Cisco Unified OS Administration] を選択し、[Go] をクリックします。
Cisco Unified Communications Operating System Administration の [Logon] ウィンドウが表示されます。

（注） Cisco Unified Communications Operating System Administration には、**http:**//server-name/**cmplatform** で直接アクセスすることもできます。

ステップ 3 管理者ユーザ名とパスワードを入力します。

（注） 管理者ユーザ名とパスワードは、インストール時に決めるか、CLI を使用して作成します。

ステップ 4 [Submit] をクリックします。
[Cisco Unified Communications Operating System Administration] ウィンドウが表示されます。

管理者パスワードとセキュリティパスワードのリセット

管理者パスワードやセキュリティ パスワードがわからなくなった場合、次の手順に従ってパスワードをリセットします。

パスワードをリセットするには、システム コンソール経由でシステムに接続している必要があります。つまり、キーボードとモニタをサーバに接続している必要があります。 システムにセキュア シェル接続している状態ではパスワードをリセットできません。

注意 サーバ グループのすべてのサーバのセキュリティ パスワードが一致する必要があります。 すべてのマシンのセキュリティ パスワードを変更してください。変更しないと、互いに通信できなくなります。

注意 セキュリティ パスワードを変更した後に、サーバ グループ内の各サーバをリセットする必要があります。 サーバをリブートしない場合、システム サービスで問題が発生するほか、サブスクライバ サーバ上の [Emergency Responder Administration] ページで問題が発生します。

（注） この手順中、物理的にシステムにアクセスできるか確認するため、有効な CD または DVD をディスク ドライブから取り出し、再挿入する必要があります。

手順

ステップ 1 次のユーザ名とパスワードを使用してシステムにログインします。

- ユーザ名：**pwrecovery**
- パスワード：**pwreset**

[Welcome to platform password reset] ウィンドウが表示されます。

ステップ 2 任意のキーを押して続行します。

ステップ 3 ディスク ドライブに CD または DVD が入っている場合は、ここで取り出します。

ステップ 4 任意のキーを押して続行します。
CD または DVD がディスク ドライブから取り出してあるかが確認されます。

ステップ 5 有効な CD または DVD をディスク ドライブに挿入します。
（注） このテストでは、音楽 CD ではなくデータ CD を使用する必要があります。
ディスクを挿入したかが確認されます。

ステップ 6 ディスクが挿入されていることをシステムが確認した後、次のいずれかのオプションを入力して続行するよう要求されます。

- **a** を入力して、管理者パスワードをリセットする。
- **s** を入力して、セキュリティ パスワードをリセットする。
- **q** を入力して、終了する。

ステップ 7 選択したタイプの新しいパスワードを入力します。

ステップ 8 新しいパスワードを再入力します。
パスワードには 6 文字以上が必要です。 システムが新しいパスワードの有効性を確認します。 パスワードが有効性テストに合格しない場合、新しいパスワードを入力するよう要求されます。

ステップ 9 新しいパスワードの強度が検証された後、パスワードがリセットされ、任意のキーを押してパスワード リセット ユーティリティを終了するよう指示されます。

Cisco Unified OS 情報の表示

[Cisco Unified OS Administration] Web ページを使用すると、オペレーティング システム、プラットフォームハードウェア、およびネットワークのステータスを表示できます。 次の各項では、この情報の表示方法について説明します。

ServerGroup 情報の表示

クラスタ情報を表示するには、次の手順を実行します。

手順

ステップ 1 メインの [Cisco Unified OS Administration] Web ページから、[Show] > [ServerGroup] を選択します。 [ServerGroup] ページが表示されます。

ステップ 2 [ServerGroup] ページのフィールドの説明については、表 1を参照してください。

ハードウェア ステータスの表示

ハードウェア ステータスを表示するには、次の手順を実行します。

手順

ステップ 1 メインの [Cisco Unified OS Administration] Web ページから、[Show] > [Hardware] を選択します。 [Hardware Status] ページが表示されます。

ステップ 2 [Hardware Status] ページの各フィールドについては、表 1を参照してください。

ネットワーク ステータスの表示

表示されるネットワーク ステータス情報は、ネットワークの耐障害性がイネーブルになっているかどうかによって異なります。 ネットワーク耐障害性が有効になっていると、イーサネット ポート 0 に障害が発生した場合、イーサネット ポート 1 が自動的にネットワーク通信を継承します。 ネットワークの耐障害性がイネーブルになっている場合、ネットワーク ポートのイーサネット 0、イーサネット 1、および Bond 0 のネットワーク ステータス情報が表示されます。 ネットワーク耐障害性が有効になっていない場合、イーサネット 0 のステータス情報のみが表示されます。

ネットワーク ステータスを表示するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Show] > [Network] を選択します。
[Network Settings] ページが表示されます。

ステップ 2 [Network Settings] ページの各フィールドについては、表 1を参照してください。

インストールされているソフトウェアの表示

ソフトウェアバージョンとインストールされているソフトウェアオプションを表示するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Show] > [Software] を選択します。
[Software Packages] ページが表示されます。

ステップ 2 [Software Packages] ページのフィールドの説明については、表 1を参照してください。

システム ステータスの表示

システム ステータスを表示するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Show] > [System] を選択します。
[System Status] ページが表示されます。

ステップ 2 [System Status] ページの各フィールドについては、表 1を参照してください。

IP 設定の表示

IP 設定を表示するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Show] > [IP Preference] を選択します。
[IP Preferences] ページが表示されます。

ステップ 2 データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、ステップ 3, （6 ページ） に進みます。
レコードをフィルタまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索テキストを指定します。

（注） 検索条件をさらに追加するには、[+] ボタンをクリックします。 条件を追加した場合、指定した条件をすべて満たしているレコードが検索されます。 条件を削除する場合、最後に追加した条件を削除するには、[-] ボタンをクリックします。追加した検索条件をすべて削除するには、[Clear Filter] ボタンをクリックします。

ステップ 3 [Find] をクリックします。
条件を満たしているレコードがすべて表示されます。 1 ページあたりの項目の表示件数を変更するには、[Rows per Page] ドロップダウン リスト ボックスで別の値を選択します。

Cisco Unified OS 設定の表示と変更

IP 設定、ホスト設定、ネットワーク タイム プロトコル（NTP）設定を表示および変更するには、設定オプションを使用します。 次の各項では、Cisco Unified OS 設定を表示および変更する方法について説明します。

イーサネット設定のセットアップ

イーサネット設定オプションを使用して、Dynamic Host Configuration Protocol（DHCP）、ポート、およびゲートウェイの情報を表示および変更できます。

[Ethernet Configuration] ページでは、DHCP を有効または無効にしたり、イーサネット ポートの IP アドレスとサブネット マスクを指定したり、ネットワーク ゲートウェイの IP アドレスを指定したりできます。

（注） イーサネット設定はすべて Eth0 にのみ適用されます。 Eth1 を対象とした設定はできません。 Eth0 の最大伝送単位（MTU）のデフォルトは 1500 です。

イーサネット設定を表示または変更するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Settings] > [IP] > [Ethernet] を選択します。 [Ethernet Configuration] ページが表示されます。

ステップ 2 イーサネット設定を変更するには、目的のフィールドに新しい値を入力します。 [Ethernet Configuration] ウィンドウのフィールドの説明については、表 1を参照してください。

（注） DHCP を有効にすると、ポート情報とゲートウェイ情報の設定が無効になり、変更できなくなります。

ステップ 3 変更を保存するには、[Save] をクリックします。

NTP サーバのセットアップ

外部 NTP サーバが Stratum 9 以上（1 ～ 9）であることを確認してください。 外部 NTP サーバの追加、削除、または変更を行うには、次の手順を実行します。

（注） パブリッシャ上では NTP サーバ設定しか構成することができません。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Settings] > [NTP Servers] を選択します。 [NTP Server List] ページが表示されます。 [NTP Server List] ページの詳細は、NTP Server Listを参照してください。

ステップ 2 NTP サーバの追加、削除、または変更ができます。

- NTP サーバを削除するには、当該のサーバの前にあるチェックボックスをオンにしてから [Delete Selected] をクリックします。
- NTP サーバを追加するには、[Add] をクリックします。 [NTP Server Configuration] ページが表示されます。 ホスト名または IP アドレスを入力してから [Save] をクリックします。
- NTP サーバを変更するには、IP アドレスをクリックします。 [NTP Server Configuration] ページが表示されます。 ホスト名または IP アドレスを変更してから [Save] をクリックします。

（注） NTP サーバに対する変更は、完了するまで最大で 5 分かかる場合があります。 NTP サーバを変更する場合、ページを更新して正しいステータスを表示する必要があります。

ステップ 3 [NTP Server Settings] ページを更新して正しいステータスを表示するには、[Settings] > [NTP Servers] の順に選択します。

（注） NTP サーバの削除、変更、または追加が完了した後、変更を反映するには、すべてのパブリッシャとサブスクライバを再起動する必要があります。

SMTP 設定のセットアップ

[SMTP Settings] ウィンドウでは、SMTP ホスト名の表示や設定ができ、SMTP ホストがアクティブであるかどうかが表示されます。

SMTP ホスト設定を設定するには、次の手順を実行します。

ヒント システムから電子メールを送信する場合は、SMTP ホストを設定する必要があります。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Settings] > [SMTP] を選択します。
[SMTP Settings] ページが表示されます。 [SMTP Settings] ページの詳細については、SMTP Settings を参照してください。

ステップ 2 SMTP ホストのホスト名または IP アドレスを入力します。

ステップ 3 [Save] をクリックします。

時刻設定のセットアップ

時刻を手動で設定するには、次の手順を実行します。

（注） サーバ時刻を手動で設定するには、設定済みの NTP サーバをすべて削除する必要があります。NTP サーバの削除の詳細については、NTP サーバのセットアップ, （7 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Settings] > [Time] を選択します。 [Time Settings] ページが表示されます。 [Time Settings] ページの詳細については、Time Settingsを参照してください。

ステップ 2 システムの日付と時刻を入力します。

ステップ 3 [Save] をクリックします。

ソフトウェア バージョンの管理

このオプションは、新しいソフトウェアにアップグレードする場合と、以前のソフトウェアのバージョンにフォールバックする場合の両方で使用します。

Emergency Responder ソフトウェア バージョンを再起動、シャットダウン、または切り替えるには、次の手順を実行します。

注意 この手順を実行すると、システムが再起動し、一時的に使用できない状態になります。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Settings] > [Version] を選択します。 [Version Settings] ページが表示されます。 [Version Settings] ページの詳細については、Version Settingsを参照してください。

ステップ 2 アクティブなパーティションで実行しているバージョンを再起動するには、[Restart] をクリックします。
[Restart] をクリックすると、現在のパーティションのシステムが、バージョンを切り替えずに再起動します。

ステップ 3 システムをシャットダウンするには、[Shutdown] をクリックします。
[Shutdown] をクリックすると、すべてのプロセスが中断され、システムがシャット ダウンします。

（注） ハードウェアの電源は自動的には切れません。

注意 サーバの電源ボタンを押すと、システムがただちにシャットダウンされます。

ステップ 4 アクティブディスク パーティションで実行中のシステムをシャットダウンし、その後非アクティブ パーティションのソフトウェア バージョンを使用してシステムを自動的に再起動するには、[Switch Versions] をクリックします。

[Switch Versions] をクリックするとシステムが再起動し、現在非アクティブであるパーティションがアクティブになります。

（注） [Switch Version] ボタンは、非アクティブのパーティションにソフトウェアがインストールされている場合にのみ表示されます。

（注） このオプションは、新しいソフトウェアにアップグレードする場合、または以前のソフトウェアのバージョンにフォールバックする場合に使用します。

Emergency Responder サーバの IP アドレスの変更

Emergency Responder パブリッシャまたは Emergency Responder サブスクライバのいずれか、あるいは両方の IP アドレスを変更できます。

次の各項では、Emergency Responder サーバの IP アドレスを変更する方法について説明します。

Emergency Responder パブリッシャまたはスタンドアロン サーバの IP アドレスの変更

インストール後に Emergency Responder パブリッシャまたはスタンドアロン サーバの IP アドレスを変更するには、次の手順を実行します。

（注） サーバで IP アドレスの変更を開始する前に、DNS サーバの IP アドレス情報を更新します。

手順

ステップ 1 次のオプションのいずれかを使用して、Emergency Responder パブリッシャの IP アドレスを変更します。

- Cisco Unified Operating System Administration で、[Settings] > [IP] > [Ethernet] に新しい IP アドレスを入力します。 Ethernet Configurationを参照してください。

- CLI で、**set network ip** コマンドを使用して新しい IP アドレスを設定します。 set network ipを参照してください。

ステップ 2 Emergency Responder パブリッシャまたはスタンドアロンサーバをリブートし、サーバが完全に動作可能になるまで待機します。 スタンドアロンサーバの場合は、サーバが動作可能になったらステップ 7 に進みます。

ステップ 3 Emergency Responder パブリッシャが完全に動作可能になったら、Emergency Responder サブスクライバ上で [Cisco Unified Operating System Administration] にログインします。

ステップ 4 [Settings] > [IP] > [Publisher] を選択します。 [Cisco Unified Operating System Administration] に Publisher の古い IP アドレスが表示されます。 パブリッシャの新しい IP アドレスを [Edit] ボックスに入力し、[Save] をクリックします。

ステップ 5 すぐに Emergency Responder サブスクライバをリブートし、Emergency Responder パブリッシャが Emergency Responder サブスクライバとの通信を維持できるようにします。

ステップ 6 utils dbreplication statusの説明に従って **utils dbreplication status** CLI コマンドを使用して、レプリケーションを確認します。 各サーバの値が 2 と等しくなるようにしてください。

ステップ 7 CTI ポートが Emergency Responder パブリッシャ サーバに登録されていることを確認します。 CTI ポートが登録されていない場合は、CTI ポートを削除してから再び追加して、CTI ポートを再作成する必要があります。 必要な CTI ポートの作成を参照してください。

Emergency Responder サブスクライバの IP アドレスの変更

インストール後に Emergency Responder サブスクライバの IP アドレスを変更するには、次の手順を実行します。

（注） サーバで IP アドレスの変更を開始する前に、DNS サーバの IP アドレス情報を更新します。

手順

ステップ 1 次のオプションのいずれかを使用して、Emergency Responder サブスクライバの IP アドレスを変更します。

- Cisco Unified Operating System Administration で、[Settings] > [IP] > [Ethernet] に新しい IP アドレスを入力します。 Ethernet Configurationを参照してください。

- CLI で、**set network ip** コマンドを使用して新しい IP アドレスを設定します。 set network ipを参照してください。

ステップ 2 Emergency Responder サブスクライバをリブートします。

ステップ 3 Emergency Responder サブスクライバが完全に動作可能になったら、Emergency Responder パブリッシャをリブートします。

ステップ 4 utils dbreplication statusの説明に従って **utils dbreplication status** CLI コマンドを使用して、レプリケーションを確認します。 各サーバの値が 2 と等しくなるようにしてください。

Emergency Responder パブリッシャとサブスクライバ両方の IP アドレスの変更

パブリッシャとサブスクライバ両方の IP アドレスを変更する場合は、サブスクライバから順にサーバの IP アドレスを変更する必要があります。

注意 サブスクライバの IP アドレスの変更が完了するまでは、パブリッシャ サーバの IP アドレスの変更を開始しないでください。

Emergency Responder パブリッシャと Emergency Responder サブスクライバの IP アドレスを変更するには、次の手順を実行します。

手順

ステップ 1 Emergency Responder サブスクライバ サーバの IP アドレスの変更については、Emergency Responder サブスクライバの IP アドレスの変更, （11 ページ）を参照してください。

ステップ 2 Emergency Responder パブリッシャ サーバの IP アドレスの変更については、Emergency Responder パブリッシャまたはスタンドアロン サーバの IP アドレスの変更, （10 ページ）を参照してください。

セキュリティ管理

次の各項では、セキュリティおよび IPSec の管理タスクの実行方法について説明します。

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できるように Internet Explorer のセキュリティ設定が正しく設定されていることを確認するには、次の手順を実行します。

手順

ステップ 1 Internet Explorer を起動します。
ステップ 2 [Tools] > [Internet Options] を選択します。
ステップ 3 [Advanced] タブをクリックします。
ステップ 4 [Advanced] タブの [Security] セクションまでスクロールします。
ステップ 5 必要に応じて、[Do not save encrypted pages to disk] 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。

Certificate Management

次の各項では、[Certificate Management] メニューのオプションを使用して実行できる機能について説明します。

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 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。
[Certificate List] ページが表示されます。 [Certificate List] ページの詳細については、Certificate List を参照してください。
ステップ 2 証明書のリストをフィルタするには、[Find] コントロールを使用します。
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。
[Certificate Configuration] ページに該当の証明書の情報が表示されます。
ステップ 4 [Certificate List] ページに戻るには、[Related Links] リストの [Back To Find/List] を選択し、[Go] をクリックします。

証明書または CTL のダウンロード

証明書または CTL を Emergency Responder からローカル システムに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 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。
[Certificate List] ページが表示されます。 証明書または CTL のファイル名をクリックします。

ステップ 2 証明書のリストをフィルタするには、[Find] コントロールを使用します。

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。
[Certificate Configuration] ページが表示されます。

ステップ 4 [Download] をクリックします。

ステップ 5 [File Download] ダイアログボックスで、[Save] をクリックします。

証明書の削除および再作成

次の各項では、証明書の削除と再作成について説明します。

証明書の削除

信頼できる証明書を削除するには、次の手順を実行します。

注意 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。 [Certificate List] で選択する証明書については、システムから既存の CSR がすべて削除されます。新しい CSR を生成する必要があります。 詳細については、Generate Certificate Signing Request, （18 ページ）を参照してください。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。
[Certificate List] ページが表示されます。

ステップ 2 証明書のリストをフィルタするには、[Find] コントロールを使用します。

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。
[Certificate Configuration] ページが表示されます。

ステップ 4 [Delete] をクリックします。

証明書の再作成

証明書を再作成するには、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 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。
[Certificate List] ページが表示されます。

ステップ 2 [Generate New] をクリックします。
[Generate Certificate] ダイアログボックスが表示されます。

ステップ 3 [Certificate Name] リストから、証明書の名前を選択します。 表示される証明書の名前の説明については、表 1：証明書の名前と説明, （15 ページ）を参照してください。

ステップ 4 [Generate New] をクリックします。

表 *1*：証明書の名前と説明

名前	説明
tomcat	この自己署名ルート証明書は、HTTPS サーバのインストール中に作成されます。
ipsec	この自己署名ルート証明書は、MGCP ゲートウェイおよび H.323 ゲートウェイとの IPSec 接続のインストール中に生成されます。

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証明書信頼リスト（CTL）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。 新しい tomcat 証明書または証明書信頼リストをアップロードした後、CLI コマンドの **utils service restart Cisco Tomcat** を入力して、Cisco Tomcat サービスを再起動する必要があります。

（注） システムが信頼証明書を他のクラスタ サーバに自動的に配信することはありません。 複数のサーバで同じ証明書が必要な場合は、証明書を各サーバに個々にアップロードする必要があります。

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。

Upload Certificate

CA ルート証明書、アプリケーション証明書、CTL ファイルをサーバにアップロードするには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。
[Certificate List] ページが表示されます。

ステップ 2 [Upload Certificate] をクリックします。
[Upload Certificate] ダイアログボックスが表示されます。

ステップ 3 [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 で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、CA ルート証明書の名前を [Root Certificate] テキスト ボックスに入力します。 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ます。

ステップ 5 次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキスト ボックスに、ファイルのパスを入力します。
- [Browse] ボタンをクリックしてファイルを選択し、[Open] 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、[Upload File] ボタンをクリックします。

信頼できる証明書のアップロード

信頼できる証明書をアップロードするには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。
[Certificate List] ページが表示されます。

ステップ 2 [Upload CTL] をクリックします。
[Upload Certificate Trust List] ダイアログボックスが表示されます。

ステップ 3 [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 で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、CA ルート証明書の名前を [Root Certificate] テキスト ボックスに入力します。 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ます。

ステップ 5 次のいずれかの手順で、アップロードするファイルを選択します。

- [Upload File] テキスト ボックスに、ファイルのパスを入力します。
- [Browse] ボタンをクリックしてファイルを選択し、[Open] 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、[Upload File] ボタンをクリックします。

サード パーティ製の CA 証明書の使用

Cisco Unified OS は、サードパーティ製の Certificate Authority（CA; 認証局）が PKCS # 10 Certificate Signing Request（CSR; 証明書署名要求）によって発行した証明書をサポートしています。 次の手順では、このプロセスの概要および参考となる文書を示します。

手順

ステップ 1 サーバに CSR を作成する。

ステップ 2 CSR を PC にダウンロードする。

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。

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。

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。

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。

ステップ 7 新しい証明書の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 の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 Unified CM の証明書を更新した場合は、TFTP サービスも再起動します。

関連トピック

Generate Certificate Signing Request, （18 ページ）
証明書または CTL のダウンロード, （14 ページ）
サードパーティ製の CA 証明書, （19 ページ）
証明書または証明書信頼リストのアップロード, （16 ページ）
コントロール センターの使用

Generate Certificate Signing Request

証明書署名要求（CSR）を作成するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。
[Certificate List] ページが表示されます。

ステップ 2 [Generate CSR] をクリックします。
[Generate Certificate Signing Request] ダイアログボックスが表示されます。

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

ステップ 4 [Generate CSR] をクリックします。

Download Certificate Signing Request

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Management] を選択します。

[Certificate List] ページが表示されます。

ステップ 2 [Download CSR] をクリックします。
[Download Certificate Signing Request] ダイアログボックスが表示されます。

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

ステップ 4 [Download CSR] をクリックします。

ステップ 5 [File Download] ダイアログボックスで、[Save] をクリックします。

サードパーティ製の CA 証明書

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、署名付きのアプリケーション証明書と CA ルート証明書の両方を CA から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。 入手の手順は、CA によって異なります。

CAPF および Emergency Responder 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 が拡張要求メカニズムをサポートしていない場合は、CSR 作成プロセスの最後のページに表示される X.509 拡張を有効にする必要があります。

Cisco Unified OS では、証明書は DER および PEM エンコーディング フォーマットで、CSR は PEM エンコーディング フォーマットで生成されます。 また、DER および DER 符号化フォーマットの証明書を受け入れます。

証明書有効期限モニタのセットアップ

証明書の有効期限日が近づいたときに、システムから自動的に電子メールを送信できます。

証明書有効期限モニタの表示と設定をするには、次の手順を実行します。

（注） [Certificate Expiration Monitor] ページに関する情報を更新するには、Cisco Certificate Expiry Monitor サービスが実行されている必要があります。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [Certificate Monitor] を選択します。
[Certificate Monitor] ページが表示されます。

ステップ 2 必要な設定情報を入力します。 [Certificate Monitor Expiration] フィールドの説明については、表 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、[Save] をクリックします。

IPSEC 管理

次のトピックでは、IPSec を管理する方法について説明します。

（注） IPSec は、インストール中にサーバ グループ内のサーバ間で自動的にセットアップされません。

既存の IPSec ポリシーの表示または変更

既存の IPSec ポリシーを表示または変更するには、次の手順を実行します。

（注） システムのアップグレード中、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意 IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [IPSEC Configuration] を選択します。[IPSEC Policy Configuration] ページが表示されます。

注意 既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

ステップ 2 [Display Detail] リンクをクリックします。 [Association Details] ページが表示されます。 このページのフィールドの説明については、表 2を参照してください。

IPSec ポリシーのセットアップ

新しい IPSec ポリシーと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、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意 IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Security] > [IPSEC Configuration] を選択します。
[IPSEC Policy List] ページが表示されます。

ステップ 2 [Add New] をクリックします。
[IPSEC Policy Configuration] ページが表示されます。

ステップ 3 [Next] をクリックします。
[Setup IPSEC Policy and Association] ページが表示されます。

ステップ 4 [IPSEC Policy Configuration] ページに関する適切な情報を入力します。 このページにあるフィールドの説明については、表 2を参照してください。

ステップ 5 新しい IPSec ポリシーを設定するには、[Save] をクリックします。

既存の IPSec ポリシーの管理

既存の IPSec ポリシーを表示、イネーブル/ディセーブル、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、IPSec ポリシーに何らかの変更を行ってもその変更は無効になります。アップグレード中は IPSec ポリシーを変更または作成しないでください。

注意 IPSec はシステムのパフォーマンスに影響します（特に暗号化した場合）。

注意 既存の IPSec ポリシーを変更すると、システムの正常な動作に影響する場合があります。

手順

ステップ 1 [Security] > [IPSEC Configuration] を選択します。
（注） [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 Operating System Administration に再ログインする必要があります。
[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、イネーブル、またはディセーブルにするには、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 Policy Configuration] ウィンドウが表示されます。

b) ポリシーをイネーブルまたはディセーブルにするには、[Enable Policy] チェックボックスをオンまたはオフにします。

c) [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横にあるチェックボックスをオンにします。
[Select All] をオンにしてすべてのポリシーを選択することも、[Clear All] をオンにしてすべてのチェックボックスをオフにすることもできます。

b) [Delete Selected] をクリックします。

ソフトウェア アップグレード

次の各項では、ソフトウェアのアップグレードを実行する方法について説明します。

ソフトウェア アップグレード手順の概要

[Software Upgrade] ページでは、DVD（ローカル ソース）または Emergency Responder がアクセス可能なネットワーク上の場所（リモート ソース）から Emergency Responder ソフトウェアをアップグレードできます。 Emergency Responder パブリッシャを最初にアップグレードして、次にサブスクライバをアップグレードします。

このバージョンの Emergency Responder では、システムの運用中にサーバにアップグレード ソフトウェアをインストールすることができません。 Emergency Responder 8.6 以前のすべてのバージョンから最新のバージョンの Emergency Responder にアップグレードするには、リフレッシュ アップグレードが必要です。 リフレッシュ アップグレードとは、非アクティブ パーティションへの新規インストールを指しており、内蔵データの移行作業が含まれます。 リフレッシュ アップグレードでは、サーバのダウンタイムが必要となります。 これは、Emergency Responder パブリッシャとサブスクライバを備えた冗長システムでは、大きな影響を与えません。

アップグレードを開始する前に、システムをバックアップします。

MCS 7825-H3 サーバ上でアップグレードを実行するには、16 GB USB キーを使用して古いシステムのデータを新しいインストール環境に移行する必要があります。

アップグレード ソフトウェアをインストールする場合、Emergency Responder ソフトウェアのインストール中にサーバが一時的に停止します。 アップグレードの開始後に、コマンドラインまたはグラフィカルユーザインターフェイスを使用してデータが移行され、システムが自動的に再起動します。この時点でサーバが停止します。停止の期間は、構成やデータ量により異なります。リフレッシュ アップグレードの開始時と終了時には、通知電子メールが送信されます。

アップグレード プロセスの進行中に、管理者がデータのエクスポートなどの変更を行った場合、そのデータはアップグレード後に失われます。

MCS 7825-H3 サーバのアップグレードの場合の例外として、以前のソフトウェアが次回のアップグレードまで非アクティブ パーティション上に保持されます。

手動のスイッチバックにより、古いバージョンに戻すことができます。 アップグレードに失敗した場合、システムは自動的に以前のバージョンに戻ります。 設定情報は自動的にアクティブ パーティションにあるアップグレード バージョンに移行されます。

何らかの理由でアップグレードから元の状態に戻す場合は、switch-version オプションを使用して、ソフトウェアの以前のバージョンがある非アクティブ パーティションからシステムを再起動できます。

ただし、非アクティブ パーティション上のデータベースは更新されないため、ソフトウェアのアップグレード後に行ったすべての設定変更は失われます。 アップグレード後にデータベースに変更を加えた場合は、元のパーティションに戻してから同じ変更を繰り返す必要があります。

警告 MCS 7825-H3 サーバ上でソフトウェアのアップグレードを行う場合、以前のバージョンの Emergency Responder に戻すオプションはありません。

サポートされるアップグレード

Emergency Responder の最新バージョンへの直接アップグレードは、リリース 7.1、8.0、8.5、および 8.6 のみでサポートされています。 このアップグレードを開始する前に、リフレッシュ アップグレードをサポートするために cop ファイルにパッチを適用する必要があります。

リリース 1.3、2.0、および 7.0 の場合、最新バージョンへのアップグレードは 2 段階の処理になります。

Emergency Responder 1.3 からアップグレードするには、最初に Emergency Responder 7.1 にアップグレードしてから、最新バージョンにアップグレードする必要があります。

Emergency Responder 2.0 または 7.0 からアップグレードするには、最初に Emergency Responder 7.1 または Emergency Responder 8.0 にアップグレードしてから、最新バージョンにアップグレードする必要があります。

Cisco Unified Operating System のアップグレード

（注） アップグレード作業の項の項目を終了してから設定作業を実行します。 アップグレード中に Cisco Emergency Responder の設定を変更しないでください。 設定の変更には、[Emergency Responder Administration] または [Emergency Responder Serviceability] ページでの変更も含まれます。 アップグレード時の設定の変更はアップグレード完了後に失われる可能性があり、一部の設定によりアップグレードが失敗する可能性があります。

警告 Emergency Responder のパブリッシャおよびサブスクライバの両方でアップグレードが完了し、サーバをアップグレードされたパーティションに切り替えて、データベース レプリケーションが機能していることを確認するまでは設定作業を実行しないでください。

手順

ステップ 1 すべての設定作業を停止します。これには、Cisco Emergency Responder に関連する各種の GUI または CLI でのすべての設定作業が含まれます。

ステップ 2 必要な COP ファイルを適用します。

ステップ 3 Emergency Responder パブリッシャをアップグレードします。

（注） アップグレードされたシステムは、アップグレードされたパーティションに自動的にリブートしません。 代わりに、2 つのオプション [Reboot to new partition] および [Do not reboot to new partition] が表示されます。 [Do not reboot to new partition] はデフォルトのオプションであり、ベスト プラクティスであると見なされています。 ただし、新規パーティションへのリブートを選択した場合は、ステップ 5 および 6 が不要となります。

ステップ 4 Emergency Responder サブスクライバをアップグレードします。

ステップ 5 Emergency Responder パブリッシャを、アップグレードされたパーティションに切り替えます。

ステップ 6 Emergency Responder サブスクライバを、アップグレードされたパーティションに切り替えます。

ステップ 7 Emergency Responder パブリッシャと Emergency Responder サブスクライバ間でデータベース レプリケーションが機能していることを確認してください。

ステップ 8 その他すべてのアップグレード作業が完了したら、必要に応じて設定作業を実行できます。

アップグレード ファイル

アップグレード プロセスを開始する前に、Cisco Emergency Responder ソフトウェアを注文して、適切なアップグレード ファイルを取得する必要があります。 COP ファイルも Cisco.com からダウンロードする必要があります。

（注） インストールする前に、パッチ ファイルの名前を変更しないでください。システムで有効なファイルとして認識されなくなります。

（注） アップグレード ファイルを解凍または untar しないでください。 これを行うと、システムはアップグレード ファイルを読み取れなくなります。

インストール プロセス中も、アップグレード ファイルにはローカル DVD またはリモートの FTP または SFTP サーバからアクセスできます。 アップグレード ファイルにアクセスする際に入力するディレクトリ名とファイル名は、大文字と小文字が区別されるため、注意してください。

DVD からのソフトウェアのインストールまたはアップグレード

ローカル ディスク ドライブに挿入された DVD からソフトウェアをインストールしてから、アップグレード プロセスを開始できます。

（注） ソフトウェアのアップグレード プロセスを開始する前にシステム データをバックアップしてください。 詳細については、Cisco Emergency Responder Disaster Recovery System の設定の章を参照してください。

ソフトウェアを DVD からインストールまたはアップグレードするには、次の手順を実行します。

手順

ステップ 1 MCS 7825-H3 サーバ上のソフトウェアをアップグレードする場合、16 GB USB キーを挿入して、データを古いシステムから新しいインストールに移行します。

（注） MCS 7825-H3 サーバ上のソフトウェアをアップグレードする場合、Cisco Emergency Responder の前のバージョンに戻すオプションはありません。 これらのマシンのいずれかでアップグレードを実行するには、16 GB USB キーを使用して、データを古いシステムから新しいインストールに移行する必要があります。

ステップ 2 適切なアップグレード ファイルを注文します。 物理的な DVD を受け取るか、電子ソフトウェア配信経由でディスク イメージ ファイルをダウンロードするかを選択できます。

（注） ディスク イメージ ファイルをダウンロードする場合は、DVD を焼くための .iso ファイルを使用して DVD を作成します。 .iso ファイルには、元の DVD ディスクの完全なイメージが含まれます。 .iso ファイルを DVD にコピーしないでください。 DVD 作成ソフトウェアを使用して、イメージに含まれているファイルを抽出し、これらを DVD に書き込む必要があります。 これにより、DVD ディスクの正確な複製が作成されます。

ステップ 3 DVD をアップグレードするローカル サーバのディスク ドライブに挿入します。

ステップ 4 [Cisco Unified OS Administration] Web ページから、[Software Upgrades] > [Install/Upgrade] を選択します。
[Software Installation/Upgrade] ページが表示されます。

ステップ 5 [Source] リストから [DVD/CD] を選択します。

ステップ 6 [Directory] フィールドに、DVD のパッチ ファイルのパスを入力します。
ファイルがルート ディレクトリにある場合は、スラッシュ（/）を入力します。

ステップ 7 [Next] をクリックしてアップグレード プロセスを続行します。

ステップ 8 インストールするアップグレード バージョンを選択して、[Next] をクリックします。

ステップ 9 次のページで、ファイル名と転送されている MB 数を含むダウンロードの進行状況をモニタします。

ステップ 10 アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動するには、[Switch to new version after upgrade] を選択します。 システムが再起動され、アップグレードされたソフトウェアが起動されます。

ネットワーク ドライブまたはリモート サーバからのソフトウェアのインストール

ソフトウェアをネットワーク ドライブまたはリモート サーバからインストールするには、次の手順を実行します。

（注） ソフトウェアのアップグレード プロセスを開始する前にシステム データをバックアップしてください。 詳細については、Cisco Emergency Responder Disaster Recovery System の設定の章を参照してください。

（注） Cisco Unified Operating System Administration にアクセスしている間は、ブラウザの制御機能（表示の更新や再読み込みなど）を使用しないでください。 代わりに、インターフェイスのナビゲーション コントロールを使用してください。

（注） MCS 7825-H3 サーバ上のソフトウェアをアップグレードする場合、Cisco Emergency Responder の前のバージョンに戻すオプションはありません。 これらのマシンのいずれかでアップグレードを実行するには、16 GB USB キーを使用して、データを古いシステムから新しいインストールに移行する必要があります。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Software Upgrades] > [Install/Upgrade] を選択します。
[Software Installation/Upgrade] ページが表示されます。

ステップ 2 [Source] リストから [Remote Filesystem] を選択します。

ステップ 3 [Directory] フィールドに、リモート システムのパッチファイルのパスを入力します。

アップグレード ファイルが Linux または UNIX サーバ上に存在する場合は、指定するディレクトリ パスの先頭にフォワード スラッシュを付加する必要があります。 たとえば、アップグレード ファイルが patches ディレクトリに存在する場合は、/patches と入力する必要があります。

アップグレード ファイルが Windows サーバ上にある場合は、FTP サーバまたは SFTP サーバに接続することになるため、次のような適切な構文を使用するよう注意してください。

- パスの先頭はフォワード スラッシュ（/）で始め、パス全体でフォワード スラッシュを使用します。
- パスは、サーバの FTP または SFTP ルート ディレクトリで始まる必要があります。C: などのドライブ レターで始まる Windows 絶対パスは入力できません。

ステップ 4 [Server] フィールドにサーバ名を入力します。

ステップ 5 [User Name] フィールドにユーザ名を入力します。

ステップ 6 [User Password] フィールドにパスワードを入力します。

ステップ 7 [Transfer Protocol] フィールドで、転送プロトコルを選択します。

ステップ 8 [Next] をクリックしてアップグレード プロセスを続行します。

ステップ 9 インストールするアップグレード バージョンを選択して、[Next] をクリックします。

ステップ 10 次のページで、ファイル名と転送されている MB 数を含むダウンロードの進行状況をモニタします。

ステップ 11 ダウンロードが完了したら、ダウンロードしたファイルのチェックサム値と、Cisco.com に表示されているチェックサム値を確認します。

注意 アップグレード ファイルが本物の整合性のあるファイルであると保証するには、2 つのチェックサム値が一致している必要があります。 チェックサム値が一致しない場合、Cisco.com から新しいバージョンのファイルをダウンロードして、再度アップグレードを試みてください。

（注） アップグレード プロセスの進行中にサーバとの接続を失った場合、またはブラウザを閉じた場合は、[Software Upgrades] メニューに再度アクセスしようとすると、次のメッセージが表示されることがあります。

Warning: Another session is installing software, click Assume Control to take over the installation.

セッションを引き継ぐ場合は、[Assume Control] を選択します。

[Assume Control] が表示されない場合は、Real Time Monitoring Tool でアップグレードをモニタすることもできます。

ステップ 12 アップグレードをインストールして、アップグレードされたパーティションに自動的に再起動するには、[Reboot to upgraded partition] を選択します。 システムが再起動され、アップグレードされたソフトウェアが起動されます。

ステップ 13 アップグレードをインストールして、後でアップグレードされたパーティションに手動で再起動する場合は、次の手順を実行します。

a) [Do not reboot after upgrade] を選択します。

b) [Next] をクリックします。
[Upgrade Status] ウィンドウにアップグレード ログが表示されます。

c) インストールが完了したら、[Finish] をクリックします。
d) システムを再起動して、アップグレードをアクティブにするには、[Settings] > [Version] を選択して、[Switch Version] をクリックします。
システムが再起動され、アップグレードされたソフトウェアが起動されます。

アップグレードの途中停止の管理

アップグレード ソフトウェアのインストール中に、アップグレードが途中停止したように見える場合があります。アップグレードログには新しいログ メッセージが表示されなくなります。アップグレードが途中停止した場合は、アップグレードをキャンセルし、I/O スロットリングを無効にして、アップグレード手順を初めからやり直す必要があります。 正常にアップグレードが完了した場合は、I/O スロットリングを有効にする必要はありません。

- I/O スロットリングを無効にするには、CLI コマンドの **utils iothrottle disable** を入力します。
- I/O スロットリングのステータスを表示するには、CLI コマンドの **utils iothrottle status** を入力します。
- I/O スロットリングを有効にするには、CLI コマンドの **utils iothrottle enable** を入力します。
デフォルトでは、iothrottle は有効になっています。
システムがキャンセルに応答しない場合は、サーバをリブートし、I/O スロットリングを無効にして、アップグレード プロセス手順を初めからやり直す必要があります。

以前のバージョンへの復帰

アップグレード後、ソフトウェア バージョンをアップグレードの実行前に戻すことができます。システムを再起動し、次の作業を実行して非アクティブなパーティションのソフトウェア バージョンに切り替えます。

（注） MCS 7825-H3 サーバ上のソフトウェアをアップグレードする場合、Cisco Emergency Responder の前のバージョンに戻すオプションはありません。

手順

ステップ 1 パブリッシャ ノードを以前のバージョンに戻します。
詳細については、パブリッシャ サーバの以前のバージョンへの復帰, （29 ページ）を参照してください。

ステップ 2 すべてのバックアップ サブスクライバ ノードを以前のバージョンに戻します。

詳細については、サブスクライバ サーバの以前のバージョンへの復帰, （29 ページ）を参照してください。

パブリッシャ サーバの以前のバージョンへの復帰

パブリッシャ サーバを以前のバージョンに復帰するには、次の手順を実行します。

手順

ステップ 1 次の URL を入力して、Cisco Unified Communications Operating System Administration を直接開きます。
https://server-name/**cmplatform**

server-name は、Emergency Responder サーバのホスト名または IP アドレスです。

ステップ 2 管理者ユーザ名とパスワードを入力します。

ステップ 3 [Settings] > [Version] を選択します。
[Version Settings] ウィンドウが表示されます。

ステップ 4 [Switch Versions] ボタンをクリックします。
システムの再起動を確認すると、システムが再起動します。処理が完了するまでに、最大で15分かかることがあります。

ステップ 5 バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a) 開いている Cisco Unified Communications Operating System Administration に再ログインします。
b) [Settings] > [Version] を選択します。
[Version Settings] ウィンドウが表示されます。
c) アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。
d) アクティブにしたサービスがすべて動作していることを確認します。
e) 次の URL を入力し、ユーザ名とパスワードを入力して Emergency Responder にログインします。
https://server-name/**ccmadmin**
f) ログインできること、および設定データが存在することを確認します。

サブスクライバ サーバの以前のバージョンへの復帰

サブスクライバ サーバを以前のバージョンに復帰するには、次の手順を実行します。

手順

手順

ステップ 1 次の URL を入力して、Cisco Unified Communications Operating System Administration を直接開きます。
https://server-name/**cmplatform**

server-name は、Emergency Responder サーバのホスト名または IP アドレスです。

ステップ 2 管理者ユーザ名とパスワードを入力します。

ステップ 3 [Settings] > [Version] を選択します。
[Version Settings] ウィンドウが表示されます。

ステップ 4 [Switch Versions] ボタンをクリックします。
システムの再起動を確認すると、システムが再起動します。処理が完了するまでに、最大で15分かかることがあります。

ステップ 5 バージョンの切り替えが正常に完了したことを確認するには、次の手順を実行します。

a) 開いている Cisco Unified Communications Operating System Administration に再ログインします。
b) [Settings] > [Version] を選択します。
[Version Settings] ウィンドウが表示されます。
c) アクティブなパーティションで、適切な製品バージョンが実行されていることを確認します。
d) アクティブにしたサービスがすべて動作していることを確認します。

ブリッジのアップグレード

ブリッジ アップグレードは、製造中止されたサーバから Emergency Responder の最新バージョンをサポートするサーバに移行するユーザに移行パスを提供します。

サポートが中止されたサーバは、ブリッジ アップグレード サーバとして機能することが許可され、アップグレードおよび起動できますが、Cisco Emergency Responder は正しく機能しません。

正常にアップグレードすると、新しいバージョンの Cisco Emergency Responder で実行できるのは DRS バックアップのみであることを通知する警告がコンソールに表示されます（この警告は、CLI セッションと GUI セッションの両方で表示されます）。

手順

ステップ 1 製造中止されたサーバで Emergency Responder の最新バージョンにアップグレードします。

ステップ 2 製造中止されたサーバの新しい Emergency Responder version バージョンを使用して、DRS バックアップを実行します。

（注） Cisco Emergency Responder および Cisco Phone Tracking エンジンは、製造中止されたサーバでのブリッジ アップグレード後は、サービスとして表示されません。

ステップ 3 製造中止されたサーバと同じホスト名で、サポートされる新しいサーバにEmergency Responderの新しいバージョンをインストールします。

ステップ 4 Emergency Responder の新しいバージョンを実行している新しくサポートされたサーバで、最初のノードに対して DRS の復元を実行します。

（注） ブリッジ アップグレード可能なサーバのリストについては、『Emergency Responder Release Notes』を参照してください。

カスタマイズされたログインメッセージのアップロード

[Cisco Unified Communications Operating System Administration] ページ、[Unified CM Administration]、およびCLIに表示されるカスタマイズされたログイン メッセージが含まれるテキスト ファイルをアップロードできます。

カスタマイズされたログイン メッセージをアップロードするには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウで、[Upgrades] > [Customized Logon Message] の順に選択します。
[Customized Logon Message] ウィンドウが表示されます。

ステップ 2 アップロードするテキスト ファイルを選択するには、[Browse] をクリックします。

ステップ 3 [Upload File] をクリックします。

（注） 10 KB を超えるファイルはアップロードできません。

システムにカスタマイズされたログイン メッセージが表示されます。

ステップ 4 デフォルトのログイン メッセージに戻すには、[Delete] をクリックします。
カスタマイズされたログインメッセージが削除され、システムにデフォルトのログインメッセージが表示されます。

Cisco Unified OS のサービス

次の各項では、Cisco Unified OS のサービスの使用方法について説明します。

別のシステムへの ping 送信

[Ping Configuration] ページで、他のシステムがネットワーク経由でアクセスできるかを確認するため、ping 要求を送信できます。

別のシステムに ping を送信するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Services] > [Ping] を選択します。
[Ping Configuration] ページが表示されます。 [Ping Configuration] ページの詳細は、Ping Configuration を参照してください。

ステップ 2 ping の送信先となるシステムの IP アドレスまたはネットワーク名を入力します。

ステップ 3 ping 間隔を秒で入力します。

ステップ 4 パケット サイズを入力します。

ステップ 5 ping 回数（システムに ping を送信する回数）を入力します。

（注） 複数回の ping を指定した場合は、**ping** コマンドを入力してもリアルタイムでは ping の日時が表示されません。 **ping** コマンドがデータを表示するのは、指定した回数だけ ping を送信した後です。

ステップ 6 IPSec を検証するかどうかを選択します。

ステップ 7 [Ping] をクリックします。
[Ping Results] テキスト ボックスに ping の統計情報が表示されます。

リモート サポートのセットアップ

[Remote Support] ページで、シスコのサポート担当者が指定日時に Emergency Responder システムにアクセスできるようにするためのリモート アカウントをセットアップできます。

リモート サポートは次の手順で行われます。

1. ユーザがリモート サポート アカウントを設定します。 このアカウントには、シスコの担当者がアクセスできる、設定可能な制限時間が含まれます。
2. リモート サポート アカウントの設定が完了すると、パス フレーズが生成されます。
3. ユーザはシスコのサポートに電話し、リモート サポート アカウント名とパス フレーズを伝えます。
4. シスコのサポート担当者はパスフレーズをデコーダ プログラムに入力し、パス フレーズからパスワードを生成します。
5. シスコのサポート担当者はデコードしたパスワードを使用して、お客様のシステムにリモート サポート アカウントでログインします。

6 アカウントの制限時間が経過すると、シスコのサポート担当者はリモート サポート アカウントにアクセスできなくなります。

リモート サポートを設定するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified OS Administration] Web ページから、[Services] > [Remote Support] を選択します。
[Remote Access Configuration] ページが表示されます。

ステップ 2 リモート サポート アカウントが設定されていない場合は、[Add] をクリックします。

ステップ 3 リモート アカウントのアカウント名と、アカウントの期限を、日単位で入力します。

（注） アカウント名の長さが 6 文字以上で、すべて小文字のアルファベットであることを確認してください。

ステップ 4 [Save] をクリックします。
[Remote Access Configuration] ページが再度表示されます。 [Remote Access Configuration] ページのフィールドの説明については、表 2を参照してください。

ステップ 5 生成されたパス フレーズを使用してシステムにアクセスする方法については、シスコの担当者にお問い合わせください。