Cisco Unity Connection の Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド、リリース 15

最終更新：2024 年 9 月 5 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

第 1 章 はじめに 1

概要 1

ブラウザ要件 2

オペレーティングシステムのステータスと設定 2

設定 3

セキュリティ設定 3

ソフトウェアのアップグレード 4

コマンドライン インターフェイス 5

第 2 章 Cisco Unified Communications Operating System Administration にログインする 7

Cisco Unified Communications Operating System Administration にログインする 7

OS 管理者およびセキュリティパスワードをリセットする 8

第 3 章 ステータスと設定 11

クラスタノード 11

ハードウェアステータス 12

ネットワーク設定 13

インストールされているソフトウェア 14

システムステータス 15

IP 設定 16

第 4 章 設定 19

概要 19

IP 設定 19

イーサネット設定 19
イーサネット IPv6 の構成設定 21
パブリッシャの設定 23
NTP サーバー 23
SMTP 設定 24
時刻設定 25

第 5 章 バージョン設定 27
バージョン設定 27
バージョンを切り替え、再起動する 27
現在のバージョンを再起動する 28
システムをシャットダウンする 28
代替手順 29

第 6 章 セキュリティ 31
セキュリティ 31
Internet Explorer のセキュリティオプションを設定する 31
証明書と証明書信頼リストを管理する 31
証明書を表示する 32
証明書をダウンロードする 32
証明書を削除、再作成する 32
サードパーティの CA 証明書を使用する 34
証明書の失効日をモニターする 40
証明書の失効 41
IPSEC 証明書を再作成する 42
IPSEC 管理 43
新しい IPSec ポリシーを設定する 43
既存の IPSec ポリシーを管理する 46
証明書の一括管理 47
セッション管理 48
暗号管理 48

暗号ストリングを設定する 49

第 7 章 ソフトウェアのアップグレード 51

ソフトウェアのインストールおよびアップグレード 51

デバイスロード管理 54

カスタムログインメッセージを設定する 54

Unity Connection のブランディングのカスタマイズ 55

ブランディング設定の前提条件 55

Unity Connection でブランディングを設定するためのタスクリスト 55

ユーザーインターフェイスのブランディングオプション 56

ブランディングファイルの構造 60

ブランディングプロパティの編集例 61

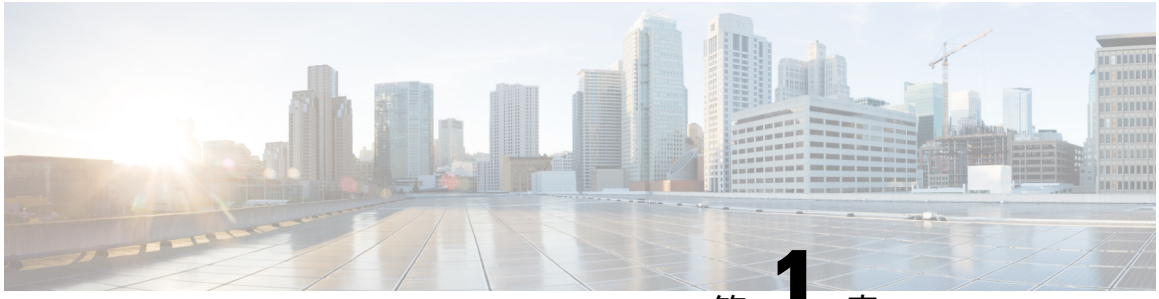
第 8 章 サービス 63

サービス 63

概要 63

ping 63

リモートサポートを設定する 64



第 1 章

はじめに

Cisco Unified Communications Manager および Cisco Unity Connection では、Cisco Unified Communications オペレーティング システムを使用して、多くの一般的なシステム管理機能を実行できます。

- 概要 （1 ページ）
- ブラウザ要件 （2 ページ）
- オペレーティングシステムのステータスと設定 （2 ページ）
- 設定 （3 ページ）
- セキュリティ設定 （3 ページ）
- ソフトウェアのアップグレード （4 ページ）
- コマンドライン インターフェイス （5 ページ）

概要

Cisco Unified Communications Operating System Administration を使用すると、Cisco Unified Communications Operating System を設定および管理できます。管理タスクの例を次に示します。

- ソフトウェアとハードウェアのステータスを確認する。
- IP アドレスの確認と更新を行う。
- 他のネットワーク デバイスに ping を送信する。
- NTP サーバーを管理する。
- システム ソフトウェアおよびオプションをアップグレードする。
- サーバーのセキュリティを管理する（IPSec や証明書を含む）
- リモート サポート アカウントを管理する
- システムを再起動する。

次のセクションでは、各オペレーティングシステムの機能について詳しく説明します。

ブラウザ要件

Cisco Unified Communications Operating System には、次のブラウザを使用してアクセスできます。

Cisco Unified Communications Operating System にアクセスできるブラウザ	以下のいずれかのオペレーティングシステムを使用
Microsoft Internet Explorer 8	• Microsoft XP サービスパック 3 • Microsoft Vista サービスパック 2 以降のサービスパック • 最新のサービスパックが適用された Microsoft Windows 7
Mozilla Firefox 3.x	• Microsoft XP サービスパック 3 • Microsoft Vista サービスパック 2 以降のサービスパック • 最新のサービスパックが適用された Microsoft Windows 7 • 最新のサービスパックを適用した Apple MAC OS X
Safari 4.x	Apple MAC OS X

すべての製品機能が正しく動作するように、Cisco Unified Communications オペレーティング システムサーバーの URL（**https://***servername*）がブラウザの「信頼済みサイト ゾーン」または「ローカル イントラネット サイト ゾーン」に含まれていることを確認します。

オペレーティングシステムのステータスと設定

[表示（Show）] メニューから、以下のような様々なオペレーティング システム コンポーネントのステータスを確認することができます。

- クラスタおよびノード
- ハードウェア
- ネットワーク
- システム
- インストールされているソフトウェアとオプション

詳細については、ステータスと設定を参照してください。

設定

[設定（Settings）] メニューから、以下のオペレーティングシステム設定を表示および更新できます。

- IP：アプリケーションのインストール時に入力した IP アドレスおよび DHCP クライアントの設定を更新します。
- NTP サーバーの設定（NTP Server Settings）：外部 NTP サーバーの IP アドレスの設定、および NTP サーバーの追加を行います。
- SMTP 設定（SMTP settings）：オペレーティングシステムが E メール通知の送信に使用する SMTP ホストを設定します。

詳細については、設定を参照してください。

[設定（Settings）]>[バージョン（Version）] ウィンドウから、システムを再起動またはシャットダウンするための次のオプションから選択できます。

- バージョンの切り替え（Switch Versions）：アクティブなディスクパーティションと非アクティブなディスクパーティションを切り替え、システムを再起動します。通常は、非アクティブなパーティションが更新され、新しいソフトウェアバージョンの実行を開始する場合に、このオプションを選択します。
- 現在のバージョン（Current Version）：パーティションを切り替えずにシステムを再起動します。
- システムのシャットダウン（Shutdown System）：実行中のすべてのソフトウェアを停止し、サーバーをシャットダウンします。

（注） このコマンドでは、サーバーの電源は切断されません。サーバーの電源を切るには、電源ボタンを押します。

詳細については、バージョン設定の章を参照してください。

セキュリティ設定

オペレーティングシステムのセキュリティオプションを使用すると、セキュリティ証明書とセキュア インターネット プロトコル（IPSec）を管理できます。**[セキュリティ（Security）]** メニューでは、次のセキュリティオプションを選択できます。

- 証明書の管理（Certificate Management）：証明書および証明書署名要求（CSR）を管理します。証明書の表示、アップロード、ダウンロード、削除、および再作成を行うことがで

きます。[証明書の管理（Certificate Management）] を使用して、ノード上の証明書の有効期限をモニターすることもできます。

- IPSECの管理（IPSEC Management）：既存のIPSECポリシーの表示や更新、新規のIPSECポリシーとアソシエーション設定を行います。

セキュリティの詳細については、セキュリティの章を参照してください。

ソフトウェアのアップグレード

ソフトウェアアップグレードオプションを使用すると、オペレーティングシステムで実行中のソフトウェアバージョンをアップグレードしたり、Cisco Unified Communications オペレーティングシステムのロケールインストーラー、ダイヤルプラン、TFTPサーバーファイルなど、特定のソフトウェアオプションをインストールしたりできます。

[インストール/アップグレード（Install/Upgrade）] メニューオプションで、ローカルディスクまたはリモートサーバーからシステムソフトウェアをアップグレードできます。アップグレードしたソフトウェアは非アクティブなパーティションにインストールされ、その後でシステムの再起動とパーティションの切り替えができます。これにより、システムで新しいソフトウェアバージョンが実行されます。

（注） すべてのソフトウェアのインストールとアップグレードは、Cisco Unified Communications オペレーティングシステムのGUIとコマンドラインインターフェイスに含まれるソフトウェアアップグレード機能を使用して行う必要があります。このシステムでアップロードおよび処理できるソフトウェアは、シスコによって承認されたものだけです。以前のバージョンのCisco Unified Communications Managerで使用していたサードパーティ製またはWindowsベースのソフトウェア アプリケーションをインストールまたは使用することはできません。

詳細については、ソフトウェアのアップグレードの章を参照してください。

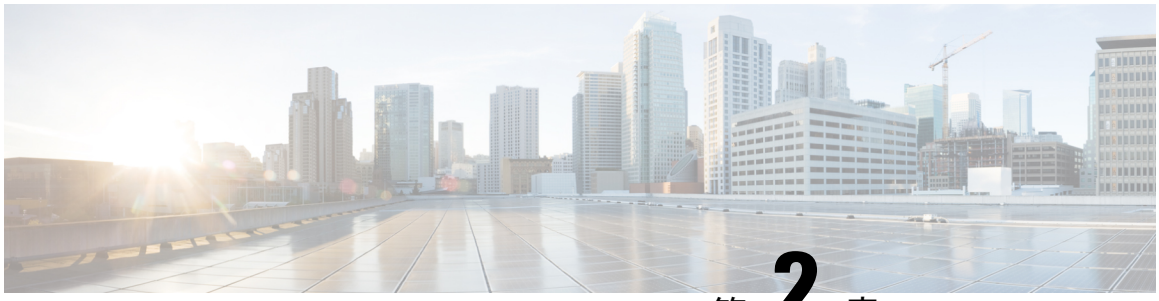
このアプリケーションでは、次のオペレーティング システム ユーティリティを使用できます。

- Ping：他のネットワークデバイスとの接続を確認します。
- リモートサポート（Remote Support）：シスコのサポート担当者がシステムへのアクセスに使用できるアカウントを設定します。このアカウントは、指定した日数が経過すると自動的に失効します。

セキュリティの詳細については、サービスの章を参照してください。

コマンドライン インターフェイス

コンソールから、またはサーバーへの安全なシェル接続を介して、コマンドライン インターフェイスにアクセスすることができます。詳細については、『Cisco Unifed Communications Solutions コマンドライン インターフェイス リファレンス ガイド』を参照してください。



第 2 章

Cisco Unified Communications Operating System Administration にログインする

この章では、Cisco Unified Communications Operating System Administration にアクセスする手順と、紛失したパスワードをリセットする手順について説明します。

- Cisco Unified Communications Operating System Administration にログインする （7 ページ）
- OS 管理者およびセキュリティパスワードをリセットする （8 ページ）

Cisco Unified Communications Operating System Administration にログインする

Cisco Unified Communications Operating System Administration にアクセスしてログインするには、次の手順に従います。

（注） Cisco Unified Communications Operating System Administration の使用中は、ブラウザコントロール（[戻る（Back）] ボタンなど）を使用しないでください。

ステップ 1 Cisco Unity Connection Administration の URL を参照します。

ステップ 2 [Cisco Unity Connection Administration] ウィンドウの右上隅にあるナビゲーション メニューから、**[Cisco Unified OS Administration]** を選択し、**[移動（Go）]** をクリックします。

[Cisco Unified Communications Operating System Administration Logon] ウィンドウが表示されます。

（注） 次の URL を入力して、Cisco Unified Communications Operating System Administration に直接アクセスすることもできます：**http://***server-name***/cmplatform**

ステップ 3 管理者ユーザー名とパスワードを入力します。

（注） 管理者のユーザー名とパスワードは、インストール時に設定されるか、コマンドライン インターフェイスで作成されます。

ステップ 4 **[送信（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。

OS 管理者およびセキュリティパスワードをリセットする

管理者パスワードまたはセキュリティパスワードを忘れた場合は、次の手順を使用してこれらのパスワードをリセットします。

パスワードリセットプロセスを実行するには、システムコンソールを介して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ーがサーバーに接続されている必要があります。セキュアシェルセッションを介してシステムに接続している場合は、パスワードをリセットできません。

注意 セキュリティパスワードは、クラスタ内のすべてのノードで一致している必要があります。セキュリティパスワードは、すべてのマシン上で変更してください。変更していない場合、クラスタノードが通信不能になります。

注意 セキュリティパスワードを変更したら、クラスタ内の各ノードをリセットする必要があります。サーバ（ノード）のリブートに失敗すると、システムサービスに問題が発生し、さらにサブスクライバサーバーの [Cisco Unified Communications Manager Administration] ウィンドウにも問題が発生します。

（注） この手順中、物理的にシステムにアクセスできることを確認するために、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。

ステップ 1 次のユーザー名とパスワードを使用してシステムにログインします。

- ユーザー名：**pwrecovery**
- パスワード：**pwreset**

[プラットフォームのパスワードリセットへようこそ（Welcome to platform password reset）] ウィンドウが表示されます。

ステップ 2 何か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 がある場合は、ここで取り出します。

ステップ 4 何かキーを押して続行します。

システムは、ディスクドライブから CD または DVD が取り出されたことを確認します。

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。

システムは、ディスクが挿入されていることを確認します。

ステップ 6 ディスクが挿入されたことをシステムが確認した後、続行するために以下のオプションのいずれかを入力するようプロンプトが表示されます。

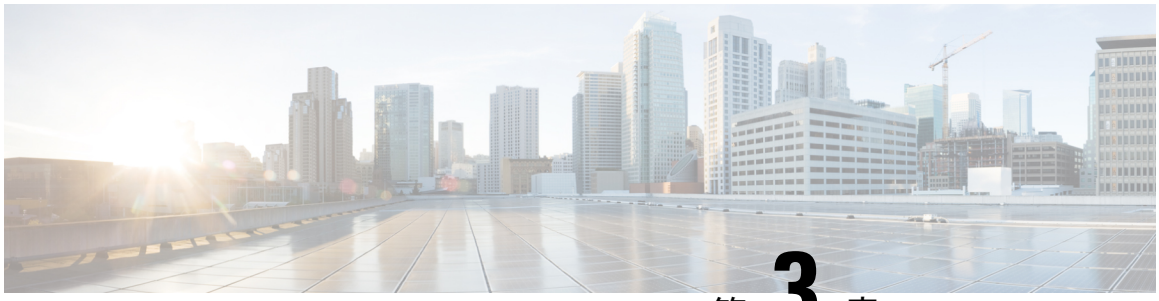
- 管理者パスワードをリセットする場合は、**a** を入力します。
- セキュリティパスワードをリセットする場合は、**s** を入力します。
- 終了する場合は、**q** を入力します。

ステップ 7 作成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 パスワードを再度入力します。

パスワードを 6 文字以上で入力してください。システムは新しいパスワードの強度をチェックします。パスワードが強度チェックに合格しない場合は、新しいパスワードを入力するように求められます。

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に指示されます。



第 3 章

ステータスと設定

この章では、システムの管理に関する情報を提供し、次の項目を含みます。

- クラスタノード （11 ページ）
- ハードウェアステータス （12 ページ）
- ネットワーク設定 （13 ページ）
- インストールされているソフトウェア （14 ページ）
- システムステータス （15 ページ）
- IP 設定 （16 ページ）

クラスタノード

クラスタ内のノードに関する情報を表示するには、次の手順を実行します。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[表示（Show）]** > **[クラスタ（Cluster）]** に移動します。

[クラスタノード（Cluster Nodes）] ウィンドウが表示されます。

ステップ 2 [クラスタノード（Cluster Nodes）] ウィンドウのフィールドの説明については、表 1: クラスタノードフィールド（表）ノード、クラスタフィールド（表）クラスタノードのフィールド説明を参照してください。

表 *1*: クラスタノードのフィールド説明

フィールド	説明
ホスト名（Hostname）	サーバーの完全なホスト名を表示します。
IP アドレス（IP Address）	サーバーの IP アドレスを表示します。
エイリアス（Alias）	サーバーのエイリアス名を表示します（定義されている場合）。

フィールド	説明
ノードのタイプ（Type of Node）	サーバーがパブリッシャノードまたはサブスクライバノードのどちらであるかを示します。

ハードウェアステータス

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。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[表示（Show）]**>**[ハードウェア（Hardware）]** に移動します。

[ハードウェアステータス（Hardware Status）] ウィンドウが表示されます。

ステップ 2 [ハードウェアステータス（Hardware Status）] ウィンドウのフィールドの説明については、 表 2 : ハードウェア、ステータスフィールド（表）ステータスハードウェアフィールド（表）オペレーティングシステムハードウェアステータスフィールド（表）ハードウェアステータスのフィールド説明を参照してください。

表 *2:* ハードウェアステータスのフィールド説明

フィールド	説明
プラットフォームタイプ（Platform Type）	プラットフォームサーバーのモデル ID を表示します。
プロセッサ速度（Processor Speed）	プロセッサの速度を表示します。
CPU タイプ（CPU Type）	プラットフォームサーバーのプロセッサのタイプを表示します。
メモリ（Memory）	メモリの総量を MBytes 単位で表示します。
オブジェクト ID（Object ID）	オブジェクト ID を表示します。
OS バージョン（OS Version）	オペレーティングシステムのバージョンを表示します。
RAID の詳細（RAID Details）	コントローラ情報、論理ドライブ情報、物理デバイス情報など、RAID ドライブに関する

ネットワーク設定

表示されるネットワーク ステータス情報は、ネットワーク耐障害性が有効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管理します。ネットワーク耐障害性が有効になっている場合、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。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[表示（Show）]** > **[ネットワーク（Network）]** に移動します。

[ネットワーク設定（Network Settings）] ウィンドウが表示されます。

ステップ 2 [ネットワーク設定（Network Settings）] ウィンドウのフィールドの説明については、表 3 : ステータスネットワークフィールド（表）ネットワークステータスフィールド（表）オペレーティングシステムネットワーク ステータス フィールド（表）ネットワーク設定のフィールド説明 を参照してください。

表 *3* : ネットワーク設定のフィールド説明

フィールド	説明
イーサネットの詳細	
DHCP	イーサネットポート 0 で DHCP が有効になっているかどうかを示します。
ステータス（Status）	イーサネットポート 0 および 1 のポートがアップかダウンかを示します。
IP アドレス（IP Address）	イーサネットポート 0（およびネットワーク フォールト トレランス（NFT）が有効になっている場合はイーサネットポート 1）の IP アドレスを表示します。
IP マスク（IP Mask）	イーサネットポート 0（および NFT がイネーブルの場合はイーサネットポート 1）の IP マスクを表示します。
リンク検出（Link Detected）	アクティブなリンクが存在するかどうかを示します。
キューの長さ（Queue Length）	キューの長さを表示します。

フィールド	説明
MTU	インターフェイスの最大伝送単位を表示します。
MAC アドレス（MAC Address）	ポートのハードウェアアドレスを表示します。
受信統計（RX）	受信したバイト、パケット、およびエラーに関する情報と、ドロップおよびオーバーランの統計情報を表示します。
送信統計情報（TX）	送信バイト、パケット、およびエラーに関する情報と、ドロップ、キャリア、およびコリジョンの統計情報を表示します。
DNS詳細	
プライマリ（Primary）	プライマリ ドメイン ネーム サーバーの IP アドレスを入力します。
セカンダリ（Secondary）	セカンダリ ドメイン ネーム サーバーの IP アドレスを入力します。
Optionsosadmin-3-2	設定されている DNS オプションを表示します。
ドメイン（Domain）	サーバーのドメインを表示します。
ゲートウェイ（Gateway）	イーサネットポート 0 のネットワークゲートウェイの IP アドレスを表示します。

インストールされているソフトウェア

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。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[表示（Show）]**>**[ソフトウェア（Software）]** に移動します。

[ソフトウェアパッケージ（Software Packages）] ウィンドウが表示されます。

ステップ 2 [ソフトウェアパッケージ（Software Packages）] ウィンドウのフィールドの説明については、表 4 : ソフトウェアインストールフィールド（表）インストールしたソフトウェアフィールド（表）ソフトウェアパッケージのフィールド説明を参照してください。

表 *4:* ソフトウェアパッケージのフィールド説明

フィールド	説明
パーティションのバージョン（Partition Versions）	アクティブパーティションと非アクティブパーティションで実行されているソフトウェアバージョンを表示します。
アクティブ バージョン インストール済みソフトウェアオプション（Active Version Installed Software Options）	アクティブなバージョンにインストールされている、ロケールやダイヤルプランを含む、インストールされているソフトウェアオプションのバージョンを表示します。
非アクティブ バージョン インストール済みソフトウェアオプション（Inactive Version Installed Software Options）	非アクティブなバージョンにインストールされている、ロケールやダイヤルプランを含む、インストールされているソフトウェアオプションのバージョンを表示します。

システムステータス

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。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[表示（Show）]** > **[システム（System）]** に移動します。

[システムステータス（System Status）] ウィンドウが表示されます。

ステップ 2 [プラットフォームステータス（Platform Status）] ウィンドウのフィールドの説明については、表 5: ステータスシステムフィールド（表）システムステータスフィールド（表）システムステータスのフィールド説明 を参照してください。

表 *5:* システムステータスのフィールド説明

フィールド	説明
ホスト名（Host Name）	Cisco Unified Communications オペレーティングシステムがインストールされている Cisco MCS ホストの名前を表示します。
日付（Date）	オペレーティングシステムのインストール時に指定された大陸と地域に基づいて日時を表示します。
タイムゾーン（Time Zone）	インストール時に選択したタイムゾーンを表示します。

フィールド	説明
ロケール（Locale）	オペレーティングシステムのインストール時に選択した言語を表示します。
製品バージョン（Product Version）	オペレーティングシステムのバージョンを表示します。
プラットフォームバージョン（Platform Version）	プラットフォームのバージョンを表示します。
稼働時間（Uptime）	システムのアップタイム情報が表示されます。
CPU	アイドル状態の CPU キャパシティのパーセンテージ、システムプロセスを実行しているパーセンテージ、およびユーザープロセスを実行しているパーセンテージを表示します。
メモリ（Memory）	合計メモリ量、空きメモリ量、使用済みメモリ量（キロバイト単位）など、メモリ使用率に関する情報を表示します。
ディスク/アクティブ（Disk/active）	アクティブディスクの合計、空き、および使用済みディスク容量を表示します。
ディスク/非アクティブ（Disk/inactive）	非アクティブなディスクの合計、空き、および使用済みディスク容量を表示します。
ディスク/ロギング（Disk/logging）	ディスクロギングに使用されているディスク容量の合計、空き容量を表示します。

IP 設定

[IP 設定（IP Preferences）] ウィンドウを使用して、システムが使用できる登録済みポートのリストを表示できます。[IP 設定（IP Preferences）] ウィンドウには、次の情報が含まれています。

- アプリケーション
- プロトコル
- ポート番号
- タイプ
- 変換されたポート
- ステータス

- 説明

[IP 設定（IP Preferences）] ウィンドウにアクセスするには、次の手順を実行します。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[表示（Show）] > [IP 設定（IP Preferences）]** に移動します。

[IP 設定（IP Preferences）] ウィンドウが表示されます。このウィンドウには、アクティブな（以前の）クエリーのレコードも表示されることがあります。

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 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。 条件を追加すると、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、**[フィルタのクリア（Clear Filter）]** ボタンをクリックします。

ステップ 3 **[検索（Find）]** をクリックします。

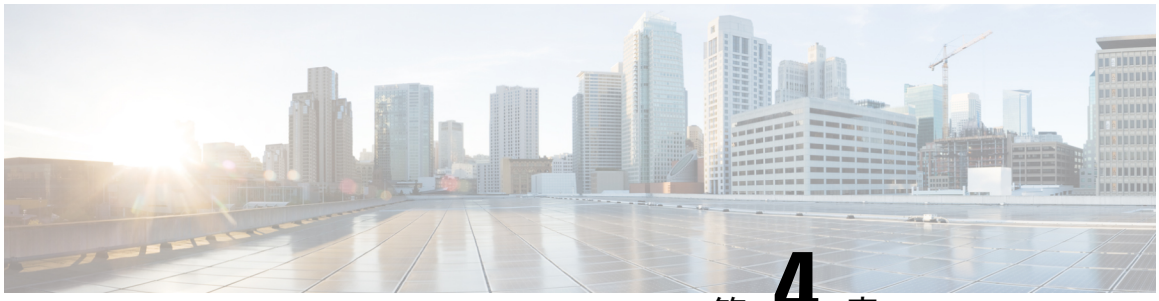
条件を満たしているレコードがすべて表示されます。1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数（Rows per Page）] ドロップダウン リスト ボックスで別の値を選択します。

[IP 設定（IP Preferences）] フィールドの説明については、以下を参照してください。

表 *6 : IP* 設定のフィールド説明

フィールド	説明
アプリケーション（Application）	ポートを使用する（リッスンする）アプリケーションの名前。
プロトコル（Protocol）	このポートで使用されるプロトコル（TCP、UDP など）。
ポート番号（Port Number）	数値ポート番号。

フィールド	説明
タイプ（Type）	このポートで許可されるトラフィックのタイプ： • パブリック（Public）：すべてのトラフィックが許可されます。 • 変換済み（Translated）：すべてのトラフィックが許可されますが、別のポートに転送されます。 • プライベート（Private）：クラスタ内の他のノードなど、定義された一連のリモートサーバーからのトラフィックのみが許可されます。
変換されたポート（Translated Port）	このポート宛てのトラフィックは、[ポート番号（Port Number）] 列にリストされているポートに転送されます。このフィールドは、変換済みタイプのポートにのみ適用されます。
ステータス（Status）	ポート使用状況のステータス： • 有効（Enabled）：アプリケーションによって使用され、ファイアウォールによって開かれます。 • 無効（Disabled）：ファイアウォールによってブロックされており、使用されていません。
説明（Description）	ポートの使用方法の簡単な説明。



第 4 章

設定

- 概要 （19 ページ）
- IP 設定 （19 ページ）
- NTP サーバー （23 ページ）
- SMTP 設定 （24 ページ）
- 時刻設定 （25 ページ）

概要

IP 設定、ホスト設定、および Network Time Protocol（NTP）設定を表示および変更するには、[設定（Settings）] オプションを使用します。

IP 設定

[IP 設定（IP Settings）] オプションを使用すると、イーサネット接続の IP とポートの設定を表示および変更できます。また、後続のノードでは、パブリッシャの IP アドレスを設定できます。

イーサネット設定

[IP 設定（IP Settings）] ウィンドウには、Dynamic Host Configuration Protocol（DHCP）がアクティブかどうかが表示され、関連するイーサネット IP アドレスとネットワークゲートウェイの IP アドレスも表示されます。

すべてのイーサネット設定は、Eth0 にのみ適用されます。Eth1 の設定は構成できません。デフォルトでは、[最大転送単位（MTU）（Maximum transmission unit (MTU)）] は 1,500 バイトに設定されます。

IP 設定を表示するには、次の手順を実行します。

注意 Cisco Unity Connection の IP 設定を変更する手順は使用しないでください。

注意 Connection サーバーの IP アドレスの変更については、https://www.cisco.com/c/ja_jp/support/unified-communications/unity-connection/products-installation-guides-list.html にある『Changing the IP Addresses of Cisco Unity Connection Servers』『*Unity Connection* アップグレードガイド』の「Cisco Unity Connection Servers の IP アドレスを変更する」を参照してください。

注意 Unity Connection サーバーのホスト名の変更については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html にある『*Cisco Unity Connection* インストール、アップグレード、およびメンテナンスガイド *15*』を参照してください。

[Cisco Unified Communications Operating System Administration] ウィンドウから **[設定（Settings）]** > **[IP]** > **[イーサネット（Ethernet）]** に移動します。

[イーサネット設定（Ethernet Settings）] ウィンドウが表示されます。[イーサネット設定（Ethernet Settings）] ウィンドウのフィールドの説明については、 表 7 : 設定イーサネットフィールド（表）イーサネット設定のフィールドと説明を参照してください。

表 *7*: イーサネット設定のフィールドと説明

フィールド	説明
DHCP	DHCP が有効か無効かを示します。
Hostname（ホスト名）	サーバーの完全なホスト名を表示します。
IP アドレス（IP Address）	システムの IP アドレスを表示します。
サブネットマスク（Subnet Mask）	IP サブネットマスクアドレスを表示します。
デフォルトゲートウェイ（Default Gateway）	ネットワークゲートウェイの IP アドレスを表示します。

イーサネット IPv6 の構成設定

（注） 次に示す設定は、Cisco Unity Connection リリース 9.0 以降に適用されます。IPv6 は、以前のバージョンの Cisco Unity Connection ではサポートされていません。

[イーサネット IPv6 構成設定（Ethernet IPv6 Configuration Settings）] ページでは、IPv6 を有効にし、IP アドレスの取得方法を決定できます。

IPv6 設定を表示または変更するには、次の手順を実行します。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[設定（Settings）]** > **[IP]** > **[イーサネット IPv6 設定（Ethernet IPv6 Configuration）]** に移動します。

ステップ 2 イーサネット IPv6 設定を変更するには、該当するフィールドに新しい値を入力します。[イーサネット IPv6 構成設定（Ethernet IPv6 Configuration Settings）] ウィンドウのフィールドの説明については、 表 4-2を参照してください。

ステップ 3 変更を保存するには、**[保存（Save）]** を選択します。

表 *8*：イーサネット *IPv6* 設定のフィールドと説明

フィールド	説明
IPv6を有効化（Enable IPv6）	IPv6 を有効にするには、このチェックボックスをオンにします。

フィールド	説明
アドレスソース（Address Source）	次のいずれかを選択します。 • ルータアドバタイズメント（Router Advertisement）：ネットワーク上のサーバーにネットワークプレフィックスをアドバタイズするようにネットワークルータが設定されている場合は、このオプションを選択します。 • DHCP：DHCPv6プロトコルを使用してサーバーにアドレスを割り当てるには、このオプションを選択します（アドレスを提供するには、ネットワーク上でDHCPv6サーバーを実行している必要があります）。 • 手動入力（Manual Entry）: [IPv6アドレス（IPv6 Address）] フィールドに手動でアドレスを入力する場合は、このオプションを選択します。 （注） Cisco Unity Connection サーバーでは、スタティックな非リンクローカル IPv6 アドレスを使用することを推奨します。サーバーがDHCPv6サーバーから、またはステートレスアドレス自動設定を介して IPv6 アドレスを取得する場合は、サーバーが DHCPv6 サーバーから 1 つの非リンクローカル IPv6 アドレスのみを取得することを確認します。
IPv6 アドレス（IPv6 Address）	アドレスソースとして [手動入力（Manual Entry）] を選択した場合は、IPv6 アドレスを入力します。 たとえば、次のように入力します。 2001:0DB8:BBBB:CCCC:0987:65FF:FE01:2345
サブネットマスク（Subnet Mask）	[アドレスソース（Address Source）] として [手動入力（Manual Entry）] を選択した場合は、ネットワークのプレフィックスに対応するアドレスのビット数を示すプレフィックス長（0～128）を入力します。 たとえば、64 と入力します。

フィールド	説明
再起動による更新（Update with Reboot）	更新した設定を保存するときにサーバーをすぐにリブートする場合は、このチェックボックスをオンにします。 （注） IPv6設定を有効にするには、システムを再起動する必要があります。

パブリッシャの設定

この機能は、Cisco Unified Communications Manager がサーバーに単独でインストールされている場合にのみ適用されます。

NTP サーバー

外部 NTP サーバーがストラタム 9 以上（1 ～ 9）であることを確認します。外部 NTP サーバーを追加、削除、または変更するには、次の手順を実行します。

（注） NTP サーバー設定は、最初のノードまたはパブリッシャでのみ設定できます。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[設定（Settings）]** > **[NTP サーバー（NTP Servers）]** に移動します。

[NTP サーバー設定（NTP Server Settings）] ウィンドウが表示されます。

ステップ 2 NTP サーバーを追加、削除、または変更できます。

（注） 発生する可能性のある互換性の問題、精度の問題、およびネットワーク ジッターの問題を回避するには、プライマリノードに指定する外部 NTP サーバーが NTP v4（バージョン 4）である必要があります。IPv6 アドレッシングを使用している場合は、外部 NTP サーバーが NTP v4 である必要があります。

- NTP サーバーを削除するには、該当するサーバーの前にあるチェックボックスをオンにして、**[削除（Delete）]** をクリックします。
- NTP サーバーを追加するには、**[追加（Add）]** をクリックし、ホスト名またはIPアドレスを入力し、**[保存（Save）]** をクリックします。
- NTP サーバーを変更するには、IP アドレスをクリックし、ホスト名または IP アドレスを変更して、**[保存（Save）]** をクリックします。

  NTP サーバーに加えた変更は、完了するまでに最大 5 分かかる場合があります。NTP サーバーに変更を加えるたびに、ウィンドウ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 サーバー設定（NTP Server Settings）] ウィンドウを更新して正しいステータスを表示するには、**[設定（Settings）]** > **[NTP]** を選択します。

（注） NTP サーバーを削除、変更、または追加した後、変更を有効にするには、クラスタ内の他のすべてのノードを再起動する必要があります。

SMTP 設定

[SMTP 設定（SMTP Settings）] ウィンドウでは、SMTP ホスト名を表示または設定し、SMTP ホストがアクティブかどうかを示すことができます。

ヒント システムから電子メールが送信されるようにするには、SMTP ホストを設定する必要があります。

SMTP 設定にアクセスするには、次の手順を実行します。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[設定（Settings）]** > **[SMTP]** に移動します。

[SMTP 設定（SMTP Settings）] ウィンドウが表示されます。

ステップ 2 ホスト名または IP アドレスを入力します。

ステップ 3 **[保存（Save）]** をクリックします。

時刻設定

手動で時間を設定するには、以下の手順に従います。

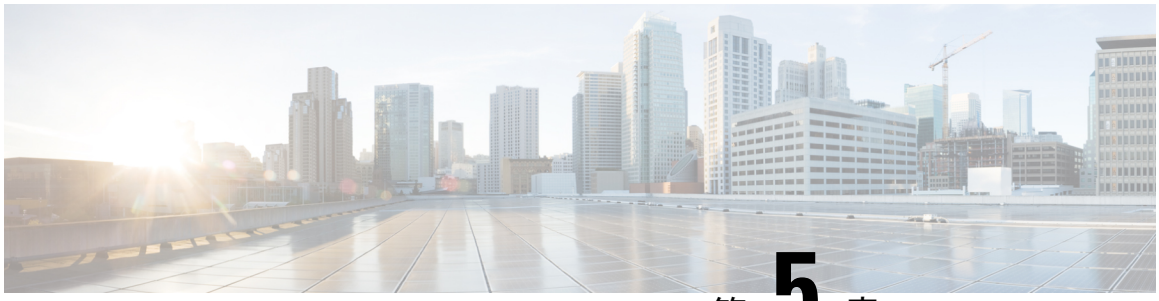
（注） サーバーの時刻を手動で設定する前に、設定した NTP サーバーを削除する必要があります。詳細については、 NTP サーバーの項を参照してください。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[設定（Settings）]** > **[時間（Time）]** に移動します。

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 **[保存（Save）]** をクリックします。

ステップ 4 Cisco Unity Connection サーバーで、日付を変更した場合、または時刻を 2 分以上変更した場合は、CLI コマンド **utils system restart** を使用してサーバーを再起動します。



第 5 章

バージョン設定

• バージョン設定 （27 ページ）

バージョン設定

バージョンを切り替え、再起動する

このオプションは、新しいソフトウェアバージョンにアップグレードする場合と、以前のソフトウェアバージョンにフォールバックする必要がある場合の両方で使用できます。アクティブなディスクパーティションで実行されているシステムをシャットダウンし、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でシステムを自動的に再起動するには、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。

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、**[設定（Settings）]** > **[バージョン（Version）]** の順に選択します。

[バージョン設定（Version Settings）] ウィンドウが表示され、アクティブパーティションと非アクティブパーティションの両方のソフトウェアバージョンが表示されます。

ステップ 2 **[バージョンの切り替え（Switch Versions）]** をクリックして、バージョンを切り替えてノードを再起動します。操作を停止するには、**[キャンセル（Cancel）]** をクリックします。

[バージョンの切り替え（Switch Version）] をクリックすると、システムが再起動し、現在非アクティブなパーティションがアクティブになります。

現在のバージョンを再起動する

バージョンを切り替えずに現在のパーティションでシステムを再起動するには、次の手順に従います。

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。

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、**[設定（Settings）]** > **[バージョン（Version）]** の順に選択します。

[バージョン設定（Version Settings）] ウィンドウが表示され、アクティブパーティションと非アクティブパーティションの両方のソフトウェアバージョンが表示されます。

ステップ 2 システムを再起動するには、**[再起動（Restart）]** をクリックします。操作を停止するには、**[キャンセル（Cancel）]** をクリックします。

[再起動（Restart）] をクリックすると、システムはバージョンを切り替えずに現在のパーティションで再起動します。

システムをシャットダウンする

注意 サーバーの電源ボタンを押して、サーバーをシャットダウンしたり、サーバーを再起動したりしないでください。これを行うと、誤ってファイルシステムが破損し、サーバーをリブートできなくなる可能性があります。

システムをシャットダウンするには、手順 1 または手順 2 に従います。

注意 この手順を実行すると、システムがシャットダウンします。

ステップ 1 [Cisco Unified Communications オペレーティング システムの管理（Cisco Unified Communications Operating System Administration）] ウィンドウで、**[設定（Settings）]** > **[バージョン（Version）]** の順に選択します。

[バージョン設定（Version Settings）] ウィンドウが表示され、アクティブパーティションと非アクティブパーティションの両方のソフトウェアバージョンが表示されます。

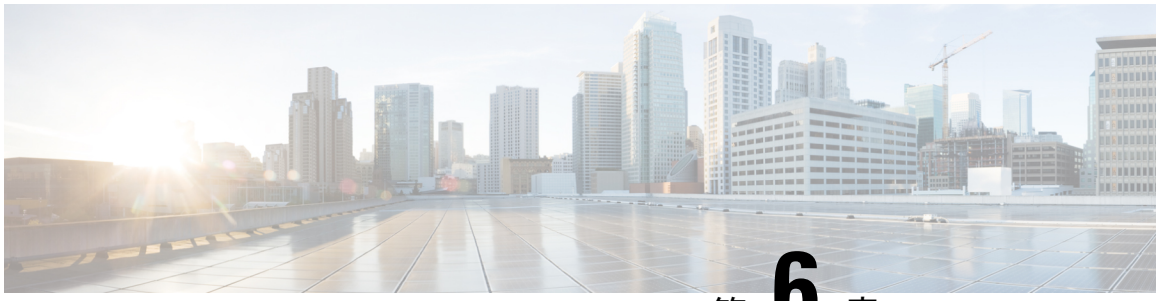
ステップ 2 システムをシャットダウンするには、**[シャットダウン（Shutdown）]** をクリックします。操作を停止するには、**[キャンセル（Cancel）]** をクリックします。

[シャットダウン（Shutdown）] をクリックすると、システムはすべてのプロセスを停止し、シャットダウンします。

（注） ハードウェアの電源がオフになるまでに数分かかる場合があります。

代替手順

CLI コマンド utils system shutdown またはコマンド utils system restart を実行します。CLIコマンドの実行方法については、『Cisco Unifed Communications Solutions コマンドライン インターフェイス リファレンス ガイド』を参照してください。



第 6 章

セキュリティ

• セキュリティ （31 ページ）

セキュリティ

Internet Explorer のセキュリティオプションを設定する

ノードから証明書をダウンロードするには、次の手順に従って Internet Explorer のセキュリティ設定を構成します。

ステップ 1 Internet Explorer を起動します。

ステップ 2 **[ツール（Tools）]** > **[インターネットオプション（Internet Options）]** に移動します。

ステップ 3 **[詳細設定（Advanced）]** タブをクリックします。

ステップ 4 [詳細設定（Advanced）] タブの [セキュリティ（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、**[暗号化されたページをディスクに保存しない（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。

証明書と証明書信頼リストを管理する

ここでは、[証明書管理（Certificate Management）] メニューから実行できる機能について説明します。

（注） [セキュリティ（Security）] メニュー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。

証明書を表示する

既存の証明書を表示するには、次の手順を実行します。

ステップ 1 **[セキュリティ（Security）] > [証明書管理（Certificate Management）]**の順に選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用できます。

ステップ 3 証明書またはトラストストアの詳細を表示するには、[共通名（Common Name）] の下にある証明書のファイル名をクリックします。

[証明書の詳細（Certificate Details）] ウィンドウに、証明書に関する情報が表示されます。 ファイルの整合性をチェックするために、証明書の SHA-512 チェックサム値も表示されます。

ステップ 4 [証明書リスト（Certificate List）] ウィンドウに戻るには、[証明書の詳細（Certificate Details）] ウィンドウで [閉じる（Close）] をクリックします。

証明書をダウンロードする

Cisco Unified Communications オペレーティング システムから PC に証明書をダウンロードするには、次の手順に従います。

ステップ 1 **[セキュリティ（Security）] > [証明書管理（Certificate Management）]**の順に選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用できます。

ステップ 3 [共通名（Common Name）] の下にある証明書のファイル名をクリックします。

[証明書詳細（Certificate Details）] ウィンドウが表示されます。

ステップ 4 **[.PEMファイルのダウンロード（Download .PEM File）]** または [.DER ファイルのダウンロード（Download .DER File）] をクリックします。

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

証明書を削除、再作成する

ここでは、証明書の削除と再生成について説明します。

証明書を削除する

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。[証明書（Certificate）] リストから選択した証明書の既存の CSR はシステムから削除されるため、新しい CSR を生成する必要があります。詳細については、証明書署名要求を生成するを参照してください。

ステップ 1 **[セキュリティ（Security）] > [証明書管理（Certificate Management）]**の順に選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、[検索（Find）] コントロールを使用できます。

ステップ 3 [共通名（Common Name）] の下にある証明書のファイル名をクリックします。

[証明書詳細（Certificate Details）] 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。

証明書を再生成する

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。

ステップ 1 **[セキュリティ（Security）] > [証明書管理（Certificate Management）]**の順に選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 **[Generate Self-signed（自己署名付きの生成）]** > または > **[CSRの生成（Generate CSR）]** をクリックします。

[証明書の生成（Generate Certificate）] ダイアログボックスが表示されます。

ステップ 3 [証明書名（Certificate Name）] リストから、証明書の名前を選択します。表示される証明書名の説明については、 表 9 : 証明書の名前と説明を参照してください。

ステップ 4 **[生成（Generate）]** をクリックします。

（注） Cisco Unified Communications Operating System で証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップの実行については、『*Cisco Unity Connection* インストール、アップグレード、およびメンテナンスガイド』を参照してください。

表 *9*：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、Unity Connection サーバーのインストール時に生成され、証明書タイプは RSA キーベースです。
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。
tomcat-ECDSA	この自己署名ルート証明書は、Unity Connection サーバーのインストール時に生成され、証明書タイプは EC キーベースです。 （注） CallManager は証明書の命名規則でのみ使用されますが、生成される証明書は Unity Connection サーバーに固有です。

サードパーティの CA 証明書を使用する

シングルサーバーおよびマルチサーバー証明書の概要

名前が示すように、単一サーバー証明書には、そのFQDNの信頼のみを識別する単一のFQDNが含まれています。単一のFQDNまたはドメインがサブジェクト代替名（SAN）拡張に存在します。クラスタ内に複数のサーバーがある場合、システムはサーバーごとに1つずつ、同じ数の X.509 証明書を生成する必要があります。

システムは、マルチサーバー証明書を使用して、複数のサーバー、ドメイン、またはサブドメインの信頼を識別します。マルチサーバー証明書の SAN 拡張には、複数の FQDN またはドメインが含まれています。

（注） テレフォニー統合の場合、マルチサーバー SAN 証明書は SIP 統合でのみサポートされます。ただし、SCCP 統合では、単一サーバー証明書のみがサポートされます。

次の表に、単一サーバー証明書とマルチサーバー証明書の基本的な違いを示します。

表 *10*：証明書の設定の比較

単一サーバー証明書	マルチサーバー証明書
CNフィールドまたはSAN拡張、あるいはその両方に単一のFQDNまたはドメインが含まれています。	SAN 拡張に存在する複数の FQDN またはドメインが含まれています。

単一サーバー証明書	マルチサーバー証明書
システムは、クラスタ内のサーバーごとに1つの証明書を使用します。	1 つの証明書で複数のサーバーを識別します。
管理者は、証明書の期限切れ、秘密キーの侵害などの状況で、個々のサーバーで証明書と秘密キーを再生成します。	この証明書は、すべてのサーバーに共通の公開キーと秘密キーのペアを1つだけカバーしているため、同じ秘密キーを証明書とともにクラスタ内のすべてのサーバーに安全に転送する必要があります。いずれかのサーバーで秘密キーが侵害された場合は、すべてのサーバーに対して証明書と秘密キーを再生成する必要があります。
管理者は、クラスタ内の各サーバーについて、証明書署名要求（CSR）の生成、署名のためのCSR の CA への送信、署名済み証明書のアップロードなどの手順を実行する必要があるため、単一のサーバー証明書の生成は、大規模クラスタの管理者にとってオーバーヘッドになる可能性があります。	管理者は、特定のサーバーで手順を1回だけ実行し、システムがクラスタ内のすべてのサーバーに関連付けられた秘密キーと署名付き証明書を配布するため、マルチサーバー証明書を管理する際のオーバーヘッドが少なくなります。

Cisco Unified Communications オペレーティングシステムは、サードパーティの認証局（CA）が PKCS # 10 証明書署名要求（CSR）で発行する証明書をサポートします。

次の表に、このプロセスの概要と、その他のドキュメントへの参照を示します。

	タスク	関連情報
ステップ 1	Cisco Unified Communications Operating System Administration にログインします。	Cisco Unified Communications オペレーティング システムの管理では、システム管理者は、マルチサーバーオプションをサポートする個々の証明書の目的で CSR を生成するときに、配布タイプを選択できます。CSR に必要な SAN エントリが自動的に入力され、デフォルトの SAN エントリが画面に表示されます。マルチサーバー CSR を生成すると、システムはその CSR をクラスタ内の必要なすべてのサーバーに自動的に配布します。同様に、マルチサーバー CA 署名付き証明書をアップロードすると、システムはその証明書をクラスタ内の必要なすべてのサーバーに自動的に配布します。
ステップ 2	サーバー上で CSR を生成します。	証明書署名要求を生成するを参照してください。
ステップ 3	CSR を PC にダウンロードします。	証明書署名要求をダウンロードするを参照してください。
ステップ 4	CSR を使用して、CA からアプリケーション証明書を取得します。	CA からのアプリケーション証明書の取得に関する情報を取得します。その他の注意事項については、 サードパーティの CA 証明書 を参照してください。
ステップ 5	CA ルート証明書を取得します。	CA からのルート証明書の取得に関する情報を取得します。その他の注意事項については、 サードパーティの CA 証明書 を参照してください。
ステップ 6	サーバーに CA ルート証明書をアップロードします。	信頼できる証明書をアップロードするを参照してください。

	タスク	関連情報
ステップ 7	アプリケーション証明書をサーバーにアップロードします。	アプリケーション証明書をアップロードするを参照してください。
ステップ 8	新しい証明書の影響を受けるサービスを再起動します。	すべての証明書タイプについて、対応するサービスを再起動します。 • Tomcat 証明書を更新する場合は、Cisco tomcat サービス、Connection IMAP サーバー、Cisco Dirsync サービス、Connection Jetty サービス、SMTP サービス、および Connection Conversation Manager サービスを再起動する必要があります。 • Tomcat-ECDSA 証明書を更新する場合は、Connection Conversation Manager サービスも再起動する必要があります。 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。

証明書署名要求を生成する

証明書署名要求を生成するには、次の手順に従います。

ステップ 1 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 証明書の一覧をフィルタするには、検索コントロールを使用します。

ステップ 3 **[CSRの生成（Generate CSR）]** をクリックすると、[証明書署名要求の生成（Generate Certificate Signing Request）] ダイアログボックスが開きます。

ステップ 4 [証明書の目的（Certificate Purpose）] のドロップダウン リスト ボックスから、必要な証明書の目的を選択します。

ステップ 5 [配信（Distribution）] ドロップダウン リスト ボックスから、必要な配信リスト項目を選択します。

（注） [マルチサーバー（SAN）（Multi-server (SAN)）] オプションは、[証明書の目的（Certificate Purpose）] ドロップダウン リスト ボックスから tomcat または tomcat-ECDSA を選択した場合にのみ使用できます。**[CSR の生成（Generate CSR）]** をクリックします。

デフォルトでは、システムは [CN] フィールドにサーバーの FQDN（またはホスト名）を入力します。必要に応じて値を変更できます。自己署名証明書の場合、CN は設定できません。

ステップ 6 マルチサーバー（SAN）の場合、[サブジェクト代替名（Subject Alternate Names）] フィールドにドメインを追加できます。

ステップ 7 [キー長（Key Length）] ドロップダウン リスト ボックスから、証明書の目的に応じて値を選択します。

- tomcat または ipsec が証明書の目的である場合は、1024、2048、3072、または 4096 を選択します。
- tomcat-ECDSA が証明書の目的である場合は、256、384、または 521 を選択します。

ステップ 8 [ハッシュアルゴリズム（Hash Algorithm）] ドロップダウン リスト ボックスから、証明書の目的に応じてを選択します。

- tomcat または ipsec が証明書の目的である場合は、SHA1 または SHA256 を選択します。
- tomcat-ECDSA が証明書の目的である場合は、SHA384 SHA512 を選択します。

ステップ 9 [Generate（生成）] をクリックして新しい CSR を生成します。

（注） 特定の証明書タイプに対して生成された新しい CSR は、そのタイプの既存の CSR を上書きします。CSR は、クラスタ内の必要なすべてのサーバーに自動的に配布されます。

証明書署名要求をダウンロードする

証明書署名要求をダウンロードするには、次の手順に従います。

ステップ 1 **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 リストから、タイプが「CSRのみ」のエントリの共通名をクリックし、共通名に一致する分布値をクリックします。

（注） マルチサーバー SAN 証明書の場合は、タイプが「CSRのみ」で、分布値が「マルチサーバー（SAN）」のエントリの共通名をクリックします。

[CSR 詳細（CSR Details）] ウィンドウが表示されます。

ステップ 3 **[CSR のダウンロード（Download CSR）]** をクリックします。

ステップ 4 CSR のダウンロードが完了したら、[閉じる（Close）] をクリックします。

クラスタ内のパブリッシャとサブスクライバの両方でマルチサーバー SAN 証明書を設定した後、tomcat サービスを再起動する必要があります。以下の手順を参照してください。

ステップ 1 SSH アプリケーションを使用して Unity Connection サーバーにサインインします。

ステップ 2 次の CLI コマンドを実行して、Tomcat サービスを再起動します。
utils service restart Cisco Tomcat

サードパーティの CA 証明書

サードパーティ 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か、アプリケーション証明書と CA 証明書の両方を含む PKCS#7 証明書チェーン（DER 形式）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。プロセスは CA によって異なります。

Cisco Unified Operating System Administration は、PEM エンコーディング形式で CSR を生成します。システムは、DER および PEM エンコード形式の証明書と、PEM 形式の PKCS#7 証明書チェーンを受け入れます。すべての証明書タイプについて、各ノードで CA ルート証明書とアプリケーション証明書を取得し、アップロードする必要があります。

Cisco Unified Operating System Administration CSR には、CA からのアプリケーション証明書のリクエストに含める必要のある拡張子が含まれています。CA が拡張要求メカニズムをサポートしていない場合は、次の手順に従って X.509 拡張を有効にする必要があります。

```
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment, Data Encipherment
```

（注） 使用する証明書に対して証明書署名要求（CSR）を生成し、SHA256 署名を使用してサードパーティ CA に署名させることもできます。そして、この署名された証明書を Cisco Unified Operating System Administration にアップロードし直すことで、Tomcat やその他の証明書が SHA256 をサポートできるようになります。

信頼できる証明書をアップロードする

信頼証明書をアップロードするには、以下の手順に従います。

ステップ 1 **[セキュリティ（Security）] > [証明書管理（Certificate Management）]**の順に選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 **[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）]** 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 **[証明書の用途（Certificate Purpose）]** ドロップダウンリストで、証明書名を選択します。

ステップ 4 **[説明（Description）]** 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。

ステップ 5 アップロードするファイルを選択し、**[参照（Browse）]** ボタンをクリックしてファイルに移動します。次に、**[開く（Open）]** をクリックします。

ステップ 6 ファイルをサーバーにアップロードするには、**[アップロード（Upload）]** をクリックします。

（注） 信頼証明書の場合、システムは証明書をクラスタの他のノードに自動的に配布します。

アプリケーション証明書をアップロードする

Cisco Unified Communications オペレーティングシステムは、サードパーティ CA が PKCS # 10 証明書署名要求（CSR）で発行する証明書をサポートします。

ステップ 1 サーバー上で CSR を生成します。

ステップ 2 CSR を PC にダウンロードします。

ステップ 3 CSR を使用して、CA または PKCS#7 形式の証明書チェーンからアプリケーション証明書を取得します。これには、CA 証明書とともにアプリケーション証明書が含まれている場合があります。

ステップ 4 CA 証明書または証明書チェーンを入手します。

tomcat アプリケーション証明書をアップロードするには、[証明書の目的（Certificate Purpose）] リストから **[Tomcat]** を選択します。

ipsec アプリケーション証明書をアップロードするには、[証明書の目的（Certificate Purpose）] リストから **[ipsec]** を選択します。

tomcat-ECDSA アプリケーション証明書をアップロードするには、[証明書の目的（Certificate Purpose）] リストから **[tomcat-ECDSA]** を選択します。

ステップ 5 **[証明書の用途（Certificate Purpose）]** ドロップダウンリストで、証明書を選択します。

ステップ 6 アップロードするファイルを選択し、**[参照（Browse）]** ボタンをクリックしてファイルに移動します。次に、**[開く（Open）]** をクリックします。

ステップ 7 ファイルをサーバーにアップロードするには、**[アップロード（Upload）]** をクリックします。

（注） システムは、アプリケーション証明書を他のクラスタノードに自動的に配布しません。複数のノードで同じ証明書を使用する必要がある場合は、各ノードに証明書を個別にアップロードする必要があります。ただし、SAN 証明書の場合、システムは証明書を他のクラスタノードに自動的に配布します。

証明書の失効日をモニターする

証明書の有効期限が近づくと、システムが自動的に電子メールを送信することができます。証明書の有効期限モニターを表示および設定するには、次の手順を実行します。

ステップ 1 現在の証明書有効期限モニターの設定を表示するには、**[セキュリティ（Security）]** > **[証明書モニター（Certificate Monitor）]** に移動します。

[証明書モニター（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。[証明書モニターの有効期限（Certificate Monitor Expiration）] フィールドの説明については、表 11 : 証明書有効期限モニターフィールド（表）証明書モニターのフィールド説明 を参照してください。

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

表 *11* : 証明書モニターのフィールド説明

フィールド	説明
通知開始時刻（Notification Start Time）	証明書の有効期限が切れ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）	通知の頻度を時間または日単位で入力します。
電子メール通知の有効化（Enable E-mail Notification）	電子メール通知を有効にするには、このチェックボックスをオンにします。
電子メール ID（Email IDs）	通知を送信する電子メールアドレスを入力します。 （注） システムが通知を送信するには、SMTP ホストを設定する必要があります。

証明書の失効

オンライン証明書ステータスプロトコル（OCSP）を使用して、証明書の失効ステータスを取得できます。

OCSP を設定するには、次の手順を実行します。

ステップ 1 **[セキュリティ（Security）]** > **[証明書管理（Certificate Management）]**の順に選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 [オンライン証明書ステータスプロトコル設定（Online Certificate Status Protocol Configuration）] 領域の [OCSP の有効化（Enable OCSP）] チェックボックスをオンにします。

ステップ 3 OCSP レスポンダに接続するために使用される OCSP URI を使用して証明書が設定されている場合は、[証明書の OCSP URI を使用（Use OCSP URI from Certificate）] を選択します。

ステップ 4 外部または設定済みの URI が OCSP レスポンダに接続するために使用される場合は、[設定済みの OCSP URI を使用（Use configured OCSP URI）] を選択します。[OCSP の設定済み URI（OCSP Configured URI）] フィールドに、証明書失効ステータスを確認する OCSP レスポンダの URI を入力します。

ステップ 5 失効チェックを実行する場合、[失効チェックの有効化（Enable Revocation Check）] チェック ボックスをオンにします。

（注） 証明書失効サービスは、失効および有効期限チェック エンタープライズ パラメータが有効に設定されている場合に、LDAP 接続と IPSec 接続に使用できます。

ステップ 6 証明書失効ステータス チェックの頻度を設定する場合に、[チェック間隔（Check Every）] の値を入力します。

- 失効ステータスを時間単位または日単位でチェックする場合に、[時間（Hours）] または [日（Days）] をクリックします。

ステップ 7 [保存（Save）]をクリックします。

警告 OCSP を有効にする前に、tomcat-trust に OCSP レスポンダ証明書をアップロードする必要があります。

（注） 証明書の失効ステータスの確認は、証明書または証明書チェーンのアップロード中にのみ実行され、証明書が失効した場合、適切なアラームが発生します。

証明書を確実に失効させるには、Cisco Certificate Expiry Monitor サービスを再起動する必要があります。[Cisco Unified Serviceability] > [ツール（Tool）] > [コントロールセンター - ネットワークサービス（Control Center - Network Services）] に移動し、Cisco Certificate Expiry Monitor サービスを再起動します。

IPSEC 証明書を再作成する

スタンドアロンまたはクラスタで ipsec 証明書を生成または再生成するには、次の手順を実行します。

ステップ 1 **[セキュリティ（Security）] > [証明書管理（Certificate Management）]** の順に選択します。

[証明書一覧（Certificate List）] ウィンドウが表示されます。

ステップ 2 **[Generate Self-signed（自己署名付きの生成）]** > または > **[CSRの生成（Generate CSR）]** をクリックします。

[証明書の生成（Generate Certificate）] ダイアログボックスが表示されます。

ステップ 3 **[証明書の目的（Certificate Purpose）]** ドロップダウンリストから [ipsec] を選択する。

ステップ 4 **[生成（Generate）]** をクリックします。

証明書の生成後、ipsec および ipsec trust は、スタンドアロンサーバーまたはパブリッシャサーバーの証明書で更新されます。

ステップ 5 サブスクライバサーバーの場合は、ステップ 1 ～ 4 に従って ipsec 証明書を生成します。生成後、サブスクライバサーバーから ipsec 証明書をダウンロードします。

ステップ 6 サブスクライバサーバーで、**[セキュリティ（Security）] > [証明書管理（Certificate Management）]** の順に選択します。

ステップ 7 **[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）]** 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 8 **[証明書の目的（Certificate Purpose）]** ドロップダウンリストから [ipsec-trust] を選択する。

ステップ 9 証明書を参照し、**[アップロード（Upload）]** をクリックします。

ステップ 10 ipsec 証明書をサブスクライバサーバーにアップロードした後、最初にパブリッシャサーバーで、次にサブスクライバサーバーで以下のサービスを再起動します。

- Cisco DRF Master
- Cisco DRF Local

IPSEC 管理

ここでは、IPSec メニューで実行できる機能について説明します。

（注） IPSec は、インストール中にクラスタ内のノード間で自動的に設定されません。

新しい IPSec ポリシーを設定する

新しい IPSec ポリシーと関連付けを設定するには、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 ポリシーに加えた変更は失われるため、アップグレード中に 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、特に暗号化において、システムのパフォーマンスに影響を与えます。

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

[IPSEC ポリシーリスト（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。このウィンドウのフィールドの説明については、 表 12 : IPSecポリシーフィールド（表）IPSEC ポリシーとアソシエーションのフィールド説明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 *12 : 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
ポリシーグループ名（Policy Group Name）	IPSec グループポリシーの名前を指定します。名前に指定できるのは、文字、数字、ハイフンのみです。
ポリシー名（Policy Name）	IPSec ポリシーの名前を指定します。名前に指定できるのは、文字、数字、ハイフンのみです。
認証方式（Authentication Method）	認証方式を指定します。
事前共有キー（Preshared Key）	[認証名（Authentication Name）] フィールドで [事前共有キー（Preshared Key）] を選択した場合は、事前共有キーを指定します。 （注） 事前共有 IPSec キーには、英数字とハイフンのみを使用できます。スペースやその他の文字は使用できません。Windows ベースのバージョンの Cisco Unified Communications Manager から移行する場合は、現在のバージョンの Cisco Unified Communications Manager と互換性があるように、事前共有 IPSec キーの名前を変更する必要がある場合があります。
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。
接続先アドレス（Destination Address）	接続先の IP アドレスまたは FQDN を指定します。
接続先ポート（Destination Port）	接続先のポート番号を指定します。
接続元アドレス（Source Address）	接続元の IP アドレスまたは FQDN を指定します。
接続元ポート（Source Port）	接続元のポート番号を指定します。
モード（Mode）	トランスポートモードを指定します。
リモートポート（Remote Port）	接続先で使用するポート番号を指定します。

フィールド	説明
プロトコル（Protocol）	特定のプロトコル、または以下のいずれかを指定します。 • TCP • UDP • 任意
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。次のオプションがあります。 • 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。 • 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。次のオプションがあります。 • NULL_ENC • DES • 3DES • BLOWFISH • RIJNDAEL
フェーズ 1 ライフタイム（Phase One Life Time）	フェーズ 1 の 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 DH（Phase One DH）	ドロップダウンリストから、[フェーズ 1 DH（Phase One DH）] 値を選択します。選択肢は、2、1、および 5 です。
フェーズ 2 ライフタイム（Phase Two Life Time）	フェーズ 2 の 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 DH（Phase Two DH）	ドロップダウンリストから、[フェーズ 2 DH（Phase Two DH）] 値を選択します。選択肢は、2、1、および 5 です。

フィールド	説明
ポリシーの有効化（Enable Policy）	WPA ポリシーを有効にするには、このチェックボックスをオンにします。

既存の IPSec ポリシーを管理する

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 ポリシーに加えられた変更は失われるため、アップグレード中に 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、特に暗号化において、システムのパフォーマンスに影響を与えます。

注意 既存の IPSec ポリシーに変更を加えると、通常のシステム動作に影響を与える可能性があります。

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 ポリシーリスト（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 ポリシー設定（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オンまたはオフにします。

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) 削除したいポリシーの横のチェックボックスをオンにします。

[すべてを選択（Select All）] をクリックするとすべてのポリシーを選択でき、**[すべてをクリア（Clear All）]** を選択するとすべてのチェックボックスをクリアできます。

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

証明書の一括管理

Extension Mobility Cross Cluster（EMCC）機能をサポートするために、システムでは、クラスタ管理者が設定した共通の SFTP サーバーとの間で一括インポートおよびエクスポート操作を実行できます。証明書の一括管理の使用方法の詳細については、『*Cisco Unified Communications Manager* セキュリティガイド』を参照してください。

証明書の一括管理の場合は、次の手順を実行します。

ステップ 1 **[セキュリティ（Security）]** > **[証明書の一括管理（Bulk Certificate Management）]** を選択します。[証明書の一括管理（Bulk Certificate Management）] ウィンドウが表示されます。

ステップ 2 [証明書の一括管理（Bulk Certificate Management）] ウィンドウで適切な情報を入力します。このウィンドウのフィールドの説明については、表 13 : 証明書の一括管理のフィールド説明を参照してください。

ステップ 3 入力した値を保存するには、**[保存（Save）]** をクリックします。

ステップ 4 証明書をエクスポートするには、**[エクスポート（Export）]** をクリックします。[証明書の一括エクスポート（Bulk Certificate Export）] ポップアップウィンドウが表示されます。

ステップ 5 ドロップダウンメニューから、エクスポートする証明書のタイプを選択します。

- Tomcat
- TFTP
- すべて

ステップ 6 **[エクスポート（Export）]** をクリックします。

選択した証明書がエクスポートされ、中央の SFTP サーバーに保存されます。

表 *13* : 証明書の一括管理のフィールド説明

フィールド	説明
IPアドレス（IP Address）	証明書をエクスポートする共通サーバーの IP アドレスを入力します。
ポート（Port）	ポート番号を入力します。 デフォルト：22
ユーザー ID（User ID）	サーバーへのログインに使用するユーザー ID を入力します。
パスワード（Password）	適切なパスワードを入力します。
ディレクトリ（Directory）	証明書を保存するサーバー上のディレクトリを入力します。 例：/users/cisco

セッション管理

プラットフォーム管理者は、Cisco Unity Connection の次の Web インターフェイスについて、ユーザーまたは管理者のアクティブな Web セッションを終了できます。

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Personal Communications Assistant
- Cisco Unity Connection Web Inbox
- Cisco Unity Connection SRSV

ユーザーまたは管理者のアクティブな Web セッションを終了するには、次の手順を実行します。

ステップ 1 **[セキュリティ（Security）] > [セッション管理（Session Management）]** に移動します。[セッション管理（Session Management）] ウィンドウが表示されます。

ステップ 2 [セッション管理（Session Management）] ウィンドウで、アクティブなログインユーザーのエイリアスを **[ユーザー ID（User ID）]** フィールドに入力します。

ステップ 3 ユーザーのアクティブな Web セッションを終了するには、**[セッションの終了（Terminate Session）]** を選択します。

（注） クラスタの場合は、クラスタの各ノードの Web セッションを終了する必要があります。

（注） セッションの終了は、プラットフォームユーザーには適用されません。アクティブな Web セッションを終了するには、プラットフォームユーザーはセッションをログアウトするか、セッションがタイムアウトするまで待機する必要があります。

暗号管理

Cisco Unity Connection は、管理者がすべての TLS および SSH 接続に使用される暗号のセットを制御できる**暗号管理**をサポートしています。Cisco Unity Connection のさまざまなセキュアインターフェイスの推奨暗号を設定できます。

TLS インターフェイス

以下で説明する TLS インターフェイスの暗号を設定できます。

インターフェイス	説明
All TLS	サポートされている Cisco Unity Connection のすべての TLS インターフェイスの暗号を設定できます。例：SIP、SCCP、HTTPS、Jetty、SMTP、LDAP、および IMAP インターフェイス。
HTTPS TLS	Cisco Unity Connection のすべての Cisco Tomcat インターフェイスの暗号を設定できます。
SIP TLS	Cisco Unity Connection の SIP インターフェイスの暗号を設定できます。例：Unity Connection でセキュアな SIP コールをサポートするテレフォニーユーザーインターフェイス。 （注） SIP インターフェイスの暗号設定は、Cisco Unity Connection の無制限バージョンではサポートされていません。

SSH インターフェイス

次に示す SSH インターフェイスの暗号とアルゴリズムを設定できます。

インターフェイス	説明
SSH 暗号	Cisco Unity Connection の SSH インターフェイスの暗号を設定できます。
SSH キー交換	Cisco Unity Connection の SSH インターフェイスの SSH キー交換アルゴリズムを設定できます。
SSH MAC	Cisco Unity Connection の SSH インターフェイスの SSH MAC アルゴリズムを設定できます。

推奨される暗号についての詳細は、https://www.cisco.com/c/ja_jp/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager* セキュリティガイド』の「暗号管理」の項を参照してください。

暗号ストリングを設定する

TLS および SSH インターフェースの暗号文字列を設定するには、以下の手順を実行します。

ステップ 1 **[セキュリティ（Security）]** > **[暗号管理（Cipher Management]** に移動します。[暗号の管理（Cipher Management）] ページが表示されます。

ステップ 2 [暗号管理（Cipher Management）] ページで、**すべての TLS** 、**HTTPS TLS**、および **SIP TLS** インターフェイスの **[暗号文字列（Cipher String）]** フィールドに暗号文字列を入力します。

（注） **HTTPS TLS** または **SIP TLS** インターフェイス用に設定された暗号文字列は、[すべての TLS（ALL TLS）] フィールドで設定された暗号文字列を上書きします。

（注） **[暗号管理（Cipher Management）]** ページで設定された暗号は、**[一般設定の編集（Edit General Configuration）]** ページの暗号設定を上書きします。したがって、TLS および HTTPS インターフェイスの暗号を設定するには、**[暗号管理（Cipher Management）]** ページを使用することをお勧めします。

ステップ 3 [SSH 暗号（SSH Ciphers）] の **[暗号文字列（Cipher String）]** フィールドに暗号文字列を入力します。

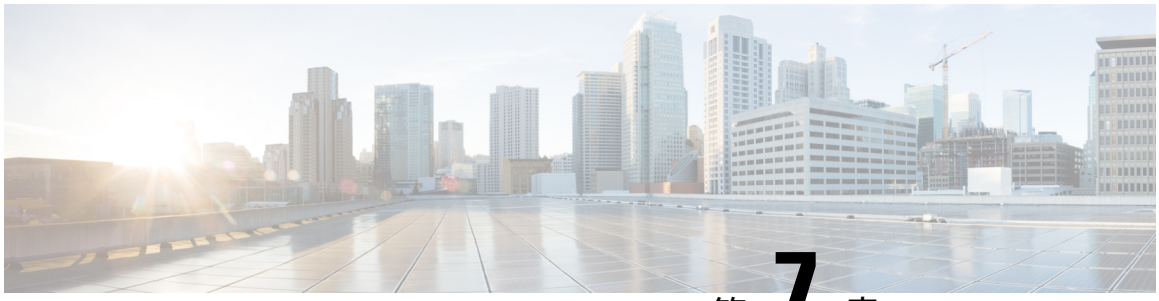
ステップ 4 **[暗号文字列（Algorithm String）]** フィールドにアルゴリズム文字列を入力し、SSH キー交換のキーアルゴリズムを設定します。

ステップ 5 **[暗号文字列（Algorithm String）]** フィールドにアルゴリズム文字列を入力し、SSH MAC の MAC アルゴリズムを設定します。

ステップ 6 **[保存（Save）]** を選択します。

ページを保存したら、次の手順を実行する必要があります。

- **すべての TLS**、**SSH 暗号**、**SSH キー交換** 、および **SSH MAC** インターフェイスで暗号を正常に設定するには、クラスタ内の両方のノードを再起動します。
- **HTTPS TLS** インターフェイスで暗号を正常に設定するには、Cisco Tomcat サービスを再起動します。
- **SIP TLS** インターフェイスで暗号を正常に設定するには、Connection Conversation Manager サービスを再起動します。



第 7 章

ソフトウェアのアップグレード

Cisco Unity Connection の出荷バージョンへのアップグレードについては、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html にある『*Cisco Unity Connection* のインストール、アップグレード、およびメンテナンスガイド、リリース*15*』の「Cisco Unity Connection のアップグレード」の章を参照してください。

Cisco Unity Connection の言語のインストールについては、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html にある『*Cisco Unity Connection* のインストール、アップグレード、およびメンテナンスガイド、リリース*15*』の「Cisco Unity Connection サーバーのメンテナンス」の章を参照してください。

- ソフトウェアのインストールおよびアップグレード （51 ページ）
- デバイスロード管理 （54 ページ）
- カスタムログインメッセージを設定する （54 ページ）
- Unity Connection のブランディングのカスタマイズ （55 ページ）

ソフトウェアのインストールおよびアップグレード

ソフトウェアアップグレードオプションを使用すると、オペレーティングシステムで実行中のソフトウェアバージョンをアップグレードしたり、Cisco Unified Communications オペレーティングシステムのロケールインストーラー、ダイヤルプラン、TFTPサーバーファイルなど、特定のソフトウェアオプションをインストールしたりできます。

[インストール/アップグレード（Install/Upgrade）] メニューオプションで、ローカルディスクまたはリモートサーバーからシステムソフトウェアをアップグレードできます。アップグレードしたソフトウェアは非アクティブなパーティションにインストールされ、その後でシステムの再起動とパーティションの切り替えができます。これにより、システムで新しいソフトウェアバージョンが実行されます。

（注） すべてのソフトウェアのインストールとアップグレードは、Cisco Unified Communications オペレーティングシステムのGUIとコマンドラインインターフェイスに含まれるソフトウェアアップグレード機能を使用して行う必要があります。このシステムでアップロードおよび処理できるソフトウェアは、シスコによって承認されたものだけです。以前のバージョンのCisco Unified Communications Managerで使用していたサードパーティ製またはWindowsベースのソフトウェアアプリケーションをインストールまたは使用することはできません。

Cisco Unity Connection をアップグレードするには、次の手順を実行します。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[ソフトウェアのアップグレード（Software Upgrades）] > [インストール/アップグレード（Install/Upgrade）]** に移動します。

[ソフトウェアのインストール/アップグレード（Software Installation/Upgrade）] ページが表示されます。

ステップ 2 Unity Connection をアップグレードするには、 ページで次の設定を行います。

フィールド	説明
パブリッシャからダウンロードクレデンシャルを使用（Use download credentials from Publisher）	（サブスクライバサーバーにのみ適用） パブリッシャサーバー用に提供されたソース設定を使用するには、このチェックボックスをオンにします。 チェックボックスがオンになっていない場合は、アップグレードプロセスのすべての設定を指定する必要があります。 デフォルトでは、このチェックボックスはオンになっています。
送信元（Source）	ドロップダウンメニューから該当するオプションを選択します。 • **DVD/CD**：ディスクドライブからアップグレードするには、このオプションを選択します • **リモートファイルシステム（Remote Filesystem）**：リモートサーバーからアップグレードするには、このオプションを選択します。 • **ローカルファイルシステム（Local Filesystem）**：以前にダウンロードしたISOまたはCOPファイルをアップグレードに使用するには、このオプションを選択します。
ディレクトリ（Directory）	（リモートファイルシステムに適用）アップグレードファイルを含むフォルダのパスを入力します。

フィールド	説明
サーバー（Server）	（リモートファイルシステムに適用） サーバー名または IP アドレスを入力します。
ユーザー名（User Name）	（リモートファイルシステムに適用） リモートサーバーへのサインインに使用するエイリアスを入力します。
ユーザーパスワード（User Password）	（リモートファイルシステムに適用） リモートサーバーへのサインインに使用するパスワードを入力します。
転送プロトコル（Transfer Protocol）	（リモートファイルシステムに適用） SFTP または FTP のいずれかの適切な転送プロトコルを選択します。
SMTP サーバー（SMTP Server）	SMTP サーバーの IP アドレスを入力します。
電子メールの接続先（Email Destination）	電子メールアドレスと SMTP サーバーを入力します。
ダウンロード後にアップグレードを続行（Continue with Upgrade after Download） [1]	ファイルのダウンロードが完了したらすぐにアップグレードを開始し、インストールを開始するには、このチェックボックスをオンにします。チェックサムと SHA の詳細は表示されません。 デフォルトでは、このチェックボックスはオンになっています。
アップグレード後にサーバーのバージョンを切り替える（Switch-Version Server after Upgrade） [1]	チェックボックスをオンにして、アップグレードが正常に完了した後にシステムを自動的に再起動します。 デフォルトでは、このチェックボックスはオフになっています。

[1] このフィールドは、Cisco Unity Connection には適用されません。

Cisco Unity Connection のアップグレードについては、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg/b_15cuciumg_chapter_0100.html にある『*Cisco Unity Connection* のインストール、アップグレード、およびメンテナンスガイド、リリース*15*』の「Cisco Unity Connection のアップグレード」の章を参照してください。

デバイスロード管理

デバイスの負荷管理の詳細については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/install_upgrade/guide/b_15cuciumg.html にある『*Cisco Unity Connection* インストール、アップグレード、およびメンテナンスガイド、リリース *15*』を参照してください。

カスタムログインメッセージを設定する

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。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウで、**[ソフトウェアのアップグレード（Software Upgrades）]** > **[ログインメッセージのカスタマイズ（Customized Logon Message）]** を選択します。

[ログインメッセージのカスタマイズ（Customized Logon Message）] ウィンドウが表示されます。

ステップ 2 **[参照（Browse）]** をクリックして、表示するログオンメッセージを含むテキストファイル（.txt）を選択します。

ステップ 3 **[ファイルのアップロード（Upload File）]** をクリックします。

カスタマイズされたログオン メッセージは、Unity Connection の次のインターフェイスのログイン画面とホーム画面に表示されます。

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Operating System Administration
- Cisco Unified Serviceability
- Disaster Recovery System Administration
- Cisco Prime License Manager
- Cisco Personal Communication Assistant
- Real-Time Monitoring Tool
- コマンドライン インターフェイス

（注） アップロードできるファイルは 10kB 以内です。

ステップ 4 （オプション）**[ユーザー確認応答が必要（Require User Acknowledgment）]** チェックボックスをオンにして、ユーザーが Web Inbox とともに上記のインターフェイスにアクセスするたびに、ポップアップウィンドウにもカスタマイズされたログオンメッセージを表示します。インターフェイスに正常にログインするには、**[OK]** をクリックしてポップアップウィンドウを明示的に確認する必要があります。

（注） Web Inbox の場合、カスタマイズされたログオンメッセージはポップアップウィンドウにのみ表示されます。

ステップ 5 デフォルトのログイン メッセージに戻すには、**[削除（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。

Unity Connection のブランディングのカスタマイズ

Cisco Unity Connection では、組織の要件に基づいて Unity Connection Web アプリケーションの外観を変更できる**ブランディングのカスタマイズ**機能がサポートされています。この機能により、オペレーティングシステム管理者は、Unity Connection Web アプリケーションの会社のロゴ、背景色、境界線の色、およびフォントの色をカスタマイズできます。 **ブランディング**は、Unity Connection の次の Web アプリケーションに適用できます。

- Cisco Unity Connection Administration
- Cisco Personal Communications Assistant
- Web Inbox

（注） Web Inbox では、会社のロゴのみを変更できます。

ブランディング設定の前提条件

Unity Connection でブランディングを設定するには、指定したフォルダ、サブフォルダ、およびその他のイメージファイルを含む branding.zip ファイルが必要です。Unity Connection には、Unity Connection Web アプリケーションのブランド変更を可能にする branding.zip テンプレートも用意されています。

branding.zip ファイルの構造の詳細については、「ブランディングファイルの構造 （60 ページ）」を参照してください。

Unity Connection でブランディングを設定するためのタスクリスト

Unity Connection でブランディング機能を設定するには、次の手順を実行します。

1. （オプション）`file get install branding.zip` CLI コマンドを実行して、branding.zip テンプレートファイルをリモートサーバーにコピーします。ファイルをリモートサーバーにコピーした後、組織の要件に従ってファイルを変更し、branding.zip として保存できます。ブランディング カスタマイズ オプションとそれらを変更する手順については、「ユーザーインターフェイスのブランディングオプション （56 ページ）」を参照してください。

   CLI コマンドについての詳細は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『シスコ ユニファイド コミュニケーション ソリューションのコマンドライン インターフェイス リファレンス ガイド』を参照してください。

2. Cisco Unified Communications Operating System Administration ページにログインし、**[ソフトウェアのアップグレード（Software Upgrades）]** > **[ブランディング（Branding）]** と進みます。[ブランディング（Branding）] ページで、**[ファイルの選択（Choose File）]** を選択してリモートサーバーから branding.zip ファイルを参照し、**[ファイルのアップロード（Upload File）]** を選択します。
3. ファイルが正常にアップロードされたら、**[ブランディングの有効化（Enable Branding）]** を選択します。

   カスタマイズされたブランディングを無効にするには、[ブランディング（Branding）]ページで **[ブランディングの無効化（Disable Branding）]** を選択します。

（注） ブランディングを有効または無効にするには、`utils branding enable/disable` CLIコマンドを実行することもできます。

CLI についての詳細は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『シスコ ユニファイド コミュニケーション ソリューションのコマンドライン インターフェイス ガイド』を参照してください。

4. Tomcat サービスを再起動して、Cisco Unity Connection Web アプリケーションのブランディングの更新を反映します。

（注） クラスタの場合は、クラスタの各ノードでブランディングを有効または無効にする必要があります。

ユーザーインターフェイスのブランディングオプション

次の図は、Unity Connection の Web アプリケーションの 1 つ（例：Cisco Unity Connection Administration）のブランディング カスタマイズ オプションを示しています。

図 *1 : Cisco Unity Connection Administration* ログイン画面のブランディング オプション

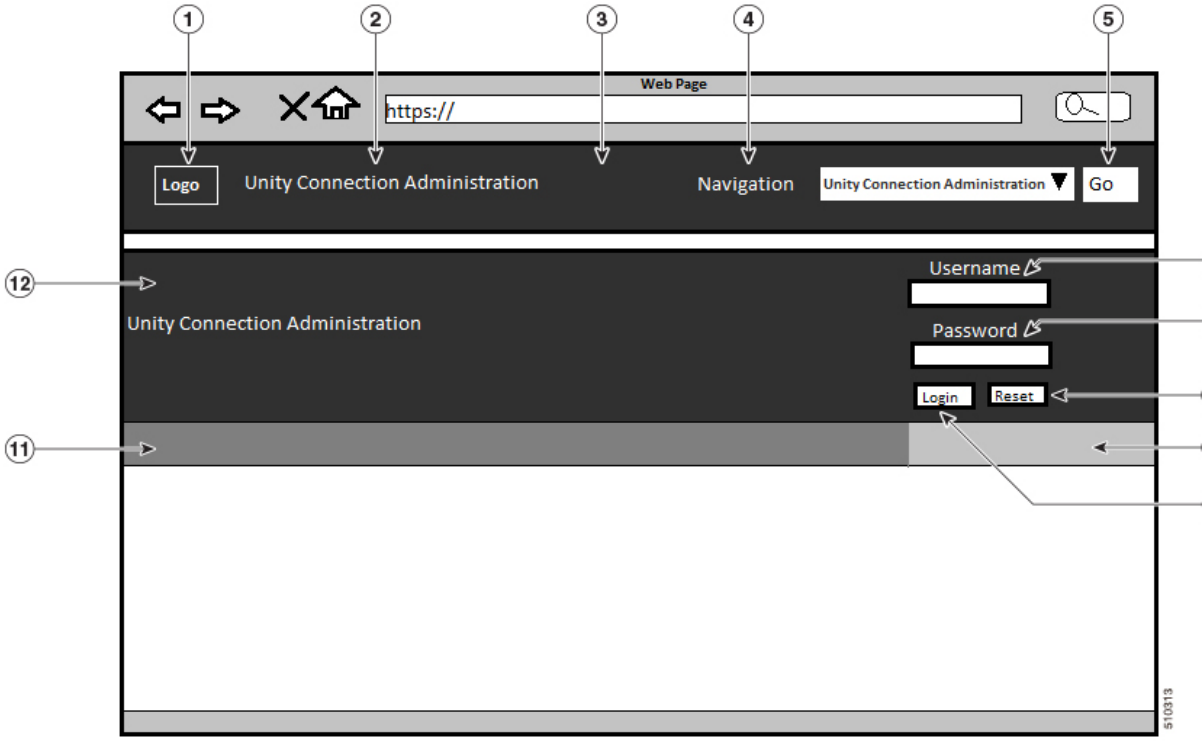
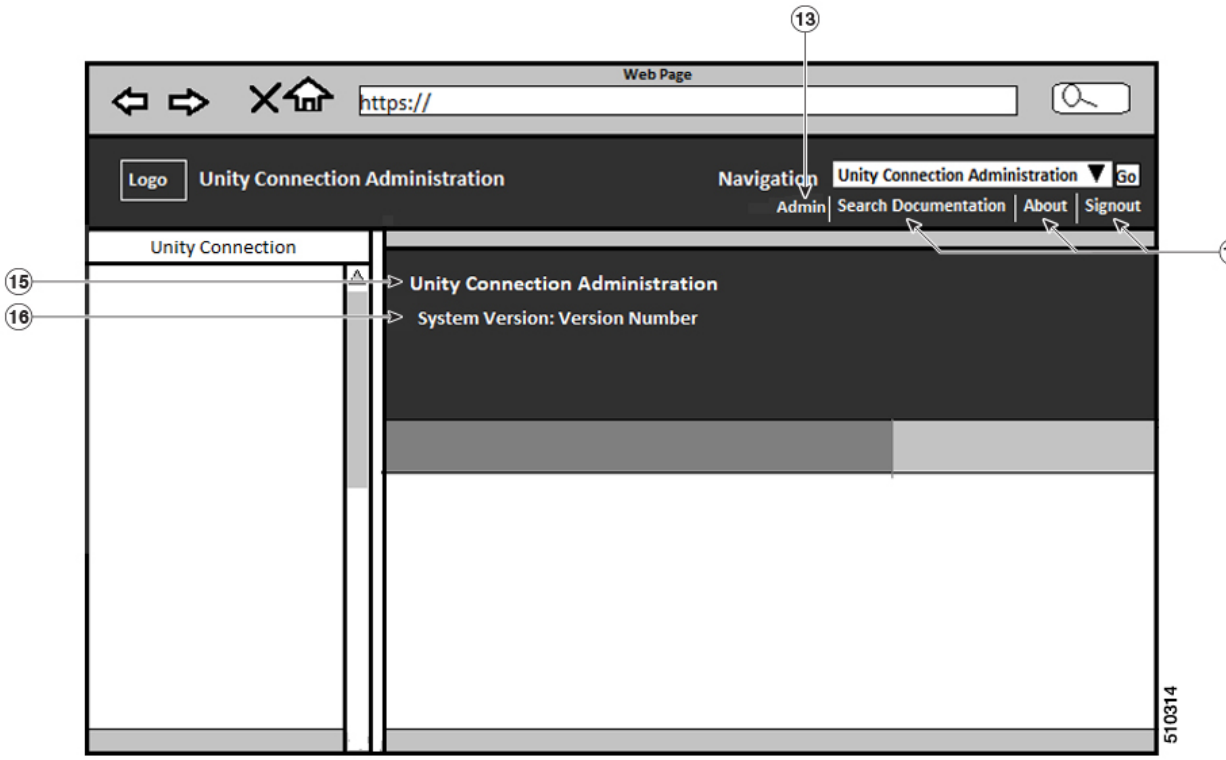


図 *2 : Cisco Unity Connection Administration* ログイン画面のブランディング オプション



以下の表は、変更可能な項目についての説明です。

項目	説明	ブランディングの編集

1	企業ロゴ	Cisco Unified Communications Manager にロゴを追加するには、会社のロゴを次のファイル名で 44x44 ピクセルイメージとして保存します。
		`ciscoLogo12pxMargin.gif`
		（44*44 ピクセル）
		（注） Web Inbox と Mini Inbox にロゴを追加するには、会社のロゴを 44*25 ピクセルの画像として以下のファイル名で保存します。
		`branding_logo.png`

2	Cisco Unity Connection Administration ヘッダーフォントの色	heading.heading.color

項目	説明	ブランディングの編集
3	ヘッダーの背景	1 つの画像を使用するか、または 6 つの画像の組み合わせを使用してグレーディング効果を作成できます。 **シングルイメージオプション**：単一のイメージとして、ヘッダー背景を保存します。 • brandingHeader.gif（652*1 ピクセル） **グレーディング バックグラウンド オプション**：グレーディング効果を得るために6つのイメージとしてヘッダー背景を保存します。 • brandingHeaderBegLTR.gif（652*1 ピクセル） • brandingHeaderBegRTL.gif（652*1 ピクセル） • brandingHeaderEndLTR.gif（652*1 ピクセル） • brandingHeaderEndRTL.gif（652*1 ピクセル） • brandingHeaderMidLTR.gif（652*1 ピクセル） • brandingHeaderMidRTL.gif（652*1 ピクセル）
4	ナビゲーション テキスト	header.navigation.color
5	[移動（Go）]ボタン	header.go.font.color header.go.background.color header.go.border.color
6	ユーザー名テキスト	splash.username.color
7	パスワードのテキスト	splash.password.color
8	リセット ボタン	splash.reset.text.color splash.reset.back.ground.color
9	背景下の色：右側	splash.hexcode.3
10	ログインボタン	splash.login.text.color splash.login.back.ground.color
11	背景下の色：左側	splash.hex.code.2
12	バナー	splash.hex.code.1
13	ユーザーテキスト（たとえば、「admin」）	header.admin.color

項目	説明	ブランディングの編集
18	ドキュメント、バージョン情報、およびサインアウトテキストの検索	header.hover.link.color
15	Unity Connection Administration テキスト見出し	splash.header.color
16	システムバージョンテキスト	splash.version.color

ブランディングファイルの構造

このセクションでは、branding.zip テンプレートに含まれるフォルダ、サブフォルダ、およびその他のファイルの構造について説明します。ヘッダーに単一のイメージを使用するか、またはヘッダー用のグレーディング効果を得るために6つのイメージの組み合わせを使用するかに応じて、フォルダー構造には 2 つのオプションがあります。

ブランディングオプション	フォルダ構造
単一ヘッダーオプション	ヘッダーの背景（吹き出し項目 3）に 1 つのイメージが必要な場合は、ブランディングフォルダに次のサブフォルダとイメージファイルが含まれている必要があります。 Branding (folder) ccmadmin (folder) BrandingProperties.properties (properties file) brandingHeader.gif (652*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image) branding_logo.png (44*25 pixel image)

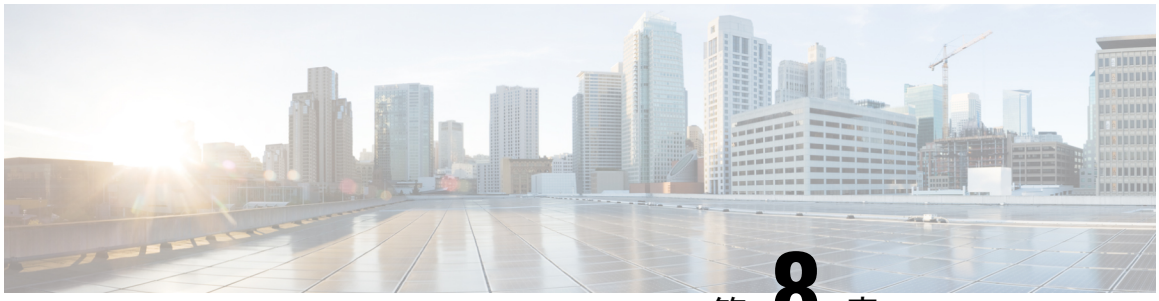
ブランディングオプション	フォルダ構造
グレーディング ヘッダー オプション	ヘッダーの背景用にグレーディングイメージを作成する場合は、グレーディング効果を得るために 6 つの個別のイメージファイルが必要です。ブランディングフォルダには、これらのサブフォルダとファイルが含まれている必要があります。 Branding(folder) ccmadmin (folder) BrandingProperties.properties (file) brandingHeaderBegLTR.gif (652*1 pixel image) brandingHeaderBegRTL.gif (652*1 pixel image) brandingHeaderEndLTR.gif (652*1 pixel image) brandingHeaderEndRTL.gif (652*1 pixel image) brandingHeaderMidLTR.gif (652*1 pixel image) brandingHeaderMidRTL.gif (652*1 pixel image) ciscoLogo12pxMargin.gif (44*44 pixel image) branding_logo.png (44*25 pixel image)

ブランディングプロパティの編集例

ブランディング プロパティは、プロパティファイル（BrandingProperties.properties）に 16 進コードを追加することで編集できます。プロパティファイルは HTML ベースの 16 進コードを使用します。たとえば、ナビゲーション テキスト項目（吹き出し項目 #4）の色を赤に変更する場合は、プロパティファイルに次のコードを追加します。

```
header.navigation.color="#FF0000"
```

このコードで、header.navigation.color は編集するブランディングプロパティで、"#FF0000" は新しい設定（赤）です。



第 8 章

サービス

• サービス （63 ページ）

サービス

概要

この章では、オペレーティング システムで使用可能なユーティリティ機能について説明します。これには、別のシステムへの ping やリモート サポートの設定が含まれます。

ping

[Ping ユーティリティ（Ping Utility）] ウィンドウでは、ネットワーク内の別のサーバーに ping を実行できます。

別のシステムに ping を実行するには、次の手順を実行します。

ステップ 1 [Cisco Unified Communications Operating System Administration] ウィンドウから **[サービス（Services）]** > **[Ping]** に移動します。

[Ping リモート（Ping Remote）] ウィンドウが表示されます。

ステップ 2 ping を実行するシステムの 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 間隔を秒単位で入力します。

ステップ 4 パケットサイズを入力します。

ステップ 5 ping カウント（システムに ping を実行する回数）を入力します。

（注） 複数の ping を指定した場合、ping コマンドは ping の日時をリアルタイムで表示しません。Ping コマンドは、指定した回数の ping が完了した後にデータを表示することに注意してください。

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 リモート（Ping Remote）] ウィンドウに ping の統計情報が表示されます。

リモートサポートを設定する

[リモートアカウントサポート（Remote Account Support）] ウィンドウから、シスコのサポート担当者が指定された時間システムにアクセスするために使用できるリモートアカウントを設定できます。

リモートサポートプロセスは次のように動作します。

ステップ 1 顧客は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時間の制限が含まれています。この時間制限は、さまざまな値に設定できます。

ステップ 2 リモートサポートアカウントが設定されると、パスフレーズが生成されます。

ステップ 3 お客様はシスコサポートに電話し、リモートサポートのアカウント名とパスフレーズを提供します。

ステップ 4 シスコサポートは、パスフレーズからパスワードを生成するデコーダプログラムにパスフレーズを入力します。

ステップ 5 シスコサポートは、デコードされたパスワードを使用してお客様のシステムのリモートサポートアカウントにログインします。

ステップ 6 アカウントの期限が切れると、シスコサポート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。

ステップ 7 [Cisco Unified Communications Operating System Administration] ウィンドウから **[サービス（Services）]** > **[リモートサポート（Remote Support）]** に移動します。

[リモートアクセス設定（Remote Access Configuration）] ウィンドウが表示されます。

ステップ 8 **[アカウント名（Account Name）]** フィールドに、リモートアカウントの名前を入力します。

アカウント名は、6 文字以上の英小文字で構成する必要があります。

ステップ 9 **[アカウントの有効期限（Account Duration）]** フィールドに、アカウント有効期限を日数で入力します。

デフォルトのアカウント期間は 30 日です。

ステップ 10 **[保存（Save）]** をクリックします。

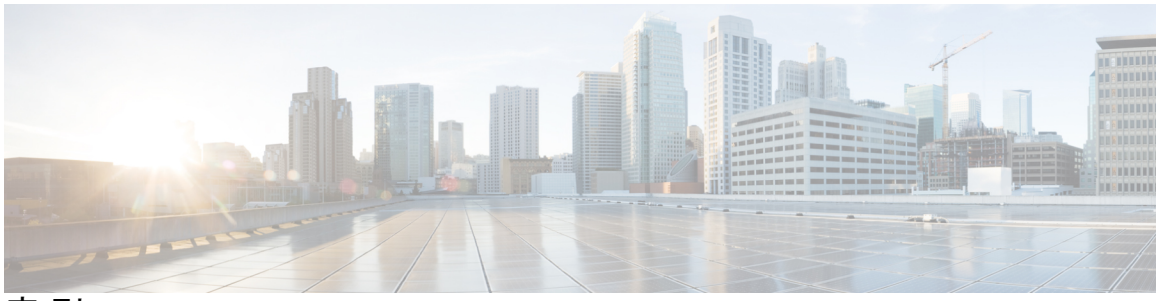
[リモートサポートステータス（Remote Support Status）] ウィンドウが表示されます。[リモートサポートステータス（Remote Support Status）] ウィンドウのフィールドの説明については、表 14: リモートサポートステータスフィールド（表）リモートサポートステータスのフィールドと説明を参照してください。

ステップ 11 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には、シスコの担当者にお問い合わせください。

ステップ 12 リモート アクセス サポート アカウントを削除するには、**[削除（Delete）]** ボタンをクリックします。

表 *14 :* リモートサポートステータスのフィールドと説明

フィールド	説明
複合化バージョン（Decode version）	使用中のデコーダのバージョンを示します。
アカウント名（Account name）	リモートサポートアカウントの名前を表示します。
有効期間（Expiration）	リモートアカウントへのアクセスが期限切れになる日時を表示します。
パスフレーズ（Pass phrase）	生成されたパスフレーズを表示します。



索 引

I

IPSec 43–44, 46
　新しいポリシーの設定 43
　ポリシーの表示 46
　ポリシーの変更 46
　ポリシーフィールド（表） 44

い

インストールしたソフトウェア 15
　フィールド（表） 15

お

オペレーティング システム 1, 7
　概要 1
　ログイン 7
オペレーティングシステム 12–13
　ネットワーク ステータス フィールド（表） 13
　ハードウェアステータス 12
　　フィールド（表） 12

く

クラスタノード 11
　フィールド（表） 11

さ

サービス 64
　リモートサポート 64
　　概要 64
　　セットアップ 64

し

システム 15, 28
　シャットダウン 28
　ステータス 15
　　フィールド（表） 15
シャットダウン、オペレーティングシステム 28
証明書 32, 38, 41
　再作成 32
　削除 32
　署名要求のダウンロード 38
　ダウンロード 32
　表示 32
　有効期限モニターフィールド（表） 41

す

ステータス 12–13, 15
　システム 15
　　フィールド（表） 15
　ネットワーク 13
　　フィールド（表） 13
　ハードウェア 12
　　フィールド（表） 12

せ

設定 20
　イーサネット 20
　　フィールド（表） 20

そ

ソフトウェア 15
　インストール 15
　　フィールド（表） 15

ね

ネットワークステータス 13
　フィールド（表） 13

の

ノード、クラスタ 11
　フィールド（表） 11

は

ハードウェア、ステータス 12
フィールド（表） 12

り

リモートサポート 64–65
ステータスフィールド（表） 65
リモートサポート *(続き)*
セットアップ 64

ろ

ログイン 7
概要 7

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。