Cisco IME サーバのインストールと設定

この章では、Cisco Intercompany Media Engine サーバのインストールと設定について説明します。インストール手順を開始する前に、インストールについての指示すべてをよく確認してください。

- システム要件，1 ページ
- よくある質問，2 ページ
- インストール前の設定の実施，5 ページ
- インストール ウィザードのナビゲーション，17 ページ
- インストールの開始，18 ページ
- インストール後の設定の実施，21 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，28 ページ
- Cisco IME のアップグレード，29 ページ
- トラブルシューティング，31 ページ

システム要件

インストールを進める前に、次の要求事項と推奨事項について考慮してください。

- Cisco Unified Communications Manager サーバで、Cisco Unified Communications Manager ソフトウェアの互換性のあるバージョンが実行されていることを確認します。 次の URL にある『Cisco Unified Communications Manager Software Compatibility Matrix』を参照してください：

  http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html。

- Cisco Unified Communications Manager サーバで NTP が有効になっていることを確認します。NTP ステータスを確認するには、Cisco Unified Communications Manager コマンドライン インターフェイスにログインし、`utils ntp status` と入力します。

- 既存のサーバにインストールする場合、ハードドライブはフォーマットされ、ドライブ上に存在するデータすべてが上書きされることに注意します。
- バックアップ電源によってシステムを保護できるよう、サーバが無停電電源装置（UPS）に接続されていることを確認します。このようにしなかった場合、物理メディアに損傷が生じて Cisco Intercompany Media Engine（Cisco IME）の新規インストールが必要となる可能性があります。

  Cisco IME ノードで UPS シグナリングを自動的にモニタし、電源喪失時にグレースフル シャットダウンを自動で開始させるには、特定の UPS とサーバ モデルの使用が必要です。 サポートされるモデルと構成の詳細については、『Release Notes for Cisco Intercompany Media Engine』を参照してください。
- スタティック IP アドレスを使用してサーバを設定し、サーバが固定された IP アドレスを得られるようにします。
- インストール中、このサーバで DNS を有効にし、NTP を設定する必要があります。
- インストール中は、設定作業を実行しないでください。
- インストールが完了するまで、シスコで検証済みのアプリケーションをインストールしないでください。
- サーバ モデル 7825 I3（160 GB SATA ディスク ドライブ）のディスク ミラーリングには、約 3 時間かかります。
- インストールを進める前に、次の情報を注意深く読んでください。

よくある質問

インストール

インストールにはどのくらい時間がかかりますか。

サーバ タイプによりますが、インストール前後の作業を除いたインストール プロセス全体で 20 ～ 30 分必要です。

どのユーザ名およびパスワードを設定する必要がありますか。

インストール中、次のユーザ名とパスワードを指定する必要があります。

- 管理者アカウントのユーザ名とパスワード

  次の領域へのログインには、管理者アカウントのユーザ名とパスワードを使用します。

  - ディザスタ リカバリ システム
  - コマンドライン インターフェイス

  管理者アカウントのユーザ名とパスワードを指定するには、次のガイドラインに従います。

  - 管理者アカウントのユーザ名： 管理者アカウントのユーザ名には、英数字、ハイフン、アンダースコアを使用できますが、先頭は英字にします。
  - 管理者アカウントのパスワード： 管理者アカウントのパスワードは、最低 6 文字とし、英数字、ハイフン、アンダースコアを使用できます。

  コマンドラインインターフェイスを使用して、管理者アカウント パスワードの変更や新規管理者アカウントの追加が行えます。 詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

- セキュリティ パスワード

  セキュリティ パスワードは最低 6 文字とします。英数字、ハイフン、アンダースコアを使用できます。

強度の高いパスワードとはどのようなパスワードですか。

インストール ウィザードは、入力されたパスワードの強度をチェックします。 強度の高いパスワードを作成するには、次の推奨事項に従います。

- 大文字と小文字を混在させる。
- 英字と数字を混在させる。
- ハイフンやアンダースコアを含める。
- 短いパスワードよりも長いパスワードの方が強度が高く安全である。

次のようなパスワードの使用は避けます。

- 固有名詞や辞書にある単語など、認識可能な単語は使用しない（数字と組み合わせた場合も含む）。
- 認識可能な単語を反転させたものは使用しない。
- aaabbb、qwerty、zyxwvuts、123321 のようにパターン化された単語や数字は使用しない。
- 他の言語で認識可能な単語は使用しない。
- いかなるものにしろ、誕生日、郵便番号、子供やペットの名前のような個人情報は使用しない。

Cisco Unified Communications アンサー ファイル ジェネレータとは何ですか。

Cisco Unified Communications アンサー ファイル ジェネレータは、Cisco Intercompany Media Engine の無人インストールのアンサー ファイルを生成する Web アプリケーションです。 個別のアンサー ファイルが USB キーまたはフロッピーディスクのルート ディレクトリにコピーされ、Cisco Intercompany Media Engine DVD と共にインストール処理中に使用されます。

この Web アプリケーションは次のサポートと情報を提供します。

- データ エントリの構文検証
- オンライン ヘルプと資料
- 新規インストールのサポート（アップグレードはサポートしません）

Cisco Unified Communications Answer File Generator は、次の URL でアクセスできます。

http://www.cisco.com/web/cuc_afg/index.html

Cisco Unified Communications アンサー ファイル ジェネレータは、Internet Explorer バージョン 6.0 以降および Mozilla バージョン 1.5 以降をサポートしています。

Linux 2.4 対応の USB キーを使用してください。 設定ファイル用に、Linux 2.4 互換であらかじめフォーマットされている USB キーの使用を推奨します。 これらのキーは W95 FAT32 フォーマットを使用します。

どのようなサーバがサポートされますか。

サポートされているサーバ モデルについては、ご使用の製品リリースのリリース ノートを参照してください。

どの SFTP サーバがサポートされますか。

どのような SFTP サーバ製品でも使用できますが、シスコでは Cisco Technology Developer Partner（CTDP）プログラムでシスコが認定した SFTP 製品を推奨します。 GlobalSCAPE などの CTDP パートナーは、自社製品での特定のバージョンの Cisco Unified Communications Manager の使用を保証しています。

サポートされている Cisco Unified Communications バージョンの GlobalSCAPE での使用については、次の URL を参照してください。

http://www.globalscape.com/gsftps/cisco.aspx

シスコでは、次のサーバを内部テストに使用しています。 これらのサーバのいずれかを使用できますが、サポートについてはベンダーに問い合わせてください。

- Open SSH（http://sshwindows.sourceforge.net/ を参照）
- Cygwin（http://www.cygwin.com/ を参照）
- Titan（http://www.titanftp.com/ を参照）

CTDP プロセスによる認証を受けていないサードパーティ製品に関連する問題のサポートについては、サードパーティ ベンダーにお問い合わせください。

サーバに他のソフトウェアをインストールできますか。

ソフトウェアのインストールとアップグレードは、すべてコマンドライン インターフェイス（CLI）で行う必要があります。 システムがアップロードして処理できるのは、シスコが承認したソフトウェアだけです。 未承認のサードパーティ ソフトウェア アプリケーションのインストールや実行はできません。

インストール前の設定の実施

Cisco Intercompany Media Engine を確実にインストールするために、次に示すインストール前の作業を行います。

手順

ステップ 1 このマニュアル全体をよく読み、インストール手順についてよく理解します。

ステップ 2 シスコは、Cisco IME のサイト分析と計画のセッションを完了しておくことを推奨します。これには、オフパス適応型セキュリティアプライアンス（ASA）の設定、IP アドレッシング、ピンホール、スタティック ネットワーク アドレス変換（NAT）、非武装地帯（DMZ）の設定が含まれま

す。 現在のネットワーク設定に適用される Cisco IME 要求事項について理解しておく必要があります。
『Cisco Unified Communications SRND』

ステップ 3 企業のファイアウォールで、必要なトラフィックを有効にします。 Cisco Intercompany Media Engine の設計と導入の早い段階で、企業のファイアウォールや DMZ の管理チーム（IT チームや情報セキュリティ チームなど）と協力しておく必要があります。 Cisco IME コールの開始前に、企業のファイアウォールに必要なアクセスコントロールリスト（ACL）がすべて承認され、実装されているようにします。

ステップ 4 製造元が提供するユーティリティを実行して、すべての新規サーバ ハードウェアの整合性を検証します（ハード ドライブやメモリなど）。

ステップ 5 新規サーバを接続するスイッチ ポートのネットワーク インターフェイス カード（NIC）の速度とデュプレックス設定を記録します。サーバとスイッチ ポートの NIC 設定を同じにする必要があります。 GigE（1000/FULL）の場合、NIC とスイッチ ポート設定は Auto/Auto にする必要があり、固定値は設定しません。
シスコ サーバに接続するスイッチポートすべてで PortFast を有効にします。 PortFast を有効にすると、転送遅延をなくすことによりスイッチはポートをブロック状態から転送状態へすぐに変更します（転送遅延は、スパニングツリー プロトコル（STP）ラーニングおよびリスニング ステートから転送ステートに変わるまでポートが待つ時間の長さを指します）。

ステップ 6 Cisco IME をインストール予定のサーバすべてが正しく DNS に登録されていることを確認します。 `GoDaddy.com` サーバと `intercompanymedianetwork.com` ブートストラップ サーバの解決と ping が実行できる必要があります。

ステップ 7 Cisco IME ライセンス ファイルを取得します。
ライセンス ファイルの取得, （10 ページ）を参照してください。

ステップ 8 インストール予定の各サーバの設定値を記録します。
設定値の記録については、サーバ設定データを参照してください。

企業および外部のファイアウォールの設定

この項では、IME トラフィックをサポートするために設定する必要がある、必要最低限のポートについて説明します。 「企業のファイアウォール設定」の表では、企業のファイアウォールに設定する必要があるポートの概要を示します。 「外部 Cisco IME ASA ファイアウォール」の表では、オフパス ASA に設定する必要があるポートの概要を示します。 これらの表中のポート設定は、デフォルト設定に基づいています。 デフォルト設定を変更した場合、これらの設定を更新する必要があります。

ご使用のネットワークに他のサーバ/ポートが必要な場合、そのトラフィックの許可も必要です。

表 *1*：企業ファイアウォール設定

インターフェイス	方向	ソース	宛先	プロトコル	ポート	説明
内側	インバウンド	Cisco Unified CM IP アドレス	オフパス ASA 内部シグナリングアドレス（物理アドレスと同じ）	TCP	8060	Cisco Unified CM と ASA シグナリング アドレスとのオフパス マッピング。 クラスタ内の各 Cisco Unified CM にエントリが必要。
内側	インバウンド	Cisco Unified CM IP アドレス	オフパス ASA 内部シグナリングアドレス（物理アドレスと同じ）	TCP	1024 ～ 65535	Cisco Unified CM と ASA シグナリング アドレスとのオフパス マッピング。 クラスタ内の各 Cisco Unified CM にエントリが必要。
DMZ	インバウンド	オフパス ASA 内部シグナリングアドレス（物理アドレスと同じ）	Cisco Unified CM IP アドレス	TCP	5060	ASA シグナリング アドレスと Cisco Unified CM との間の SIP シグナリング。 クラスタ内の各 Cisco Unified CM にエントリが必要。 ポート番号設定可能。
内側	インバウンド	Cisco Unified CM IP アドレス	Cisco IME サーバ DMZ IP アドレス	TCP	5620	Cisco IME と Cisco Unified Communications Manager との間の VAP 通信

インターフェイス	方向	ソース	宛先	プロトコル	ポート	説明
内側	インバウンド	ユニファイドコミュニケーション デバイスすべて（MeetingPlace、ボイスメール、ソフトクライアント IP 範囲、音声ゲートウェイなど、ASA 経由の通信が必要なすべてのメディアデバイスを含む）	オフパス ASA 内部メディアの終端 IP	UDP	16384 ～ 32767	UDP ポートは、Cisco IME が有効な ASA メディアの終端アドレス設定および同時コール数に基づいて制限可能です。
DMZ	インバウンド	オフパス ASA 内部メディアの終端 IP（送信元ポート範囲は Cisco IME 設定に基づいて制限可能です）	ユニファイド コミュニケーションデバイスすべて（MeetingPlace、ボイスメール、ソフトクライアント IP 範囲、音声ゲートウェイなど、ASA 経由の通信が必要なすべてのメディア デバイスを含む）	UDP	16384 ～ 32767	メディア トラフィックの UDP ポート
内側	インバウンド	内部ネットワークまたはいずれかの管理ワークステーション	Cisco IME サーバ DMZ IP アドレス	TCP	22	ライセンスやソフトウェアのアップロード、アップグレード、CLI アクセスのための Cisco IME サーバへの SFTP アクセス

インターフェイス	方向	ソース	宛先	プロトコル	ポート	説明
内側	インバウンド	内部ネットワークまたはいずれかの管理ワークステーション	Cisco IME サーバ DMZ IP アドレス	HTTPS	443	Cisco IME サーバからの RTMT ダウンロード
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	GoDaddy Web サイト	HTTPS	443	GoDaddy からの証明書ダウンロード
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	任意	TLS	6084	Cisco IME サーバからインターネットへのアウトバウンド IME 分散キャッシュ通信
外側	インバウンド	任意	Cisco IME サーバ DMZ IP アドレス	TLS	6084	インターネットから Cisco IME サーバへのインバウンド IME 分散キャッシュ通信
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	任意	TLS	8470	Cisco IME サーバからインターネットへのアウトバウンド IME 分散キャッシュ通信
外側	インバウンド	任意	Cisco IME サーバ DMZ IP アドレス	TLS	8470	インターネットから Cisco IME サーバへのインバウンド IME 分散キャッシュ通信

表 *2*：外部 ***Cisco IME ASA*** ファイアウォール（オフパス ***ASA***）

インターフェイス	方向	ソースの説明	宛先の説明	プロトコル	ポート	説明
DMZ	インバウンド	Cisco Unified CM IP アドレス	リモート Cisco Unified CM	TCP	5560 ～ 5590	リモート Cisco Unified CM への内部 Cisco Unified CM シグナリング（リモート PAT 設定）

インターフェイス	方向	ソースの説明	宛先の説明	プロトコル	ポート	説明
DMZ	インバウンド	Cisco Unified CM IP アドレス	リモート Cisco Unified CM	TCP	5060	リモート Cisco Unified CM への内部 Cisco Unified CM シグナリング（リモート PAT 設定）
外側	インバウンド	任意	Cisco Unified CM IP アドレス	TCP	5060	内部 Cisco Unified CM へのリモート Cisco Unified CM シグナリング

関連トピック

インストール前の設定の実施，（5 ページ）

ライセンス ファイルの取得

製品付属の製品認可キー（PAK）を使用して、Cisco IME サーバに必要なライセンスを取得できます。 ライセンス ファイルには、Cisco IME のサポートされているバージョン、Cisco IME サーバの MAC アドレス、ライセンスされた Cisco IME アプリケーション数（ピアカウント）、GoDaddy からの証明書取得に必要な情報（タグと署名）が含まれます。 証明書によって、Cisco IME サーバが IME 分散キャッシュ リング上にある他の Cisco IME サーバへの TLS 接続を確立できるようになります。

Cisco IME サーバのライセンス ファイルを取得するには、次の手順に従います。

手順

ステップ 1 Cisco Intercompany Media Engine の注文に付属の製品認証キー（PAK）を、http://www.cisco.com/go/license の License Registration Web ツールに入力します。

ステップ 2 [送信(Submit)] をクリックします。

ステップ 3 システム プロンプトの指示に従います。 Cisco Intercompany Media Engine をインストール予定のサーバのネットワーク インターフェイス カード（NIC）の MAC アドレスと、有効な電子メール アドレスを入力する必要があります。 MAC アドレスを知るには、Cisco IME コマンドライン インターフェイス（CLI）にログインし、show status と入力します。 [ライセンスMAC(License MAC)] フィールドに MAC アドレスが表示されます。
入力した電子メール アドレス宛てに電子メールでライセンス ファイルが送信されます。

ライセンス ファイルの形式は、`IME<timestamp>.lic` です。 `.lic` 拡張子を保持していれば、ライセンスファイルの名前を変更することもできます。 ファイルの内容に何らかの編集を加えると、ライセンスは使用できなくなります。

ステップ 4 ステップ 3 で入力した MAC アドレスに一致するサーバに、ライセンス ファイルをアップロードします。
ライセンス ファイルのアップロード, （22 ページ）を参照してください。

ライセンス ファイルの例

次のコードは、Cisco IME ライセンス ファイルの例を示しています。

```
INCREMENT IME_SERVICE cisco 8.0 permanent uncounted \VENDOR_STRING=<ime>
<peercount>5</peercount><tag>163d18ab727c0fa14fce75c6651b1362</tag>
<signature>154fe09fdbb012407cbfac8c74c55cb6be460199c813b0af29b83bc3b10824519bef7427f7a
be7a7b9e6692e9b905e73fa9a1199c90ef7fd269c89f0a9179677bbee34cb1eeb915f03e2372cb1e9d272d
af907be0077c7fd128ecc0216f036bb9447f06857cdcb4b066e746dc80ebe33fc212117b5c6c95aa404751
6120e403c320f703a9a94ac7c177a07963dd83aa79b75c1c585250481bce340ef3bf02f86633f245cbfaef
c2a1851b29c6cf48f580655c8a983b65d5584e316f350a15ff90478cbcb8e39128049edbb6972b33203130
00f28db28cc51a8eb7666a40184cb5389e216cdfeac7c1d42b0e4fdf2c608bea28faeff807fcc0862497dd
59ca676</signature></ime><LicFileVersion>1.0</LicFileVersion> \
HOSTID=00163569b2e0 \
NOTICE="<LicFileID>20090730162506350</LicFileID><LicLineID>1</LicLineID> \
<PAK></PAK>" SIGN="0288 1F4A 07D6 0C34 F35B D4D5 0339 C538 \
AC1E BC65 8697 9D5F 18D3 A57D 27DD 18D2 8C3B 14BA E72F 4932 \
E27D 7BE9 C410 5477 9B85 AAF7 2F42 8C44 0985 CFF1"
```

関連トピック

インストール前の設定の実施, （5 ページ）

サーバ設定データ

サーバ情報

一部のフィールドはオプションであり、ご使用の設定には適用されない場合があります。 表の一番右の列に、インストール後にフィールドを変更できるかどうかを示しています。また、変更可能な場合は、該当するコマンドライン インターフェイス（CLI）コマンドを記載しています。

注意 フィールドの一部はインストールが完了してしまうと、ソフトウェアを再インストールしない限り変更できなくなります。そのため、適切な値を入力するように注意してください。

表 *3*：サーバ設定データ

パラメータ	説明	エントリの変更可否
[管理者ID(Administrator ID)]	このフィールドは、Cisco Intercompany Media Engine サーバ上の CLI へのセキュア シェル アクセスに使用する管理者アカウントのユーザ ID を指定します。	インストール後はエントリを変更できません。 （注） インストール後に追加の管理者アカウントを作成することはできますが、元の管理者アカウントのユーザ ID は変更できません。
[管理者パスワード(Administrator Password)]	このフィールドは、CLI へのセキュア シェル アクセスに使用する管理者アカウントのパスワードを指定します。 このパスワードは、adminsftp ユーザでも使用します。adminsftp ユーザは、ローカル バックアップ ファイルへのアクセスやサーバ ライセンスのアップロードなどに使用します。 パスワードは最低 6 文字とし、英数字、ハイフン、アンダースコアを使用するようにします。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI>**set password admin**
[国(Country)]	リストから、インストール環境に応じて適切な国を選択します。 （注） 入力した値は、証明書署名要求（CSR）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI >**set web-security**
[DHCP]	シスコは、[DHCP] オプションに [いいえ(No)] を選択するよう要求します。 [いいえ(No)] を選択した後、ホスト名、IP アドレス、IP マスク、ゲートウェイを入力します。	インストール後にエントリを変更しないでください。

パラメータ	説明	エントリの変更可否
[DNS有効(DNS Enable)]	DNS サーバは、ホスト名を IP アドレスに、IPアドレスをホスト名に解決します。 Cisco IME では DNS サーバの使用が必須です。 [はい(Yes)] を選択して、DNS を有効にします。	インストール後にエントリを変更しないでください。
[DNSプライマリ(DNS Primary)]	プライマリ DNS サーバとして指定する DNS サーバの IP アドレスを入力します。 IP アドレスは、ドット付き 10 進表記（`ddd.ddd.ddd.ddd`）で入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network dns** DNS とネットワークの情報を参照するには、次の CLI コマンドを使用します。 CLI > **network eth0 detail**
[DNSセカンダリ(DNS Secondary)]	セカンダリ DNS サーバ（オプション）として指定する DNS サーバの IP アドレスを入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network dns**
[ゲートウェイアドレス(Gateway Address)]	ネットワーク ゲートウェイの IP アドレスを入力します。 ゲートウェイがない場合でも、このフィールドには 255.255.255.255 を設定する必要があります。 ゲートウェイがない場合、通信はご使用のサブネット上のデバイスだけに制限されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network gateway**
[ホスト名(Hostname)]	サーバの一意なホスト名を入力します。 ホスト名は最大 64 文字で、英数字とハイフンを使用できます。 ハイフンは先頭に使用できません。	インストール後にエントリを変更できます。 CLI > **set network hostname**

パラメータ	説明	エントリの変更可否
[IPアドレス(IP Address)]	ご使用のサーバの IP アドレスを入力します。	インストール後にエントリを変更できます。 CLI > **set network ip eth0** （注） ネットワーク耐障害性が有効になっている場合、IP アドレスの変更前に set network failover dis と入力して無効にする必要があります。 IP アドレス変更後、set network failover ena と入力してネットワーク耐障害性を再度有効にします。
[IPマスク(IP Mask)]	このマシンの IP サブネット マスクを入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network ip eth0**
[ロケーション(Location)]	サーバの場所を入力します。 システムは、サードパーティの証明書取得に使用する証明書署名要求（CSR）の生成にこの情報を使用します。 組織にとって意味のある任意の場所を入力できます。 たとえば、サーバの所在する都道府県や都市にします。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**

パラメータ	説明	エントリの変更可否
[MTUサイズ(MTU Size)]	最大伝送単位（MTU）は、ホストがネットワーク上で送信する最大のパケットをバイト単位で表します。 ご使用のネットワークの MTU サイズをバイト単位で入力します。 ネットワークのMTU設定がよくわからない場合、デフォルト値を使用します。 デフォルトでは 1500 バイトが指定されます。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set network mtu**
[NICデュプレックス(NIC Duplex)]	ネットワーク インターフェイス カード（NIC）のデュプレックス モードを Full と Half から選択します。 ネットワーク インターフェイス カード（NIC）のデュプレックス モードを Full と Half から選択します。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set network nic**
[NICスピード(NIC Speed)]	NICのスピードを、10メガビット毎秒と100メガビット毎秒から選択します。 このパラメータは、自動ネゴシエーションを使用しないよう選択した場合にだけ表示されます。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set network nic**

パラメータ	説明	エントリの変更可否
[NTPサーバ(NTP Server)]	同期に使用する1つ以上のネットワーク タイム プロトコル（NTP）サーバのホスト名またはIPアドレスを入力します。 NTPサーバは5つまで入力できます。 互換性、精度、およびネットワーク ジッターに関する潜在的な問題を回避するには、プライマリ ノードに指定した外部NTPサーバが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、外部NTPサーバはNTP v4である必要があります。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **utils ntp server**
[組織(Organization)]	組織の名前を入力します。 このフィールドを使用して、複数の組織ユニットを入力できます。 複数の組織ユニット名を入力するには、エントリをカンマで区切ります。 カンマを含むエントリの場合、エントリの一部に含まれるカンマの前にバックスラッシュを入力します。 入力した値は、証明書署名要求（CSR）の生成に使用されます。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[セキュリティパスワード(Security Password)]	パスワードは、最低6文字の英数字である必要があります。パスワードにはハイフンとアンダースコアを使用できますが、先頭に使用できるのは英数字だけです。 このパスワードを保存します。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set password security**

パラメータ	説明	エントリの変更可否
[都道府県(State)]	サーバの所在する都道府県を入力します。 入力した値は、証明書署名要求（CSR）の生成に使用されます。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[タイムゾーン(Time Zone)]	このフィールドは、現地タイムゾーンと、グリニッジ標準時（GMT）からの差を指定します。 マシンの所在地に適したタイムゾーンを選択します。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set timezone** 現在のタイム ゾーン設定を参照するには、次のCLIコマンドを入力します。 CLI > **show timezone config**
[ユニット(Unit)]	ユニットを入力します。 入力した値は、証明書署名要求（CSR）の生成に使用されます。	次のCLIコマンドを使用してインストール後にエントリを変更できます。 CLI > **set password admin**

インストール ウィザードのナビゲーション

表 *4* : ナビゲーションのオプションと操作

ナビゲーションのオプション	キーボード操作
次のフィールドへ移動	Tab
前のフィールドへ移動	Alt+Tab
オプションの選択	Space バーまたは Enter
リスト内のスクロール	↑または↓
前のウィンドウに戻る	Space バーまたは Enter を押し、[戻る(Back)] を選択（使用可能な場合）
ウィンドウについてのヘルプ表示	Space バーまたは Enter を押し、[ヘルプ(Help)] を選択（使用可能な場合）

関連トピック

インストール前の設定の実施, （5 ページ）

インストールの開始

（注） 新しいサーバにソフトウェアがプレインストールされている場合、新しい製品リリースを使用してそのサーバのイメージを再作成する場合以外は、DVD からインストールする必要はありません。

インストールを開始するには、次の手順に従います。

手順

ステップ 1 インストール DVD をトレイに入れてサーバを再起動し、DVD からサーバを起動します。
サーバの起動処理が完了すると、[DVDが見つかりました(DVD Found)] ウィンドウが表示されます。

ステップ 2 メディア チェックを実行する場合、[はい(Yes)] をクリックします。
すでにメディア チェックに合格している DVD の場合、メディア チェックのスキップを選択できます。
メディア チェックでは DVD の整合性がチェックされ、[メディアチェックの結果(Media Check Result)] ウィンドウが表示されます。

ステップ 3 [はい(Yes)] を選択した場合は、次のいずれかの作業を実行します。

- [メディアチェックの結果(Media Check Result)] で [合格(Pass)] と表示された場合は、[OK] をクリックしてインストールを続行します。
- メディアがメディア チェックに失敗した場合は、別のコピーを `Cisco.com` からダウンロードするか、別の DVD を直接シスコから入手します。

システムインストーラは次のハードウェアチェックを実行して、システムが正しく設定されていることを確認します。 インストーラがハードウェア設定に何らかの変更を加える場合、システムの再起動を求めるプロンプトが表示されます。 リブートの間も DVD はドライブに入れたままにしておいてください。

- 最初に、インストール プロセスは正しいドライバかどうかをチェックします。 次の警告が表示された場合は、[はい(Yes)] をクリックします。
「ハードドライブが見つかりません。(No hard drives have been found.) インストールを完了するには、デバイスドライバを手動で選択する必要があります。(You probably need to manually choose device drivers for install to succeed.) 今すぐドライバを選択しますか(Would you like to select drivers now?)」
- インストールでは次に、サポートされているハードウェアプラットフォームかどうかをチェックします。 サーバがハードウェア要件を厳密に満たしていない場合、インストール プロセ

スに重大なエラーが発生して失敗します。 この失敗が正常なものでないと思われる場合、エラーをキャプチャしてシスコ サポートに報告します。

- インストール プロセスは次に、RAID 設定と BIOS 設定を確認します。
  （注） この手順が繰り返された場合は、もう一度 [はい(Yes)] をクリックしてください。
- インストール プログラムで BIOS 更新が必要な場合、システムの再起動が必要なことが通知されます。 何かキーを押してインストールを継続します。
  ハードウェア チェックが完了すると、[製品展開の選択(Product Deployment Selection)] ウィンドウが表示されます。

ステップ 4 [OK] をクリックします。
ソフトウェアが現在サーバにインストールされている場合、[ハードドライブの上書き(Overwrite Hard Drive)] ウィンドウが表示され、ハード ドライブ上の現在のソフトウェアのバージョンと DVD 上のバージョンとが表示されます。 インストールを継続する場合 [はい(Yes)] を、キャンセルする場合 [いいえ(No)] をクリックします。

注意 [ハードドライブの上書き(Overwrite Hard Drive)] ウィンドウで [はい(Yes)] を選択すると、ハード ドライブにある既存のデータはすべて上書きされて消去されます。

[プラットフォームインストレーションウィザード(Platform Installation Wizard)] ウィンドウが表示されます。

ステップ 5 次のいずれかの作業を実行します。

- 設定情報を手動で入力し、設定済みのソフトウェアをインストールプログラムによってサーバにインストールする場合は、[続行(Proceed)] をクリックして、基本インストールを続行します。
- 次の作業のいずれかを行う場合は、[スキップ(Skip)] をクリックして続行します。
  - サーバにプリインストールされたソフトウェアを手動で設定： この場合、ソフトウェアのインストールは必要ありませんが、プリインストールされたソフトウェアの設定が必要です。
  - 無人インストールを実行： この場合、USB キーまたはフロッピーディスクに保存した既存の設定情報を使用します。
  - ソフトウェアをインストールしてから手動で設定： この場合、インストール プログラムがソフトウェアをインストールし、手動設定を求めるプロンプトが表示されます。 サーバにまずアプリケーションをプリインストールしておき、設定情報は後で入力する場合、[スキップ(Skip)] を選択します。 この方法は、他の方法より時間がかかる場合があります。

システムの再起動後、[既存のインストール設定(Preexisting Installation Configuration)] ウィンドウが表示されます。

ステップ 6 インストール プログラムの手順に従います。

ステップ 7 自動ネゴシエーションを有効にするか、無効にするかを指定します。

インストール プロセスでは、イーサネット ネットワーク インターフェイス カード（NIC）の速度とデュプレックスの設定を自動ネゴシエーションによって自動設定するように設定できます。この設定はインストール後に変更できます。

- 自動ネゴシエーションを有効にするには、[はい(Yes)] をクリックします。
  （注） このオプションを使用する場合、ハブまたはイーサネット スイッチが自動ネゴシエーションに対応している必要があります。
- 自動ネゴシエーションを無効にするには、[いいえ(No)] をクリックします。
  - NIC の適切な速度とデュプレックス設定を選択し、[OK] をクリックします。

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

ステップ 8 MTU サイズを変更します。
最大伝送単位（MTU）は、ホストがネットワーク上で送信する最大のパケットをバイト単位で表します。 ネットワークの MTU 設定がよくわからない場合、デフォルト値として指定されている 1500 バイトを使用します。

注意 MTU サイズの設定が不適切な場合、ネットワークのパフォーマンスが低下する場合があります。

- デフォルト値（1500 バイト）を使用する場合は、[いいえ(No)] をクリックします。
- MTU サイズをオペレーティング システムのデフォルトから変更する場合、[はい(Yes)] をクリックします。
  - 新しい MTU サイズを入力し、[OK] をクリックします。

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

ステップ 9 DHCP を選択するかどうか尋ねられたときは、[いいえ(No)] をクリックします。
シスコではダイナミック ホスト設定プロトコル（DHCP）ではなく、サーバにスタティックなネットワーク IP アドレスを設定することを要求しています。
[スタティックネットワーク設定(Static Network Configuration)] ウィンドウが表示されます。

ステップ 10 スタティックなネットワーク設定値を設定し、[OK] をクリックします。
[DNSクライアント設定(DNS Client Configuration)] ウィンドウが表示されます。

ステップ 11 [はい(Yes)] をクリックして、DNS を有効にします。
シスコは、DNS を有効にすることを要求します。

ステップ 12 DNS クライアント情報を入力し、[OK] をクリックします。
新しい設定情報を使用してネットワークが再起動します。[管理者ログイン設定(Administrator Login Configuration)] ウィンドウが表示されます。

ステップ 13 インストール プログラムの手順に従います。

ステップ 14 外部 NTP サーバを設定するか、システム時刻を手動設定するかを選択します。
シスコでは、正確なシステム時刻のため、外部 NTP サーバの使用を推奨します。 外部 NTP サーバがストラタム 9 以上まで識別できる（つまり、ストラタム 1 ～ 9 を含む）ことを確認します。

- 外部 NTP サーバをセットアップする場合、[はい(Yes)] をクリックします。

最低 1 つの NTP サーバの IP アドレス、NTP サーバ名または NTP サーバ プール名を入力します。 NTP サーバは 5 つまで設定できます。 シスコでは、最低 3 つの NTP サーバを設定することを推奨します。 [続行(Proceed)] をクリックしてインストールを継続します。

（注） [テスト(Test)] ボタンが表示された場合、[テスト(Test)] を選択して NTP サーバにアクセスできるかどうかを確認できます。

システムは NTP サーバと接続し、自動でハードウェア クロックに時刻を設定します。

- システム時刻を手動設定する場合、[いいえ(No)] をクリックします。
  ハードウェア クロックに設定する適切な日付と時刻を入力します。 [OK] をクリックしてインストールを継続します。

  [セキュリティ設定(Security Configuration)] ウィンドウが開きます。

ステップ 15 手順に従って、インストール プログラムを完了させます。

システムがソフトウェアのインストールと設定を行います。 DVD ドライブがイジェクトされ、サーバが再起動します。 DVD を再挿入しないでください。 インストールプロセスが完了すると、管理者アカウントとパスワードでログインするようプロンプトが表示されます。

次の作業

インストール後の設定の実施, （21 ページ）

インストール後の設定の実施

サーバにソフトウェアをインストールした後、以下のリストの手順に従い、インストール後の作業を実行する必要があります。

手順

ステップ 1 クライアント マシンにリアルタイム モニタリング ツールをインストールします。
リアルタイムモニタリングツールを使用して、システムの健全性のモニタや、ログの参照と収集が行えます。

リアルタイム モニタリング ツールのインストール手順と詳しい情報については、RTMT のインストールを参照してください。

ステップ 2 Cisco Intercompany Media Engine ライセンス ファイルをサーバにアップロードします。
ライセンス ファイルのアップロード, （22 ページ）を参照してください。

ステップ 3 Cisco Intercompany Media Engine 証明書を `GoDaddy.com` から取得します。
証明書の購入と登録, （23 ページ）および証明書の更新, （24 ページ）を参照してください。

ステップ 4 Cisco Unified Communications Manager と Cisco Intercompany Media Engine との間のセキュアな通信のために、自己署名証明書またはサードパーティの証明書にアクセスし、インストールします。
次の項を参照してください。

- 自己署名証明書の生成
- サードパーティ証明書の生成

ステップ 5 バックアップの設定を行います。
Cisco Intercompany Media Engine データは毎日バックアップするようにします。 ディザスタ リカバリ システムを参照してください。

ステップ 6 VAP サーバをセットアップします。
詳細については、VAP サーバのセットアップ, （25 ページ）を参照してください。

ステップ 7 Cisco IME サーバをセットアップします。
詳細については、IME サーバのセットアップ, （26 ページ）を参照してください。

ライセンス ファイルのアップロード

次の手順を実行して、ライセンス ファイルの申請時に入力した MAC アドレスを持つ Cisco IME サーバに、ライセンス ファイルをアップロードします。 ライセンス ファイルの取得については、ライセンス ファイルの取得, （10 ページ）を参照してください。

はじめる前に

サーバに Cisco IME サーバ ソフトウェアがインストールされていることを確認します。

手順

ステップ 1 Cisco IME ライセンス ファイル（.lic）を、ローカル ハード ドライブ上の一時ディレクトリに保存します。

ステップ 2 SFTP クライアントを開き、インストール中にセットアップした adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続します。

ステップ 3 cd license と入力してライセンス ディレクトリに移動し、このディレクトリにライセンス ファイルをコピーします。

ステップ 4 put `<license filename>` と入力します。ここで、`<license filename>` には電子メールで受け取ったライセンス ファイルの名前を指定します。

ステップ 5 Cisco IME コマンドライン インターフェイス（CLI）にログインして **utils ime** license file install `<license filename>` と入力し、Cisco IME ライセンスをアップロードします。

（注） 受信するライセンス ファイルの形式は、IME<タイムスタンプ>.lic です。 .lic 拡張子を保持していれば、ライセンス ファイルの名前を変更することもできます。 ファイルの内容に何らかの編集を加えると、ライセンスは使用できなくなります。

インストール後、サーバはライセンス ファイルを `/usr/local/ime/conf/licfiles` に保存します。 サーバはライセンス ログを `/active/cm/trace/ime/licensing/log4j` に保存します。

関連トピック

インストール後の設定の実施, （21 ページ）

証明書の購入と登録

IME 分散キャッシュ リングの証明書は、GoDaddy が提供します。 GoDaddy は、タグ、peerIDCount、署名など Cisco IME ライセンス内の情報を使用して各サーバを一意に識別し、証明書を生成します。

Cisco IME サーバ用の証明書は、GoDaddy の Web サイトで購入します。 証明書購入後、GoDaddy に証明書を登録します。 登録プロセスでは、証明書を取得できる有効なサーバがあることを示す情報を提供します。 証明書は購入日から 1 年間有効です。

Cisco IME サーバは、有効期限日付の前に証明書の更新を試みます。 自動登録に失敗した場合、サーバは EnrollFailure アラームを生成します。 この場合、証明書の手動更新が必要です。 証明書の更新の詳細については、証明書の更新, （24 ページ）を参照してください。

新規証明書の購入と登録は、次の手順に従います。

はじめる前に

ライセンスを Cisco IME サーバにインストールします。手順は、ライセンス ファイルのアップロード, （22 ページ）に説明されています。

手順

ステップ 1 http://www.godaddy.com に移動します。

ステップ 2 アカウント マネージャにログインします。

ステップ 3 [使用している製品(My Products)] セクションで、[SSL証明書(SSL Certificates)] をクリックします。

ステップ 4 Cisco IME サーバ用の証明書を購入します。

（注） 証明書購入の詳細については、GoDaddy の Web サイト上にある Cisco Intercompany Media Engine 証明書の要求とインストールについてのサポート トピック（http://help.godaddy.com/article/5414）を参照してください。

購入プロセスでは、ご使用のサーバのサーバ ID の入力が必要です。 この ID を入手するには、Cisco IME サーバの CLI にログインし、show ime certenrollment server ID と入力します。

ステップ 5 プロンプトが表示されたら、Cisco IME サーバ CLI に `utils ime certenrollment enroll` と入力して Cisco IME サーバに証明書をインストールします。

ステップ 6 登録に成功した場合、Cisco IME サーバは SuccessfulEnrollment アラートを生成します。失敗した場合、EnrollFailure アラートを生成します。

ステップ 7 Cisco IME サーバ上の証明書を表示するには、CLI に移動して `show cert own intercompanymedianetwork` と入力します。

（注） システムは、手動登録と自動登録のログ ファイルを、ディレクトリ `/active/platform/log/cli*.log` と `/active/platform/log/certm.log` にそれぞれ保存します。

関連トピック

インストール後の設定の実施，（21 ページ）

証明書の更新

次の手順で証明書を手動更新する必要があります。

手順

ステップ 1 http://www.godaddy.com に移動します。

ステップ 2 アカウント マネージャにログインします。

ステップ 3 [使用している製品(My Products)] セクションで、[SSL証明書(SSL Certificates)] を選択し、更新する証明書を探します。

（注） 証明書更新の詳細については、GoDaddy の Web サイト上にある Cisco Intercompany Media Engine 証明書の更新についてのサポート トピック（http://help.godaddy.com/article/5415）を参照してください。

ステップ 4 GoDaddy が支払を受領すると、次のいずれかのイベントが発生します。

- GoDaddy が以前の証明書の期限前に支払を受領した場合、証明書が更新され、それ以上の作業は必要ありません。
- GoDaddy が以前の証明書の期限後に支払を受領した場合、Cisco IME サーバ CLI で `utils ime certenrollment enroll` と入力します。

ステップ 5 登録に成功した場合、Cisco IME サーバは SuccessfulEnrollment アラートを生成します。失敗した場合、EnrollFailure アラートを生成します。

ステップ 6 Cisco IME サーバ上の証明書を表示するには、CLI に移動して `show cert own intercompanymedianetwork` と入力します。

（注） システムは、手動登録と自動登録のログ ファイルを、ディレクトリ `/active/platform/log/cli*.log` と `/active/platform/log/certm.log` にそれぞれ保存します。

関連トピック

インストール後の設定の実施，（21 ページ）

VAP サーバのセットアップ

この手順に記載されているコマンドのオプションについて詳しくは、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

VAP サーバをセットアップするには、次の手順を実行します。

手順

ステップ 1 Cisco IME CLI で、コマンド `add ime vapserver` を実行して VAP サーバの名前とポートを設定します。

VAP サーバの名前、ポート、認証モードの指定を求められます。 ここで入力する名前が、このインスタンスの固有識別子となります。 Cisco Unified Communications Manager の名前と一致させる必要はありません。 選択する認証モードは、Cisco Unified Communications Manager と一致させる必要があります（暗号化済または認証済）。

（注） 同じ Cisco IME サーバを使用する複数の Cisco Unified Communications Manager がある場合、各クラスタに VAP サーバ エントリを追加する必要があります。 各 VAP サーバ名に、一意のポート番号を指定してください。 1 つのインスタンスを認証済モード用、もう 1 つを暗号化済および認証済モード用にした、複数の VAP サーバ インスタンスを持つことができます。 これらのインスタンスは、異なるポートを使用する必要があります。

ステップ 2 コマンド `show ime vapserver all` を実行して、管理しているすべての VAP サーバを表示します。

ステップ 3 次のコマンドを実行して、設定した VAP サーバ インスタンスごとに必要なオプションを設定します。

（注） シスコでは、認証モードを暗号化済に設定することを強く推奨します。

- `set ime vapserver authenticationmode`
- `set ime vapserver enabled`
- `set ime vapserver keepaliveinterval`
- `set ime vapserver maxconnectionsallowed`
- `set ime vapserver port`

ステップ 4 コマンド `add ime vapusercredentials` を実行して、Cisco IME サーバの VAP ユーザ クレデンシャルを設定します。

入力するアプリケーションのユーザ名とパスワードは、Cisco Unified Communications Manager の管理ページでアプリケーション ユーザに入力したものと一致している必要があります。

チケットのパスワードと Epoch は、Cisco IME ASA で設定されたものと一致している必要があります。 シスコでは、最低 20 文字のパスワードを作成することを推奨します。

次の作業

Cisco IME サーバをセットアップした後に、サーバは IME 分散キャッシュに参加できるようになります。 詳細については、IME サーバのセットアップ, （26 ページ）を参照してください。

関連トピック

インストール後の設定の実施, （21 ページ）

IME サーバのセットアップ

Cisco IME サーバをセットアップするには、次の手順を実行します。

手順

ステップ 1 Cisco IME サーバに外部アドレスをセットアップします。
詳細については、IME サーバの外部アドレスのセットアップ, （27 ページ）を参照してください。

ステップ 2 次のコマンドを実行して、IME サーバのピア ID のリストとブートストラップ サーバの IP アドレスを表示します。

- `show ime peerid`
  ピア ID が表示されない場合、Cisco IME 証明書に問題がある可能性があります。 設定を継続する前に、この問題を修正する必要があります。
- `show ime bootstrap ip`
  最低 1 つの IP アドレスが表示されることを確認します。 IP アドレスがまったく表示されない場合、Cisco IME が DNS 経由でブートストラップ サーバに接続できないことを意味します。

ステップ 3 コマンド `show ime dht summary` を実行して、IME 分散キャッシュ上の IME サーバの状態を確認します。

例：

```
Peer ID = 514dd001c7553593ebefee2b076ad9d4
DHT Health........................ = GREEN
BootStrap: 5619e12c7a647e1d3364c8a46c9e58f7
Last Contact (sec)................. = 48
Current Sequence................... = 1250036323
Num. Tokens Received............... = 3
Delay from BootStrap............... = 1
Peer Count Distance................ = 5
```

DHT Health フィールドに、Peer ID フィールドのサーバのステータスが表示されます。 緑色は正常に動作している状態を示します。

ピア ID のステータスが緑色で表示されない場合、Cisco IME 証明書が正しくインストールされていることを確認し、Cisco IME ポートと Cisco IME 対応 ASA をチェックします。

show ime addressing コマンドを使用して、パブリック IP アドレスが正しく設定されたことを確認する必要がある場合もあります。

ステップ 4 コマンド `set ime customerinfo` を実行して、IME サーバにお客様連絡先情報を設定します。この情報はご使用の Cisco IME サーバ上に保存され、シスコ テクニカル サポートが Cisco IME サーバの設定ミスを検出した場合にお客様に連絡するときに使用されます。

お客様情報の設定後、`show ime customerinfo` コマンドで情報を表示できます。

次の情報を尋ねるプロンプトが表示されます。

- [会社名(Company Name)]：Cisco IME サーバを使用する企業の名前
- [ユニット名(Unit Name)]：企業内の部門（都市名や部署）
- [都道府県(State)]：サーバの位置する都道府県
- [国(Country)]：サーバの位置する国
- [サポート担当者名(Support Contact Name)]：ご使用の Cisco IME サーバでシスコが設定ミスを検出した場合に連絡する担当者
- [サポート電子メール(Support Contact Email)]：会社のサポート連絡先電子メール
- [サポート電話番号(Support Contact Phone)]：サポート連絡先電話番号

関連トピック

インストール後の設定の実施, （21 ページ）
VAP サーバのセットアップ, （25 ページ）

IME サーバの外部アドレスのセットアップ

Cisco IME サーバに外部アドレスを設定するには、次の手順を実行します。

手順

ステップ 1 Cisco IME CLI にログインし、コマンド `set ime addressing publicipaddrv4 external ip addr` を入力します。

例：
たとえば、Cisco IME のパブリック IP アドレスが 65.65.65.65 となる場合、`set ime addressing publicipaddrv4 65.65.65.65` と入力します。

ステップ 2 コマンド `show ime addressing` を入力して設定を確認します。

例：
次の例では、Cisco IME サーバのパブリック IP アドレスとプライベート IP アドレスが表示されています。

```
admin: show ime addressing
=====================================
Public IP Address = 65.65.65.65
Private IP Address = 10.10.10.10
DHT Port = 6084
Validator Port = 8470
=====================================
```

関連トピック

インストール後の設定の実施，（21 ページ）
IME サーバのセットアップ，（26 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

パスワードのリセットプロセス実行では、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、サーバにキーボードとモニタを接続する必要があります。 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、パスワードはリセットできません。

（注） この手順の間、システムに物理的にアクセスできることを証明するため、有効な CD または DVD をディスクドライブから取り出し、挿入することが必要になります。

手順

ステップ 1 次のユーザ名とパスワードでシステムにログインします。

- ユーザ名：pwrecovery
- パスワード：pwreset

[プラットフォームパスワードの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 何かキーを押して継続します。

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

ステップ 4 何かキーを押して継続します。
システムは、CD や DVD をディスク ドライブから取り出したことをテストで確認します。

ステップ 5 ディスク ドライブに有効な CD または DVD を挿入します。
（注） このテストでは、音楽 CD ではなくデータ CD を使用します。

システムはディスクが挿入されたことをテストで確認します。

ステップ 6 システムは、ディスクが挿入されたことを確認した後、次のオプションのいずれかを選択して継続するようプロンプトを表示します。

- 管理者パスワードをリセットするには、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には、s を入力します。
- 終了するには、q を入力します。

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。
パスワードは、6 文字以上である必要があります。 システムは新規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かった場合、新しいパスワードを入力するよう求められます。

ステップ 9 システムが新しいパスワードの強度を確認すると、パスワードがリセットされます。 何か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プロンプトが表示されます。

Cisco IME のアップグレード

アップグレード プロセスを開始する前に、Cisco.com から適切なアップグレード ファイルを入手しておく必要があります。

次の手順で、Cisco Intercompany Media Engine（Cisco IME）サーバ ソフトウェアをアップグレードします。

（注） Cisco IME をアップグレードする場合、Cisco Unified Communications Manager 上で Cisco IME サービスと通信するサービスは停止します。 この停止により、Cisco Unified Communications Manager は、アップグレードが完了し Cisco IME サーバが新しいリリースに切り替えられるまで一時的にルートの学習を停止します。 この期間中、Cisco IME サービスがダウンしていることを示すアラートが Cisco Unified Communications Manager サーバに表示されます。 Cisco Unified Communications Manager への影響を最小限にするため、シスコでは Cisco IME サーバのアップグレードは活動が少ない時間帯に行うことを強く推奨します。 アップグレード手順には、約 20 ～ 30 分かかります。

手順

ステップ 1 Cisco Intercompany Media Engine サーバをアップグレードするためのアップグレード メディアを取得します。

ステップ 2 Cisco.com からソフトウェア実行ファイルをダウンロードした場合、次のいずれかを実行します。

- 次の手順を実行して、ローカル ディレクトリからのアップグレードを準備します。
  - Cisco IME アップグレード ファイルをローカル ハード ドライブの一時ディレクトリにコピーします。
  - ダウンロードしたアップグレード ファイルを ISO イメージとして DVD に焼き付け、アップグレード ディスクを作成します。
    （注） ダウンロードしたアップグレード ファイルを ISO イメージとして DVD に焼き付け、アップグレード ディスクを作成します。
  - SFTP クライアントを開き、インストール中にセットアップした adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続します。
  - cd upgrade と入力してアップグレードディレクトリに移動し、ライセンス ファイルをそのディレクトリにコピーします。
  - put `<upgrade filename>` と入力します。ここで、`<upgrade filename>` には Cisco.com からダウンロードした、または DVD で入手したアップグレード ファイルの名前を指定します。
- put `<upgrade filename>` と入力します。ここで、`<upgrade filename>` には Cisco.com からダウンロードした、または DVD で入手したアップグレード ファイルの名前を指定します。
  シスコが準備したアップグレード ディスクがある場合、ディスクの内容をリモート サーバにコピーします。

  アップグレード ファイルをダウンロードした場合、ダウンロードしたファイルをリモート サーバにコピーします。

ステップ 3 DVD をサーバに挿入した後、もしくはアップグレードファイルをリモートサーバやローカルディレクトリにアップロードした後、Cisco IME CLI にログインし、utils system upgrade initiate と入力します。

ステップ 4 アップグレードするときのソースを次の中から選択します。

- 1：リモート ファイルシステム、SFTP 経由
- 2：リモート ファイルシステム、FTP 経由
- 3：ローカル DVD/CD

- 4：ローカル アップロード ディレクトリ

ステップ 5 選択したアップグレード オプションのシステム プロンプトに従います。

ステップ 6 システムは、アップグレードプロセス完了時にプロンプトを表示します。バージョンの自動切り替えオプションを選択しなかった場合、utils system switch-version と入力し、さらに yes と入力してサーバの再起動と新しいソフトウェア バージョンへの切り替えを承認します。

ステップ 7 インストールが完了したら、Cisco IME CLI にログインし、次の内容を確認します。

- Cisco IME CLI にログインし、show ime dht summary と入力して DHT の健全性のステータスが緑色で表示されていることを確認します。 サーバがリングに参加し、ステータスが緑色に変わるまでに 20 分かかる場合があります。
- show ime vapstatus summary と入力して、[登録ステータス(Registration Status)] が [登録済み(Registered)] になり、[クライアントIP ADDR(Client IP ADDR)] が Cisco Unified Communications Manager サーバの IP アドレスと同じになっていることを確認します。

ローカル アップグレード ディレクトリからアップグレードした場合、ISO ファイルは、アップグレードの完了後、ハード ドライブ上のローカル ディレクトリから自動的に削除されます。 同じロードを使用して別のアップグレードを行う必要がある場合は、ISO ファイルをローカル ディレクトリに再度コピーするか、別のソースを選択する必要があります。

トラブルシューティング

次の項を使用して、Cisco Intercompany Media Engine ソフトウェアのインストール中に発生する問題のトラブルシューティングを行います。

- インストール時のネットワーク エラー, （31 ページ）
- ログ ファイルの調査, （32 ページ）

インストール時のネットワーク エラー

インストールプロセスの中で、インストールプログラムは入力されたネットワーク設定を使用してサーバがネットワーク接続に成功するかどうかを検証します。 サーバに接続できない場合、メッセージが表示され、次のオプションのいずれかを選択するよう促されます。

- [再試行(RETRY)]：インストール プログラムによって、ネットワーキングの検証が再試行されます。 検証に失敗すると、エラー ダイアログボックスが再度表示されます。
- [確認（インストールのチェック）(REVIEW (Check Install))]：このオプションでは、ネットワーキング設定を確認して変更できます。 検出された場合、インストールプログラムはネットワーク設定のウィンドウに戻ります。

ネットワーキングは各ネットワーキング ウィンドウの完了後に検証されるため、メッセージが複数回表示される場合があります。

- [停止(HALT)]：インストールを停止します。 ネットワーク設定のトラブルシューティングに役立てるため、インストール ログ ファイルを USB ディスクにコピーできます。
- [無視(IGNORE)]：インストールを継続します。 ネットワーキングのエラーのログが記録されます。 場合によっては、インストール プログラムがネットワーキングを複数回検証することがあり、このエラー ダイアログボックスも複数回表示されます。 ネットワーク エラーを無視して継続すると、インストールが失敗する場合があります。

ログ ファイルの調査

インストールの問題が発生した場合、コマンドライン インターフェイスで次のコマンドを入力してインストール ログ ファイルを調査できます。

コマンドラインからインストールログファイルの一覧を取得するには、次のように入力します。

CLI>`file list install *`

コマンド ラインからログ ファイルを表示するには、次のように入力します。

CLI>`file view install log_file`

`log_file` にはログ ファイル名を指定します。

リアルタイム モニタリング ツールを使用してログを表示することもできます。 リアルタイム モニタリング ツールの使用とインストールについて詳しくは、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

システム履歴ログを表示またはダウンロードすることにより、インストール イベントの詳細情報を取得できます。 詳細については、次の資料を参照してください。

- システム履歴ログ
- 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』の「*Working with Trace and Log Central*」の章