



# Cisco TelePresence Management Suite

## インストールおよびアップグレード ガイド

初版 : 2023 年 5 月

ソフトウェアバージョン 15.13.5





# 目次

はじめに	7
前提条件	8
導入サイズの見積り	8
ハードウェア要件	9
通常展開と Cisco Business Edition 6000	9
大規模な導入	10
通常規模の展開で推奨されるハードウェアと仮想化	11
大規模な展開で推奨されるハードウェアと仮想化	12
サーバ ソフトウェアおよび設定要件	12
オペレーティング システムとソフトウェア	13
インストール中のアクセス要件	13
日付と時刻の設定	13
SQL Server ソフトウェアとアクセス許可要件	14
ソフトウェア	14
ネットワーク	15
設定とアクセス許可	15
クライアント ソフトウェアの要件	16
サーバ ネットワークの依存関係	16
Cisco TMS が使用するポート	17
セキュリティ設定に関するその他の情報	17
拡張製品との互換性	18
アップグレードの要件および推奨事項	18
IIS 内の仮想ディレクトリ	18
冗長展開	18
2012 より前のバージョンの SQL Server および 2012 より前のバージョンの Windows Server の使用	18
Cisco TMSXE を使用するお客様が 14.4 または 14.4.1 からアップグレードする際の手順	19
Cisco TMSXN を使用するお客様が 14.4 または 14.4.1 からアップグレードする際の手順	20
14.2 よりも前のバージョン	21
Cisco TMS Agent のレガシー プロビジョニング	21
13.2 よりも前のバージョン	22
展開のベストプラクティス	24
データベースのメンテナンス計画	24
復旧モデル	24

定期的なメンテナンス タスク	25
セキュリティ	25
Web および API 通信	25
システムとの通信	26
Cisco TMS の初期セットアップ	26
ユーザー管理	26
ゾーン	26
フォルダ階層	26
会議のデフォルト設定	26
Cisco TMS のインストールまたはアップグレード	28
ご使用になる前に	28
インストーラの実行	28
データベースの作成またはアップグレード	33
リリース キーの追加とネットワーク設定の事前設定	33
ゾーンの事前設定とインストール フォルダの場所の設定	35
証明書の追加	36
Cisco TMS Log Collection Utility のインストール	37
Windows SNMP Service の有効化	41
Cisco TMS への初回アクセス	41
冗長展開の設定	44
事前情報	44
サポートされている構成	44
ライセンス	44
データベースの冗長性	45
Cisco TelePresence Management Suite Provisioning Extension	45
ロード バランサを使用した冗長展開の制限	45
ロード バランサを使用した展開	45
推奨ハードウェア	45
Active Directory およびユーザ認証の要件	45
概要	45
アーキテクチャの概要およびネットワーク構成図	47
インストールと設定	48
フェールオーバーの動作のテスト	49
Cisco TMS のアップグレード	49
ノードに障害が発生した場合のリカバリ	50
冗長展開の管理対象システムのトラブルシューティング	50
ホット スタンバイの展開	51
プライマリ Cisco TMS Server の設定	51
セカンダリ Cisco TMS Server の設定	51
ローカル ファイルの同期	52
オプション : TLS クライアント証明書の有効化	52
Cisco TMS のアップグレード	52
プライマリ サーバで障害が発生した場合のリカバリ	53
バージョン 14.4 以降からの冗長展開のアップグレード	54
サーバをアップグレードする前に	54
プライマリ ノードのアップグレード	54
セカンダリ ノードのアップグレード	54

バージョン 14.4 より前の Cisco TMS からの冗長展開のアップグレードを行う	54
サーバをアップグレードする前に	54
プライマリ サーバのアップグレードと設定	54
プライマリサーバでの設定の更新と検証を行う	55
セカンダリ サーバのアップグレードを行います	55
ACE 構成の例	55
F5 BIG-IP の設定例	56
同期用ローカル ファイル	59
Cisco TMS の移動またはアンインストール	60
新しいサーバに Cisco TMS を移動する	60
ご使用になる前に	60
アプリケーションおよびデータベースの移行	60
アプリケーションの移行後	62
Cisco TMSXE の移動	62
Cisco TMSPE の移動	63
データベースを外部 SQL Server に移動する	64
Cisco TMS のアンインストール	65
サーバからのすべての Cisco TMS 情報を削除する	65
Cisco TMS データベースを外部 SQL Server に移動する	66
TMS Log Collector のアンインストール	66
トラブルシューティング	68
インストールのタイムアウト	68
Windows OS ソフトウェアを 2008R2 から 2012R2 にアップグレードすると、 「TMSSchedulerService」が停止します	68
トラブルシューティングの手順	68
ソリューション	68
SQL Server 接続の問題により、Cisco TMS のインストールまたはアップ グレードが終了した	69
トラブルシューティングの手順	69
解決策	69
TLSv1.0 が無効になっている場合、Windows Server 2016/2012R2 での Cisco TMS のインストールまたはアップグレードが終了する	70
トラブルシューティングの手順	71
解決策	71
付録	72
付録 1：IIS モジュールを必要最低限に制限する	72
付録 2：スパム防止の IIS リクエストの構成	73
IIS 8 および 8.5	73
IIS 7	76
Cisco TMS バンドル	77
インストーラの実行	77
注意事項	86
アクセシビリティ通知	86
Cisco の法的情報	87
Cisco の商標または登録商標	87



## はじめに

## はじめに

Cisco TelePresence Management Suite (Cisco TMS) は、単一の構造化されたインターフェイスからビデオ会議ネットワークの管理とモニタリングを行うためのポータルです。Cisco TMS は、オンサイトおよびリモートのビデオシステムに対する集中管理と、ビデオネットワーク全体に対する導入およびスケジューリングのシステムを提供します。

TelePresence Management Suite (TMS) は、基本的なテレプレゼンスネットワーク用の Cisco システム設定を自動化し、追加設定なしで動作します。組織のニーズを満たすように Cisco TMS の動作を調整したり、ユーザーのアクセス権限を設定したり、Cisco TMS の通話処理機能がすべて利用できるようにネットワークモデルを設定したりできます。

このマニュアルでは、新規インストールの情報および既存のバージョンのアップグレードとアンインストールの情報および、Cisco TMS の新サーバーへの移行情報について説明します。

**注：** Cisco TMS の使用時には、テレプレゼンスネットワーク上で、Cisco TelePresence Manager などの他のテレプレゼンス管理システムを使用しないでください。

## 関連資料

次の表に、このドキュメントで参照されているドキュメントと Web サイト、および関連するマニュアルを示します。Cisco TelePresence Management Suite の最新バージョンに関するすべての資料は、<http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/tsd-products-support-series-home.html> でご確認いただけます。

Cisco TMS 確証機能に関する資料は、<http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-extensions/tsd-products-support-series-home.html> でご確認いただけます。

表 1 関連ドキュメント

タイトル	リンク
<i>Cisco TelePresence Management Suite リリースノート</i>	<a href="http://cisco.com">http://cisco.com</a>
<i>Cisco TelePresence Management Suite のライセンスのインストール、リリース キーおよびオプション キー (Installing licenses; release and options keys for the Cisco TelePresence Management Suite)</i>	<a href="http://cisco.com">http://cisco.com</a>
<i>Cisco TelePresence Management Suite 管理者ガイド</i>	<a href="http://cisco.com">http://cisco.com</a>
<i>Cisco TelePresence Management Suite プロビジョニング拡張機能導入ガイド</i>	<a href="http://cisco.com">http://cisco.com</a>
<i>Cisco TelePresence ビデオ通話 サーバークラスタ作成およびメンテナンス導入ガイド</i>	<a href="http://cisco.com">http://cisco.com</a>

**ヒント：** Cisco TMS ページの右上にあるクエスチョンマークのアイコン (?) をクリックすると、Web ヘルプにアクセスできます。

## トレーニング

トレーニングはオンラインおよびシスコ指定のトレーニング会場で受講できます。当社が提供するすべてのトレーニングの詳細およびトレーニング オフィスの場所については、[www.cisco.com/go/telepresencetraining](http://www.cisco.com/go/telepresencetraining) [英語] を参照してください。

## 用語集

TelePresence 関連の用語集は [tp-tools-web01.cisco.com/start/glossary/](http://tp-tools-web01.cisco.com/start/glossary/) [英語] で入手できます。



# 前提条件

この章では、Cisco TelePresence Management Suite をインストールまたはアップグレードする前に確認が必要な、ハードウェアとソフトウェアの要件、およびその他の考慮事項と依存関係について説明します。

導入サイズの見積り	8
ハードウェア要件	9
サーバ ソフトウェアおよび設定要件	12
SQL Server ソフトウェアとアクセス許可要件	14
クライアント ソフトウェアの要件	16
サーバ ネットワークの依存関係	16
セキュリティ設定に関するその他の情報	17
拡張製品との互換性	18
アップグレードの要件および推奨事項	18

## 導入サイズの見積り

Cisco TMS の要件は、サイズや展開の複雑性によってことなり、拡大します。インストールの複雑性は、主にアクティビティの量、Cisco TMS が管理し、予約可能なエンドポイントの数によって決まります。

次のチャートを使用して導入の相対的なサイズを特定します。目的とする導入が複数の条件と一致する場合には、最も高いレベルを適用します。

	通常および Cisco BE6000	大規模
Cisco TMS	<ul style="list-style-type: none"><li>■ &lt; コントロールシステム 200 台</li><li>■ 同時参加者が最大 100 人</li><li>■ 同時進行するスケジュール済み会議が最大 50 個</li></ul>	<ul style="list-style-type: none"><li>■ &lt; システムライセンスを使用するシステム 5,000 台（つまり、コントロールシステム、Cisco TMS に追加する Unified CM に登録されたシステム、および管理対象外のルーム）。このようなシステムを 5,000 台を超えて追加することはサポートされていません。</li><li>■ 同時参加者が最大 1800 人</li><li>■ 同時進行するスケジュール済み会議が最大 250 個</li></ul>



## 前提条件

Cisco TMSXE	Microsoft Exchange で予約可能なエンドポイントが最大 50 個	<p>&lt; オンプレミス Microsoft Exchange で予約可能なエンドポイント 1,800 個 または</p> <p>&lt; Office 365（またはオンプレミスの Exchange と Office 365 の組み合わせ）で予約可能なエンドポイント 1,000 個</p> <p>Office 365 では、Exchange に対する遅延がオンプレミス展開に比べて一般に大きくなることに注意してください。その結果、Cisco TMSXE で、関連するイベントがすべて処理される前に予約が保存される場合があります。その場合、同じ予約に対して複数の電子メール通知がユーザに届きます。</p>
Cisco TMSPE	<ul style="list-style-type: none"> <li>&lt; Collaboration Meeting Room 1,000 個</li> <li>&lt; Cisco VCS プロビジョニングユーザー 2,000 人（注意：Cisco VCS プロビジョニングは、BE6000 ではサポートされていません）</li> </ul>	<ul style="list-style-type: none"> <li>&lt; Collaboration Meeting Room 48,000 個</li> <li>&lt; Cisco VCS プロビジョニングユーザー 100,000 人</li> </ul>
共存	3 つのアプリケーションと Microsoft SQL Server はすべて共存可能	<ul style="list-style-type: none"> <li>Cisco TMSXE は専用サーバー上にある必要があります。</li> <li>Cisco TMS および Cisco TMSPE は、外部 SQL Server を使用する必要があります。</li> </ul>

Cisco TMS のパフォーマンスと規模に影響を与えるその他の要因として、次が挙げられます。

- Cisco TMS Web インターフェイスにアクセスするユーザー数。
- スケジュールまたは監視されている会議の同時開催。
- アドホック会議モニタリングの使用。
- 複数の拡張またはカスタムクライアントによる Cisco TMSBA の同時使用。予約スループットは、Cisco TMS の **【新規会議 (New Conference)】** ページを含むすべてのスケジュール インターフェイスで共有されます。

実際の予約スピードは、会議のサイズ、機能、および会議のスケジュールの複雑さによって異なります。

## ハードウェア要件

導入サイズの見積りに基づいて該当するハードウェア要件を以下で確認してください。

SQL Server を含むすべてのアプリケーションは、以下のハードウェア要件に対応する仕様の仮想マシンにもインストールできます。

## 通常展開と Cisco Business Edition 6000

通常の実装では、Cisco TMS と拡張は同じサーバーに配置できます。

	要件	Cisco BE6000
CPU	2 コア (Xeon 2.4 Ghz 以上) 、専用	1 vCPU

## 前提条件

	要件	Cisco BE6000
メモリ	8 GB、専用	4 GB の vRAM、専用
サーバで提供されるディスク容量	60 GB	60 GB

Cisco Business Edition 6000 の Cisco TMSPE には、エンドポイントまたは FindMe 用の Cisco VCS ベースのユーザープロビジョニングが含まれていないことに注意してください。

## 大規模な導入

大規模展開の場合、Cisco TMSXE と SQL Server は外部にする必要がありますが、Cisco TMS と Cisco TMSPE は常に共存させることができます。

## Cisco TMS および Cisco TMSPE サーバー

	要件
CPU	2 コア (Xeon 2.2 Ghz 以上) 、専用
メモリ	8 GB、専用
サーバで提供されるディスク容量	80 GB 注：Cisco TMS や Cisco TMSPE を正常に実行するには、ディスク容量の 20% が空いている必要があります。

## Microsoft SQL Server

このサーバーは、Cisco TMS Server と同じタイムゾーンにある必要があります。

	要件
CPU	4 コア (Xeon 2.2 Ghz 以上) 、専用
メモリ	16 GB、専用
サーバで提供されるディスク容量	60 GB

大規模な展開を計画している場合は、次の点にも注意してください。

- 大規模 **tmsng** データに必要なディスク容量は通常、20 ~ 30 GB です。
- ほとんどの展開において、3 つの Cisco TMSPE データベースのサイズが、6 GB を超えることはほとんどありません。
- SQL Server の主なパフォーマンス制限要因は RAM とディスク I/O です。最大パフォーマンスを得るためには、これらの値をできるだけ増やす必要があります。

## Cisco TMSXE サーバー

このサーバの要件は、サポートされているオペレーティング システムの推奨ハードウェア要件と同じです。

## 推奨される Cisco TMS 構成の変更

大規模な展開では、SQL Server と Cisco TMS サービスの負荷を軽減するために、次の設定を強く推奨します。

- **[管理ツール (Administrative Tools) ] > [構成 (Configuration) ] > [会議設定 (Conference Settings) ] : [スケジュールされた通話のデフォルトの予約タイプ (Default Reservation Type for Scheduled Calls) ] を [ワンボタン (One Button To Push) ] に設定**

## 前提条件

- [管理ツール (Administrative Tools)] > [構成 (Configuration)] > [一般設定 (General Settings)] : [電話帳エントリのルーティング (Route Phone Book Entries)] を [いいえ (No)] に設定
- [管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)] : [アドホック会議の検出を有効にする (Enable Ad Hoc Conference Discovery)] を [MCU 限定 (Only for MCUs)] または [いいえ (No)] に設定

## 通常規模の展開で推奨されるハードウェアと仮想化

シスコでは、サポートされる上限位内の通常規模の展開に対して次の仕様を推奨しています。これらはすべてテスト済みです。以下に示す仕様を使用すると、Cisco TelePresence Management Suite (TMS) の展開全体を 1 つのラックマウント型サーバーでホストできます。

## ハードウェア

サーバ	Cisco UCS C220 M3S ラック サーバ
CPU	Intel Xeon プロセッサ E5-2430 v2 (2.50 GHz) X 2
ディスク	146 GB 6G SAS 15K RPM SFF HDD/ホットプラグ/ドライブ スレッド マウント (RAID-6 構成) X 8。 製品番号 : A03-D146GC2。
ディスク コントローラ	LSI MegaRAID 9265-8i 6 Gbps
メモリ	8 GB/1600 Mhz X 4
ハイパーバイザソフトウェア	VMware ESXi 7.0、6.7 および 6.5 は、以下で説明されている仕様の仮想マシンを 3 台ホストします。

## Cisco TMS および Cisco TMSPE 仮想マシン

CPU	vCPU X 2
メモリ	8 GB
ディスク	120 GB

## Microsoft SQL Server 仮想マシン

CPU	vCPU X 2
メモリ	8 GB
ディスク	120 GB

## Cisco TMSXE 仮想マシン

CPU	vCPU X 2
メモリ	8 GB
ディスク	100 GB

## 前提条件

## 大規模な展開で推奨されるハードウェアと仮想化

シスコでは、サポートされる上限位内の大規模な展開に対して次の仕様を推奨しています。これらはすべてテスト済みです。以下に示す仕様を使用すると、Cisco TMS の展開全体を 1 つのラックマウント型サーバーでホストできます。

## ハードウェア

サーバ	Cisco UCS C220 M3S ラック サーバ
CPU	Intel Xeon プロセッサ E5-2430 v2 (2.50 GHz) X 2
ディスク	146 GB 6G SAS 15K RPM SFF HDD/ホットプラグ/ドライブ スレッド マウント (RAID-6 構成) X 8。 製品番号 : A03-D146GC2。
ディスク コントローラ	LSI MegaRAID 9265-8i 6 Gbps
メモリ	8 GB/1600 Mhz X 4
ハイパーバイザソフトウェア	VMware ESXi 6.7、6.5 および 6.0 は、以下で説明されている仕様の仮想マシンを 3 台ホストします。 注 : Cisco TMS は、VMware ファイルシステム 5 で認定されています。

## Cisco TMS および Cisco TMSPE 仮想マシン

CPU	vCPU X 4
メモリ	8 GB
ディスク	200 GB

## Microsoft SQL Server 仮想マシン

CPU	vCPU X 4
メモリ	16 GB
ディスク	250 GB

## Cisco TMSXE 仮想マシン

CPU	vCPU X 4
メモリ	8 GB
ディスク	100 GB

## サーバ ソフトウェアおよび設定要件

ソフトウェア要件は導入のサイズとは無関係です。サイズに適したハードウェア要件については、[「展開サイズの見積もり \(8 ページ\)」](#) および [「ハードウェア要件 \(9 ページ\)」](#) を参照してください。

## 前提条件

## オペレーティング システムとソフトウェア

製品	バージョン	補足事項
Windows Server	<ul style="list-style-type: none"> <li>■ Microsoft Windows Server 2019 (64 ビット)</li> <li>■ Windows Server 2016 64 ビット</li> <li>■ Windows Server 2012 R2 64 ビット</li> <li>■ Windows Server 2012 64 ビット</li> </ul>	<ul style="list-style-type: none"> <li>■ サーバのオペレーティング システムは英語、日本語、または中国語でなければなりません。</li> <li>■ Standard/DataCenter エディションはすべて、Windows Server 2012、2016、および 2019 でサポートされています。</li> <li>■ 新規インストールでは Windows Server 2019 を使用することを推奨します。</li> <li>■ すべてのバージョンに最新のサービス パックを使用することを推奨します。</li> <li>■ 注 : Windows Server 2016 には、Windows 認証用の HTTP2 に関する既知の問題があります。次のレジストリエントリを使用して Windows Server 2016 で HTTP2 を無効にし、Microsoft が問題を修正するまで HTTP を使用し続ける必要があります。 <ul style="list-style-type: none"> <li>- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters <ul style="list-style-type: none"> <li>· EnableHttp2Tls REG_DWORD 0</li> <li>· EnableHttp2Cleartext REG_DWORD 0</li> </ul> </li> </ul> </li> </ul> <p>レジストリを変更したら、Windows Server を再起動します。</p> <p>Active Directory ドメインコントローラへのインストールはサポートされていません。</p>
.NET フレームワーク	<ul style="list-style-type: none"> <li>■ 4.8 .NET Framework</li> <li>■ 4.7 .NET Framework</li> <li>■ 4.7.1 .NET Framework</li> </ul>	<p>Cisco TMS をインストーラを実行する前にインストールする必要があります。</p> <p>注 : .NET Framework 4.7 は、Windows Update Service から自動的にインストールされる場合があります。</p>

## Windows アップデート

組織のネットワーク ポリシーに従って Windows アップデート を有効にして適用します。

## 注 :

- Windows Update を介して更新される最新のタイムゾーンデータを維持することが重要です。
- Windows Server を最新の状態に保つことをお勧めします。

## Windows Server FIPS

Cisco TMS をホストする Windows Server の FIPS モードを有効にすることで、Cisco TMS がデバイスを管理する機能に悪影響を及ぼす可能性があります。手順に関しては、Microsoft のサポート項目 [/System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing/](#) を参照してください。

## インストール中のアクセス要件

インストールを実行する管理者は、Windows サーバへの管理者アクセス権を持っている必要があります。

## 日付と時刻の設定

## 推奨される NTP Server

Cisco TMS を正しく機能させるには、Windows Server の時間を正しく設定する必要があります。サーバーが分離されている場合は、Cisco TMS と SQL Server の時間と日時が一致している必要があります。

## 前提条件

このため、両方のサーバを同じ Active Directory ドメインにして、それらが同じ NTP (Network Time Protocol) サーバを使用するように設定することを強く推奨します。手順については、Microsoft の項目「[How to configure an authoritative time server in Windows Server](#)」を参照してください。

## タイムゾーン

Cisco TMS を新しいデータベースで初期インストールすると、Cisco TMS をホストしている Windows Server のタイムゾーンの変更はサポートされなくなります。

日付/時刻は SQL Server と同じである必要があります、タイムゾーンも同じである必要があります。

## SQL Server ソフトウェアとアクセス許可要件

Cisco TMS は、すべての顧客データを **tmsng** という SQL データベースに保管します。この完全独立型のストレージにより、顧客情報のバックアップとリカバリが容易になります。

新規インストールの場合、インストーラは SQL Server のデフォルトを使用して **tmsng** を作成します。アップグレードでは、既存の Cisco TMS データベースを再利用します。

関連項目：

- メンテナンスのベストプラクティスの詳細については、「[データベースメンテナンス計画 \(24 ページ\)](#)」を参照してください。
- サイズに適したハードウェア要件の詳細については、「[展開サイズの見積もり \(8 ページ\)](#)」と「[ハードウェア要件 \(9 ページ\)](#)」を参照してください。

## ソフトウェア

これは、以下でテストされています。次のいずれかが必要です。

製品	バージョン	テスト済みサービスパックレベル	補足事項
Microsoft SQL Server 2019	すべてのバージョン、64 ビットのみ		
Microsoft SQL Server 2017	すべてのバージョン、64 ビットのみ		このため、10 GB よりも増大すると予測されるデータベースを伴う導入では、フル エディションを使用する必要があります。
Microsoft SQL Server 2016	すべてのバージョン、64 ビットのみ	サービスパック 1	新規インストールの場合、Microsoft SQL Server 2012/2014/2016/2017 の使用が推奨されます。
Microsoft SQL Server 2014	すべてのバージョン、64 ビットのみ	サービスパック 2	注意：Microsoft SQL Server 2012/2014/2016/2017 Express では、データベースサイズが 10 GB までに制限されています。
Microsoft SQL Server 2012	すべてのバージョン、64 ビットのみ	サービスパック 4	
SQL Server Browser			データベースとして別のサーバ上の名前の付いたインスタンスを使用するときは、実行する必要があります。
SQL Native Client 11	13.0.1601.5 以降のバージョン		Cisco TMS と SQL Server が異なるサーバでホストされている場合、Cisco TMS のインストールまたはアップグレード前に SQL Native Client 11 を Cisco TMS Server にインストールする必要があります。Native Client 13.0.1601.5 以降のバージョンがインストールされていることを確認します。詳細については、「 <a href="#">SQL Server 接続の問題が原因で Cisco TMS のインストールまたはアップグレードが終了した (69 ページ)</a> 」項を参照してください。

## 前提条件

## ネットワーク

Cisco TMS Server と SQL Server 間の遅延は、20 ミリ秒以下である必要があります。

## 設定とアクセス許可

デフォルトの SQL 言語は英語に設定されている必要があります。

### 認証モード

インストールおよびアップグレードの場合、データベースサーバーで *SQL Server 認証モード* と *Windows 認証モード*（混合モード）を有効にする必要があります。

インストールが完了すると、以降のアップグレードまで混合モードを無効にして *Windows 認証* を有効にできます。

認証モードの変更手順については、『*Cisco TelePresence Management Suite 管理者ガイド*』の「Cisco TMS ツール」章または Web ヘルプを参照してください。

### ユーザおよびデータベースの作成

Cisco TMS のインストールまたはアップグレードを行う際に、既存の SQL Server を使用する場合は、インストーラから、SQL データベースのユーザーとパスワードの入力を求められます。デフォルトは、サーバ sa（システム管理者）のユーザー名とパスワードの入力です。

**注：** Cisco TMS の sa パスワードでは、セミコロン (;) は使用できません。

sa アカウントが使用できない場合は、次のいずれかを使用します。

- 自動設定を使用しますが、セキュリティが制限されている役割を使用します。
  - a. SQL Server の管理者に、*dbcreator* と *securityadmin* のサーバーの役割を持つ SQL ユーザーとログインを作成するように依頼します。  
このアカウントは、Cisco TMS のサービスアカウントになります。
  - b. インストール中に SQL Server の認証情報を入力するように要求された場合は、そのアカウントのユーザー名とパスワードを入力します。  
Cisco TMS は、サーバーのデフォルト値を使用して **tmsng** をデータベースを自動的に作成し、自身を所有者として割り当て、提供されたアカウントを引き続き使用して、インストール後にデータベースにアクセスします。
- SQL Server の管理者に、セキュリティが最大制限されたユーザの役割を使用して手動でデータベースを作成するように依頼します。
  - **tmsng** という名前のデータベースを、データベース照合 Latin1\_General\_CI\_AI（大文字と小文字を区別せず、アクセント記号も区別しない）で作成します。
  - Cisco TMS サービスアカウントに使用する SQL ユーザーとログインを作成し、このユーザーに **tmsng** データベースの *dbowner* のロールを付与します。Cisco TMS を機能させるためには、インストール後にこのアクセス権限を維持する必要があります。SQL ユーザーは、デフォルトのスキーマとして *dbo* を使用する必要があります。

### スナップショットの分離

インストーラによって、自動的に次のようなスナップショット分離設定が **tmsng** に対して設定されます。この設定は次のように維持する必要があります。

- ALLOW\_SNAPSHOT\_ISOLATION を ON に設定する必要があります。
- READ\_COMMITTED\_SNAPSHOT を ON に設定する必要があります

### 必要なデータベース設定

**注：** **tmsng** データベースへのインストール中に適用される設定の変更はサポートされていません。



## 前提条件

## クライアント ソフトウェアの要件

管理者を含むすべてのユーザーは、Web インターフェイスを使用して Cisco TMS にアクセスします。

Cisco TMS Server にアクセスするには、Windows のユーザー名とパスワードが必要です。ローカルマシンのアカウントまたはドメインのアカウント（このサーバーがドメインに参加している場合）のいずれかが必要です。

Web ブラウザ	<p>Cisco TMS は次のものでテストされています。</p> <ul style="list-style-type: none"> <li>■ Microsoft Internet Explorer バージョン 11</li> <li>■ Firefox version 77</li> <li>■ Google Chrome バージョン 83</li> </ul> <p>その他のブラウザでも動作する場合がありますが、積極的にテストされておらず、サポートされません。</p>
Java Runtime Environment (JRE)	<p>Version 8 が推奨されます。</p> <p>Cisco TMS で <b>[モニタリング (Monitoring)]</b> ページを使用するには、JRE が必要です。インストールされていない場合は、ほとんどのブラウザで、ブラウザ プラグインを自動的にダウンロードしてインストールするように求められます。セキュリティ上の制限により JRE の自動インストールができない場合は、<a href="http://www.java.com">http://www.java.com</a> からダウンロード可能な JRE インストールファイルを、手動でクライアントコンピュータにインストールしてください。</p>

## サーバ ネットワークの依存関係

Cisco TMS をインストールする前に、次のネットワークの依存関係を考慮する必要があります。

- 推奨されるドメインメンバーシップ：Cisco TMS にログインしている各ユーザーには、Web サイトに対する認証のため、Windows のユーザーログインが必要です。ユーザーには、Cisco TMS Windows Server 上のローカルアカウント、またはサーバーが Active Directory 経由で信頼するドメインアカウントが必要です。サーバーをドメインのメンバーにすることによって、すべての信頼ドメインのユーザーは、Cisco TMS へのログインに既存の Windows ログイン情報を自動的に使用できます。Cisco TMS 権限を使用して Cisco TMS にログインした後も、ユーザーが実行できることを制限できます。アクティブディレクトリのメンバーシップ認証は、各ユーザにローカルの Windows アカウントを作成する必要がないため、ほとんどの導入において推奨されます。
- IP およびホスト名でアクセス可能な Cisco TMS Web サイト：すべてのデバイスがドメインネームシステム (DNS) ホスト名またはポート番号をサポートするわけではないため、Web サイトはポート 80 の IP アドレスからアクセスする必要があります。一部の機能は Cisco TMS にホスト名からアクセスできるようにするため、Cisco TMS には完全修飾ドメイン名でもアクセスする必要があります。
- メールサーバーアクセス：Cisco TMS では、電子メールを送信できるようにするため、SMTP サーバーへのアクセスが必要です。この用途には、社内の既存のメール サーバを利用できます。Cisco TMS は、必要に応じて認証用に SMTP AUTH ログインをサポートしています。
- 管理対象デバイスへのネットワーク アクセス：Cisco TMS には、デバイスを管理するための特定のプロトコルとアクセス権が必要です。ネットワーク ファイアウォールまたは NAT ルータは、Cisco TMS に対するトラフィックの送受信を許可する必要があります。
- Microsoft IIS のコンポーネント ASP.NET および ASP を有効にする必要があります。
- Windows ファイアウォール機能はデフォルトで有効になり、着信ポートと発信ポートの両方を制御します。Windows ファイアウォールが有効になっている場合に、どのポートが開放されている必要があるかについては、「[Cisco TMS が使用するポート \(17 ページ\)](#)」を参照してください。
- アンチウイルス プログラムまたはその他のセキュリティ対策により、アプリケーションの SMTP ポートを使用したメールの直接送信がブロックされていないことを確認してください。



## 前提条件

## Cisco TMS が使用するポート

Cisco TMS が使用する次のポートは、Windows ファイアウォールで有効にする必要があります。構成および使用デバイスによっては、すべてのインストールですべてのサービスが使用されるとは限りません。

サービスまたはシステム	トランスポート プロトコル	ポート	Cisco TMS を基準にした方向	
			着信	発信
FTP	TCP	20、21		X
HTTP	TCP	80	X	X
Cisco TelePresence System (CTS) 用 HTTP	TCP	8081		X
HTTPS	TCP	443	X	X
Cisco TelePresence System (CTS) の HTTPS	TCP	9501		X
Unified CM の HTTPS	[TCP]	8443		X
LDAP	TCP	389		X
LDAPS	TCP	636		X
Polycom GAB	TCP	3601	X	
SMTP	TCP	25		X
SNMP	UDP	161		X
SNMP トラップ	UDP	162	X	X
SSH	TCP	22		X
Telnet	TCP	23		X
Telnet チャレンジ	TCP	57		X
Telnet Polycom	TCP	24		X

SQL 接続では、デフォルトの SQL Server インスタンスに使用される TCP ポートが構成可能です。名前を付けられた SQL Server インスタンスに使用されるポートは動的であり、サービスが再起動されるたびに変更されます。SQL Server が特定のポートをリッスンするように構成する方法については、TechNet の項目「[Configure a Server to Listen on a Specific TCP Port \(SQL Server Configuration Manager\)](#)」を参照してください。

## 複数の IP アドレスには未対応

Cisco TMS は複数の IP アドレスを使用することはできず、利用可能な最初のネットワーク インターフェイスにのみバインドされます。このため、複数のネットワークカードや、同じカードの IP エイリアスはサポートされません。複数の IPv4 アドレスと複数の IPv6 アドレスはサポートされていませんが、単一の IPv4 アドレスと単一の IPv6 アドレスはサポートされます。

Cisco TMS はネットワークでパブリックとプライベートの両方のネットワークがルーティングによってインターコネクトされている限り、両方のネットワークを管理することができます。複数のネットワーク インターフェイス カードを使用して両方のネットワークを Cisco TMS に直接接続することはできません。

## セキュリティ設定に関するその他の情報

- Cisco TMS は SSLv3 とそれ以降のバージョン、および 3DES をサポートしていません。
  - SSLv3 とそれ以下のバージョン、および 3DES を無効にする方法については、Microsoft の項目「[Cryptographic Algorithms and Protocols](#)」を参照してください。

## 前提条件

- Cisco TMS は暗号方式を制御しません。
  - サポートされている暗号の詳細については、[Microsoft の項目「Cipher Suites」](#)を参照してください。
  - サポートされている暗号の構成方法については、[Microsoft の項目「Cipher Suites Priority Order」](#)を参照してください。
- Cisco TMS は RC4 暗号方式を制御しません。RC4 暗号スイートを無効化する方法については、[Microsoft の項目「RC4 の無効化」](#)を参照してください。

注：Windows マシンが Open SSL がサーバとして機能する OpenSSL デバイスを持つクライアントとして動作する場合の、Microsoft の暗号の問題の詳細については、<https://www.cisco.com/c/en/us/support/docs/conferencing/telepresence-management-suite-tms/212421-windows-ciphers-cause-tls-issue-between.html> を参照してください。

## 拡張製品との互換性

製品	バージョン
Cisco TelePresence Management Suite Extension for Microsoft Exchange	5.13
Cisco TelePresence Management Suite Provisioning Extension	1.14

注：すべての機能と修正を利用できるようにするには、最新バージョンが必要です。

## アップグレードの要件および推奨事項

ご使用の Cisco TMS のアップグレードを開始する前に、現在稼働している Cisco TMS のバージョンに適用される以下のすべてのセクションを確認してください。

### IIS 内の仮想ディレクトリ

Cisco TMS のどのバージョンからアップグレードするときも、すべての仮想ディレクトリは削除され、新しいバージョンのインストール時に再作成されます。このとき、仮想ディレクトリに対するカスタム設定もすべて削除されることに注意してください。

### 冗長展開

[「バージョン 14.4 より前の Cisco TMS からの冗長展開のアップグレードを行う \(54 ページ\)」](#)を参照してください。

## 2012 より前のバージョンの SQL Server および 2012 より前のバージョンの Windows Server の使用

Cisco TMS をアップグレードする場合で、2012 より前のバージョンの SQL Server または 2012 より前のバージョンの Windows Server を実行している場合は、Cisco TMS のアップグレードの前にサーバーをアップグレードする必要があります。詳細については、[「ソフトウェア \(14 ページ\)」](#)を参照してください。

14.4 および 14.6 では、SQL および Windows サーバの要件が変更されました。Cisco TMS をアップグレードする場合で、2008 R2 より前のバージョンの SQL Server または 2008 R2 より前のバージョンの Windows Server を実行している場合は、Cisco TMS のアップグレードの前にサーバーをアップグレードする必要があります。SQL Server および Windows Server は 2017 にアップグレードすることをお勧めします。

サポートされているバージョンの完全な概要については、[「サーバーソフトウェアおよび構成要件 \(12 ページ\)」](#)および [「ソフトウェアおよび権限要件 \(14 ページ\)」](#)を参照してください。

32 ビット DB インストールモードでの既存の (SQL 2012 を使用するまたはその他のバージョン) Cisco TMS からアップグレードを行うには、Microsoft がダイアログボックスの移行のために提供する推奨手順に従う必要があります。ただし、Cisco TMS 15.7 は引き続き 32 ビット SQL DB で動作します。SQL Server 2017 と Windows Server 2016 にアップグレードすることをお勧めします。Cisco TMS を 15.9 に移行したいユーザーは、Microsoft が推奨する手順を使用して DB を 64 ビットに移行する必要があります。

## 前提条件

## Cisco TMSXE を使用するお客様が 14.4 または 14.4.1 からアップグレードする際の手順

このアップグレード手順の要件に関する追加の背景情報については、「[Cisco TelePresence Management Suite リリースノート \(14.4.2\)](#)」を参照してください。

## Cisco TMSXE および Cisco TMS のアップグレード

Cisco TMSXE を使用するお客様および 14.4 または 14.4.1 からアップグレードするお客様は、順番に従って次のアップグレード手順に従う必要があります。

1. Cisco TMSXE を バージョン 4.1 にアップグレードします。
2. Cisco TMS をこのバージョンにアップグレードします。
3. 15 分間待ってから Cisco TMSXE ログを確認します。**TMSXE-log-file.txt** で、**INFO ReplicationEngine - No changes on TMS** と記載されている行を確認します。  
これにより、Cisco TMS が解決できるすべての予約が、Cisco TMS から Microsoft Exchange に正しく複製されていることが確認できます。

この行を確認できない場合は、シスコのサポート担当者にお問い合わせください。

## Cisco TMS で重複する会議を解決する

この 2 番目の手順はアップグレード後なるべく早く実行する必要がありますが、ただちに実行する必要はなく、メンテナンス時間帯の確保も不要です。

1. Cisco TMS に移動し、「外部プライマリキーが重複する会議シリーズが見つかりました (Conference series with duplicate external primary keys found)」という重要な Cisco TMS チケットがないか確認します。
  - このチケットがない場合、何もする必要はありません。
  - チケットが見つかった場合、手順 2 および 3 に進みます。
2. Cisco TMS ツールで **[重複キーの解決 (Resolve Duplicate Keys)]** ツールを実行し、重複のリストから適切な会議を選択します。  
どれが正しい会議が明らかでない場合は、会議に参加するシステムの Exchange リソース カレンダーを確認してください。リソース カレンダーの大部分またはすべてが、重複する会議の 1 つと一致する場合、おそらくそれが適切な会議です。  
それでも正しい会議を特定できない場合は、会議の所有者に問い合わせてください。
3. 15 分間待ってから Cisco TMSXE ログを確認します。**TMSXE-log-file.txt** で、**INFO ReplicationEngine - No changes on TMS** と記載されている行を確認します。これにより、残りすべての問題のある予約が Cisco TMS から Microsoft Exchange に正しく複製されていることが確認できます。この行を確認できない場合は、シスコのサポート担当者にお問い合わせください。

## Exchange リソース カレンダーで残りの重複するアポイントメントを手動で解決する

展開の状況によっては、Cisco TMS のこのバージョンの Cisco TMS へのアップグレード時に自動的に特定またはクリーンアップされない重複する Exchange アポイントメントがリソースカレンダーに少数残ることがあります。

重複がよく発生するのは、会議テンプレートを使用するか、14.4 より前のバージョンの Cisco TMS の既存の会議をコピーして会議を作成し、それからその会議を 14.4 または 14.4.1 で (Cisco TMS または Microsoft Exchange で) 編集した場合です。

このような重複する Exchange アポイントメントを特定して解決するには、次の手順を実行します。

1. Cisco TMSXE サーバーにログオンし、現在からスケジュール範囲の最後まででの検索期間で Meeting Analyzer を実行します。  
大規模な導入においては、これを営業時間外に実行するか、Exchange サーバの負荷を減らすために短い検索対象期間で Meeting Analyzer を実行することをお勧めします。

## 前提条件

2. Meeting Analyzer レポートで、「Cisco TMS で一致する会議が見つかりません (No matching conferences found in)」というフラグが付けられたアポイントメントを探します。  
このフラグが付けられたアポイントメントがない場合、何もする必要はありません。  
フラグ付きのアポイントメントが見つかった場合は、手順 3 に進みます。
3. Exchange リソース カレンダーに対してフル アクセスできるユーザでログインします。
  - a. Microsoft Outlook を開きます。
  - b. 手順 2 で特定した重複するアポイントメントの 1 つを探します。
4. 重複するアポイントメントの開始時間、終了時間、または情報カテゴリが Cisco TMS の対応するアポイントメントと異なる場合は、すべての Exchange リソースカレンダーから削除します。  
アポイントメントに相違点がない場合は、以下の「適切なアポイントメントを特定するための変更の適用」手順に進みます。
5. 手順 3 に戻り、問題のある別のアポイントメントを処理します。

## 適切なアポイントメントを特定するための変更の適用

開始時間、終了時間、および件名が同じアポイントメントがリソース カレンダーに 2 つ以上ある場合は、重複するアポイントメントを区別できず、どれを削除すべきか判断できません。差異を確認できるようにする変更を適用し、適切なアポイントメントを特定するには、次の手順に従います。

1. Cisco TMS で、[予約 (Booking)] > [会議のリスト (List Conferences)] の順に選択し、会議を見つけます。
2. 会議を編集し、会議時間を 5 分短縮して [会議の保存 (Save Conference)] をクリックします。Cisco TMSXE では 3 分以下の変更は無視されるため、この時間は重要です。
3. Cisco TMSXE レプリケーターが変更を処理し、Exchange リソースカレンダーが新しい終了時間に更新されるのを待ちます。これには数分かかることがあります。
4. 終了時間が新しくなった Exchange のアポイントメントが、Cisco TMS に正しくリンクされているアポイントメントになります。ここで、終了時間が変更されなかった重複する 1 つ以上のアポイントメントを削除します。
5. Cisco TMS では、元の会議終了時間を元に戻します。

## Cisco TMSXN を使用するお客様が 14.4 または 14.4.1 からアップグレードする際の手順

このアップグレード手順の要件に関する追加の背景情報については、「[Cisco TelePresence Management Suite リリースノート \(14.4.2\)](#)」を参照してください。

## Cisco TMS のアップグレードと重複する会議の解決

Cisco TMSXN を使用し、14.4 または 14.4.1 からアップグレードするお客様は、最初にこのバージョンの Cisco TMS にアップグレードし、アップグレード後なるべく早くこの手順を実行する必要があります。ただし、ただちに実行する必要はなく、メンテナンス時間帯の確保も不要です。

1. Cisco TMSXN Synchronizer が Cisco TMS からのデータを処理するまで 15 分待ちます。
2. Cisco TMS で、「外部プライマリーが重複する会議シリーズが見つかりました (Conference series with duplicate external primary keys found)」と記載されている重要な Cisco TMS チケットがないか確認します。  
このチケットがない場合、何もする必要はありません。  
チケットが見つかった場合は、手順 4 に進みます。
3. Cisco TMS ツールで、[重複キーの解決 (Resolve Duplicate Keys)] ツールを実行し、重複のリストから適切な会議を選択します。  
どの会議が適切かわからない場合は、会議に関係するシステムの Domino カレンダーを確認します。リソース カレンダーの大部分またはすべてが、重複する会議の 1 つと一致する場合、おそらくそれが適切な会議です。  
それでも正しい会議を特定できない場合は、会議の所有者に問い合わせてください。

## 前提条件

## Cisco TMSXN Synchronizer の再起動

このプロセスによって、Cisco TMS から Domino への複製が再開され、Cisco TMS にあるすべての今後の予約（すでに存在している予約以外）が Domino に書き込まれます。

1. Domino Administrator から、[ファイル (Files)] > [ビデオ会議リソース (Video Conference Resources)] を開きます。
2. [予約 (Reservations)] > [日付順 (By Date)] に移動し、予約を選択します。
3. [操作 (Actions)] > [Synchronizer の再起動 (Restart Synchronizer)] の順に選択します。
4. Domino ログ ファイルを監視し、「Agent 出力 : 0 からの Synchronizer が終了しました (Agent printing: Synchronizer from zero finished)」というステートメントの表示を待ちます。このステートメントが表示されると、Cisco TMS からのすべての予約が Domino に再度複製されています。

## 14.2 よりも前のバージョン

Cisco TMS タイムゾーンのサポートは 14.2 で改善され、以前のバージョンからのアップグレード後にタイムゾーンデータのずれを修正するタイムゾーン更新ツールができました。このツールをサポートした最後のバージョンは 14.3.2 でした。

次の場合、最新バージョンにアップグレードする前に、14.3.2 にアップグレードしてタイムゾーン ツールを実行する必要があります。

- 米国と欧州の両方、または北半球と南半球の両方から会議のスケジュールを設定するユーザがいる場合
- 州や地域によって DST ルールが異なる国（例：オーストラリア）のユーザである場合

**注意：**上記いずれかの場合に直接アップグレードすると、データが不正確になるおそれがあります。

Cisco TMS およびテレプレゼンスネットワークで会議の予約を行うすべての開催者のタイムゾーンが同じ場合や、タイムゾーンで米国（アリゾナ州とハワイ州を除く）のように同じ DST ルールを使用する場合、14.3.2 を経由してアップグレードを行う必要はありません。

タイムゾーンの更新の詳細および手順については、14.3.2 の『Cisco TMS のインストールおよびアップグレードガイド』を参照してください。

タイムゾーンの不一致が解消されたら、15.13.5 にアップグレードできます。

## Cisco TMS Agent のレガシー プロビジョニング

13.2.x からのアップグレードまたはレガシープロビジョニング機能を使用する以前のバージョンの場合、Cisco TMS 15.13.5 にアップグレードする前に Cisco TelePresence Management Suite Provisioning Extension を移行する必要があります。

この移行には、13.2 バージョンの Cisco TMS が必要です。現在それより古い Bluetooth を使用している場合は、以下を実行する必要があります。

1. Cisco TMS を 13.2.x. にアップグレードする  
13 以前のバージョンからアップグレードする場合は、このアップグレードを実行するためにシスコから Cisco TMS 13 リリースキーを取得する必要があります。
2. Cisco TMS 13.2 向けの『Cisco TelePresence Management Suite Provisioning Extension 導入ガイド』に従って、Cisco TMSPE をインストールし、プロビジョニング データベースを移行します。
3. 展開に、タイムゾーンの変更により 14.3.2 を介したアップグレードが必要になるかどうかを確認します。  
「[14.2 以前のバージョン \(21 ページ\)](#)」を参照してください。
4. タイムゾーンの問題が解決したら Cisco TMS 15.13.5 にアップグレードします。

## 前提条件

## 13.2 よりも前のバージョン

デフォルトの予約の確認用電子メール テンプレートとフレーズ ファイルは 13.2 で更新されました。これらのテンプレートがカスタマイズされたテンプレートである 13.2 よりも前のバージョンからアップグレードする場合、新しい追加はカスタマイズされたファイルに自動的に追加されませんが、引き続き使用することができます。

この新しい値のデフォルトの使用法を確認し、これらの値をテンプレートに持たせるには、カスタマイズされた予約の確認テンプレートまたはフレーズを保有するお客様は次の手順を実行する必要があります。

1. **[管理ツール (Administrative Tools) ] > [構成 (Configuration) ] > [電子メールテンプレートの編集 (Edit Email Templates) ]** の順に選択します。
2. **Booking Confirm** テンプレートを開きます。
3. **[デフォルトに戻す (Revert to Default) ]** をクリックします。

デフォルトに設定されると、カスタマイズをテンプレートまたはフレーズ ファイルに再度追加できます。

## 13.0 よりも前のバージョン

13.0 までのバージョンからのアップグレードは、Cisco TMS 15.13.5 でテストされ、サポートされます。それよりも前のバージョンでは、サーバの要件、データベース、およびバックエンドが大幅に変更されているため、アップグレードではなく新規インストールを実行することを推奨します。







# 展開のベストプラクティス

この章では、Cisco TMS のインストールと初期構成のベストプラクティスについて説明します。

データベースのメンテナンス計画 .....	24
セキュリティ .....	25
Cisco TMS の初期セットアップ .....	26

## データベースのメンテナンス計画

Cisco TMS と Cisco TMSPE の両方は、SQL Server のデフォルト設定に基づいてデータベースを作成します。データベースには次のものがあります。

- **tmsng** (Cisco TMS )
- **tmspe** (Cisco TMSPE メイン)
- **tmspe\_vmr** (Cisco TMSPE Collaboration Meeting Rooms)
- **tms\_userportal** (Cisco TMSPE セルフサービスポータル)

データベースのメンテナンス計画を作成および維持するためのベスト プラクティスについて以下で説明します。データベースは、Microsoft SQL Server Management Studio Express などの外部ツールで管理する必要があります。

## 復旧モデル

必要な動作に応じて、データベースは単純復旧モデルまたは完全復旧モデルに設定できます。書くリカバリモデルの機能詳細については、MSDN の項目 [「Recovery Models \(SQL Server\)」](#) を参照してください。

### 単純復旧

一般的な Cisco TMS 展開の場合、単純復旧モデルを使用することをお勧めします。これは、バックアップ間のリカバリのみをサポートします。

このモデルでは、定期的な間隔でデータベースをバックアップし、トランザクション ログは省略します。データベースではログの領域が再利用されるので、ファイル サイズは限られます。データベース トランザクション ログのサイズは小規模で、データベース バックアップの間に増え続けることはありません。

### 完全復旧

大規模な Cisco TMS 展開をしたことがある SQL Server 管理者は、追加容量や完全復旧モデルが提供する完全性ツールを選択する場合があります。これは、データベース トランザクションログを使用した任意の時点までのリカバリがサポートされます。

この復旧モデルでは、データベース トランザクション ログ ファイルはバックアップの間に常に増加するため、メンテナンスを行わずに放置すると、データベースが容量を使い切って停止する原因になる場合があります。

この復旧モデルでは、データベースおよびトランザクション ログの定期的なバックアップは必須です。



## 展開のベストプラクティス

### 復旧モデルの特定または変更

データベースの復旧モデルを特定または変更するには、お使いの SQL Server バージョン向けの Microsoft の手順書を参照してください。

- [データベースのリカバリモデルの表示または変更](#) (SQL Server 2012 や 2016)

### 定期的なメンテナンス タスク

ベスト プラクティスとして、バックアップとインデックスのメンテナンスのための定期的なメンテナンス タスクを設定します。データベースメンテナンスは Cisco TMS のパフォーマンスに影響することに注意してください。これらのタスクは組織のスケジュールされたメンテナンス時間に実行します。

#### バックアップ

組織のリカバリポリシーに従って、最低でも週に 1 回は tmsng データベースのバックアップを行います。

- [SQL Server データベースのバックアップと復元](#) (SQL Server 2012 や 2016)

#### インデックスのメンテナンス

過度のフラグメンテーションを避けるために、定期的にデータベース インデックスのメンテナンスを実施します。毎月またはフラグメンテーションが 30% を超えたときに、インデックスの再構築を行うことをお勧めします。

- [インデックスの再編成と再構築](#) (SQL Server 2012 や 2016)

### SQL Server メンテナンスプラン

(Express ではなく) SQL Server のフルバージョンを使用する場合、組み込みのメンテナンス計画機能およびウィザードを前述のタスクに利用できます。使用方法については、次の Microsoft の記事を参照してください。

- [メンテナンスプランの作成](#) (SQL Server 2012 や 2016)

### データベース サイズの管理

データベースを縮小する定期的なメンテナンスタスクは行わないことを強くお勧めします。時間とともにデータベース サイズは正常に安定し、30% のバッファを加えた固定サイズとして指定することができます。

いくつかの状況では、アップグレードの最中にデータベース サイズが著しく増加します。このような場合には、データベースを縮小する 1 回だけの操作をお勧めします。

## セキュリティ

このセクションでは、Cisco TMS の展開をより安全行うために推奨される方法を説明します。

### Web および API 通信

デフォルトで、Cisco TMS インストーラは、Web 通信用の HTTP を設定します。これにより、管理者によって自己署名証明書が提供されない場合に証明書を作成することができます。実稼働環境で有効な証明書を使用し、自己署名証明書の使用をラボ展開のみに制限することを強くお勧めします。

セキュリティ設定の詳細については、『[Cisco TMS 管理者ガイド](#)』の **[高度なセキュリティ設定 (Advanced Security Settings)]** > **[通信セキュリティ (Communication Security)]** 項を参照してください。

### セキュリティ向上のために IIS を構成する

IIS マネージャで次の手順を実行します。

## 展開のベストプラクティス

1. Polycom システムを使用しない場合は、次の手順を実行して Polycom の電話帳コンポーネントを無効にします。
  - a. デフォルトの Web サイトのツリー ビューを展開します。
  - b. `/pwx` コンポーネントを右クリックし、**[削除 (Remove)]** を選択します。
2. Web および API トランザクションの HTTP の無効化：
  - a. `/tms` コンポーネントをクリックして選択します。
  - b. **[IIS]** セクションで、**[SSL 設定 (SSL Settings)]** をダブルクリックします。
  - c. **[SSL を使用 (Require SSL)]** をオンにして、**[アクション (Actions)]** パネルで **[適用 (Apply)]** をクリックします。
  - d. `/tms` コンポーネントを展開し、`/public` をクリックして選択します。
  - e. **[IIS]** セクションで、**[SSL 設定 (SSL Settings)]** をダブルクリックします。
  - f. **[SSL を使用 (Require SSL)]** をオフにして、**[アクション (Actions)]** パネルで **[適用 (Apply)]** をクリックします。
3. スпам防止のリクエストを設定します。設定手順の詳細については、[「付録 2：スパム防止の IIS リクエストの構成 \(73 ページ\)」](#) を参照してください。

## システムとの通信

Cisco TMS は、デフォルトで、HTTP を使用してシステムと通信しますが、一部のレガシーシステムとは SNMP を使用します。

レガシーシステムを使用する場合は、サーバー上で **Windows SNMP Service** を有効にすることで、SNMP を使用できます。

注：SNMP トラップは、MXP や Polycom などのレガシーエンドポイントの冗長セットアップで、F5 ロードバランサを介して Cisco TMS Server に送信する必要があります。

## Cisco TMS の初期セットアップ

Cisco TMS 構成は、展開後や運用中でも通常いつでも修正できます。ただし、メンテナンスおよび運用を簡単にするために、インストールの直後、ユーザにシステムの利用を許可する前に、ユーザ アカウント ポリシー、ゾーン、および基本設定のデフォルトを設定することをお勧めします。

手順については、組み込みの Cisco TMS ヘルプまたは『Cisco TMS 管理者ガイド』を参照してください。

## ユーザー管理

すべての Cisco TMS ユーザーを管理する際は、Microsoft Active Directory の使用が強く推奨されます。

## ゾーン

インストールの最中にゾーンの初期設定を行うことができます。インストール後に構成を表示したり、修正したりするには、**[管理ツール (Administrative Tools)]** > **[ロケーション (Locations)]** > **[ISDN ゾーン (ISDN Zones)]** または **[IP ゾーン (IP Zones)]** の順に選択します。

## フォルダ階層

システムに Cisco TMS を追加する前に、**[システム (Systems)]** > **[ナビゲータ (Navigator)]** 内のエンドポイントおよびインフラストラクチャ システムについて、よく構造化された拡張性の高いフォルダ階層を計画することを強くお勧めします。

## 会議のデフォルト設定

ユーザが会議の予約を始める前に、接続タイプ、帯域幅などについてデフォルト設定を見直して調整することをお勧めします。**[Administrative Tools]** > **[Configuration]** > **[Conference Settings]** に移動します。





# Cisco TMS のインストールまたはアップグレード

この章では、Cisco TMS の新規インストールまたはアップグレードの手順について説明します。

ご使用になる前に .....	28
インストーラの実行 .....	28
Cisco TMS への初回アクセス .....	41

## ご使用になる前に

次の内容について確認してください。

- 使用環境へのインストールに関するすべての「[前提条件 \(8 ページ\)](#)」が考慮されます
- 必要な Cisco TMS ソフトウェアバンドルは、Cisco.com からダウンロードできます
- Cisco TMS リリースキーおよびすぐに追加する予定のシステムと機能のオプションキー

アップグレードの場合も、Cisco TMS の現在のバージョンからアップグレードする際に適用する特定の手順や要件に関して「[アップグレードの要件と推奨事項 \(18 ページ\)](#)」を見直してください。

バックアップデータベースの復元は、以前のバージョンに戻すために唯一の方法であるため、更新前に Cisco TMS データベース (tmsng) コピーをバックアップすることが強く推奨されます。

インストール中にサーバをリブートするように複数回要求される場合があります。インストーラは、サーバのリブート後に自動的に再開します。

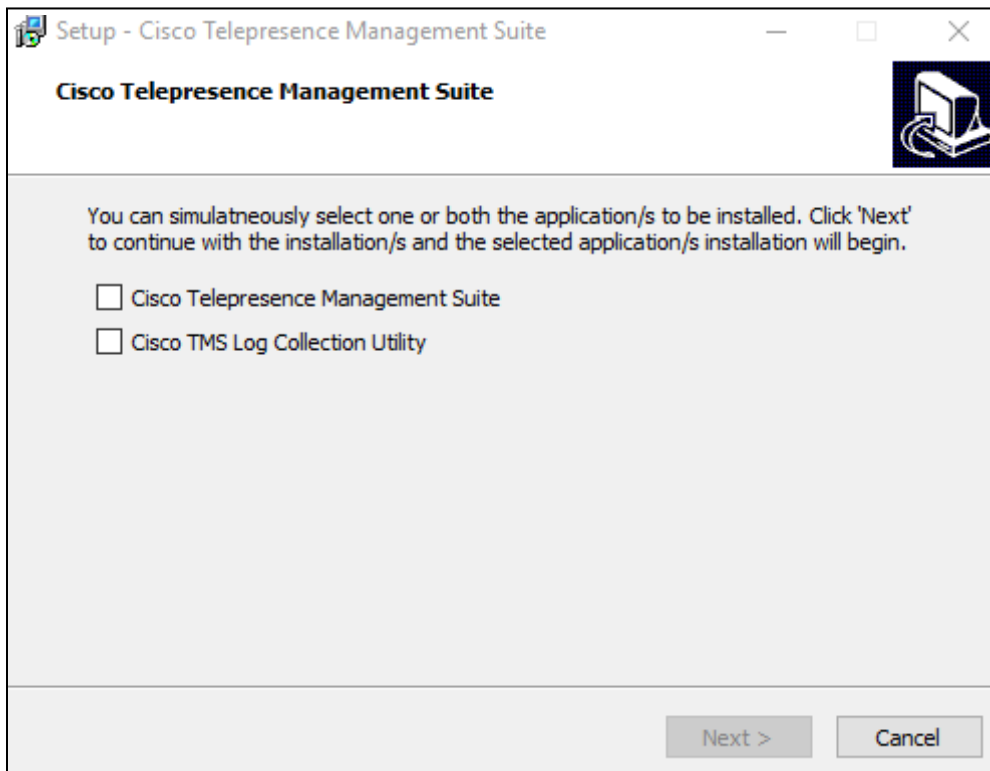
## インストーラの実行

追加する必要がある Windows コンポーネントによって、インストール時にサーバを複数回リブートするように求められる場合がありますことに注意してください。インストーラは、サーバのリブート後に自動的に再開します。

1. TMS Log Collector や Cisco TMS ツールなど開いているすべてのアプリケーションを閉じて、インストールを妨害する恐れのあるウイルス スキャン ソフトウェアやその他ソフトウェアを無効にします。
2. **Cisco TMS.zip** アーカイブをフォルダに展開します。
3. **Cisco TMS** の実行可能ファイルを管理者として実行します。

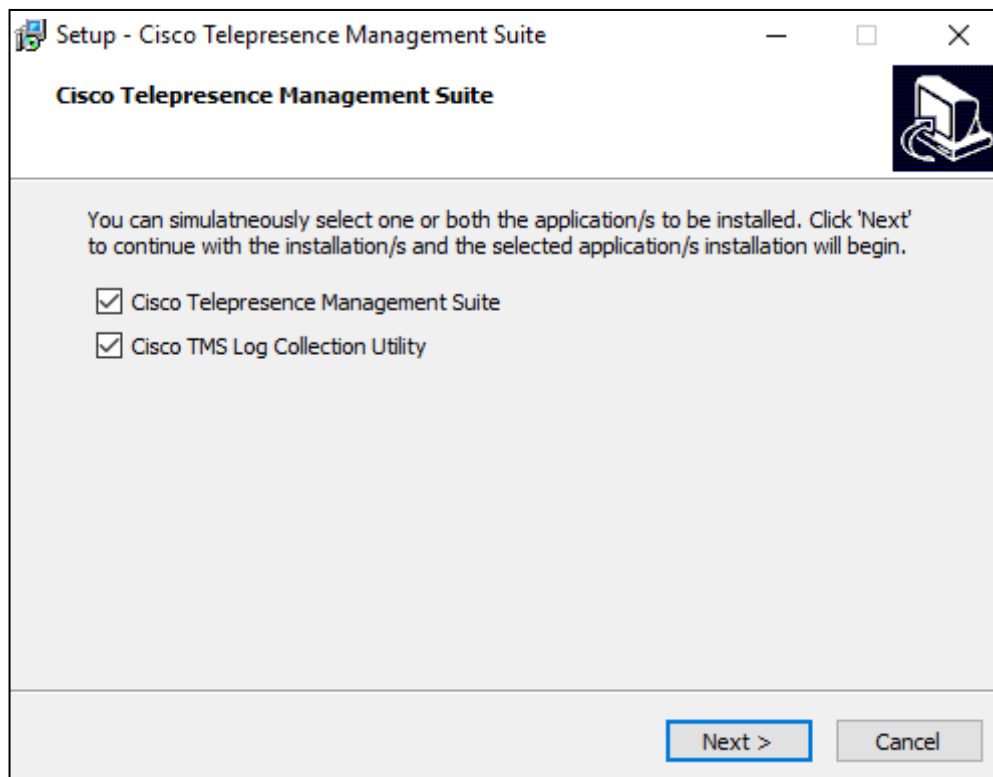
## Cisco TMS のインストールまたはアップグレード

4. インストーラパッケージを実行すると、次のオプションを示すダイアログボックスが表示されます。
  - a. Cisco Telepresence Management Suite
  - b. Cisco TMS Log Collection Utility

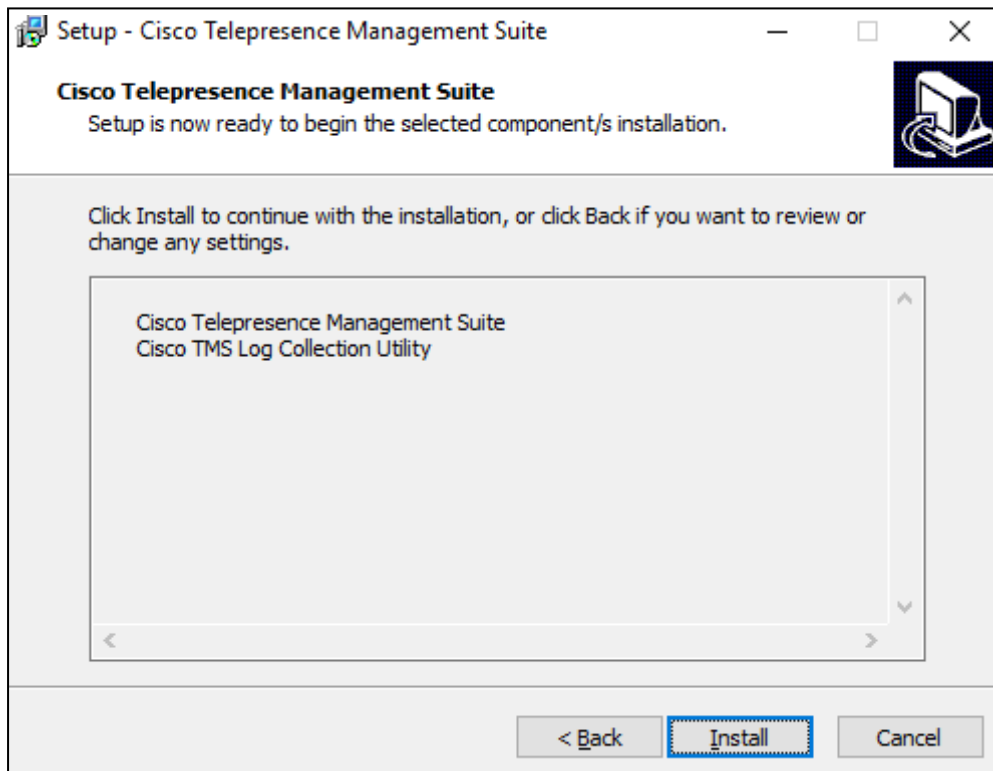


5. インストールするアプリケーションを選択し、[次へ (Next) ] をクリックします。

## Cisco TMS のインストールまたはアップグレード

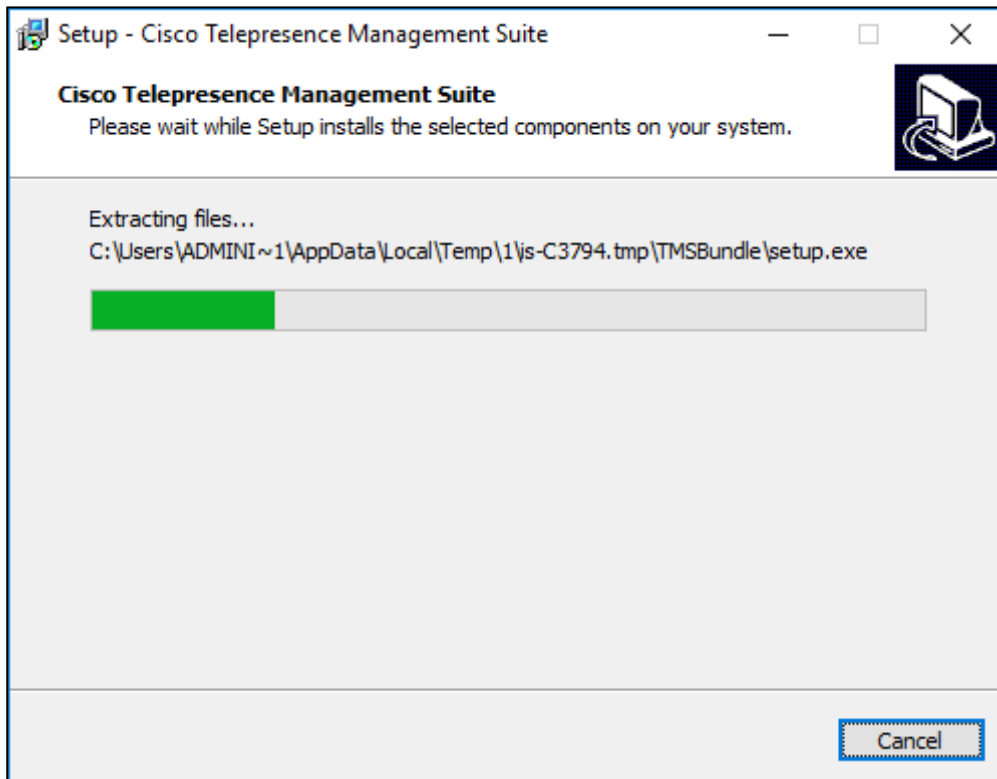


6. [インストール (Install)] をクリックして、選択したアプリケーションをインストールします。



7. インストールが開始されます。

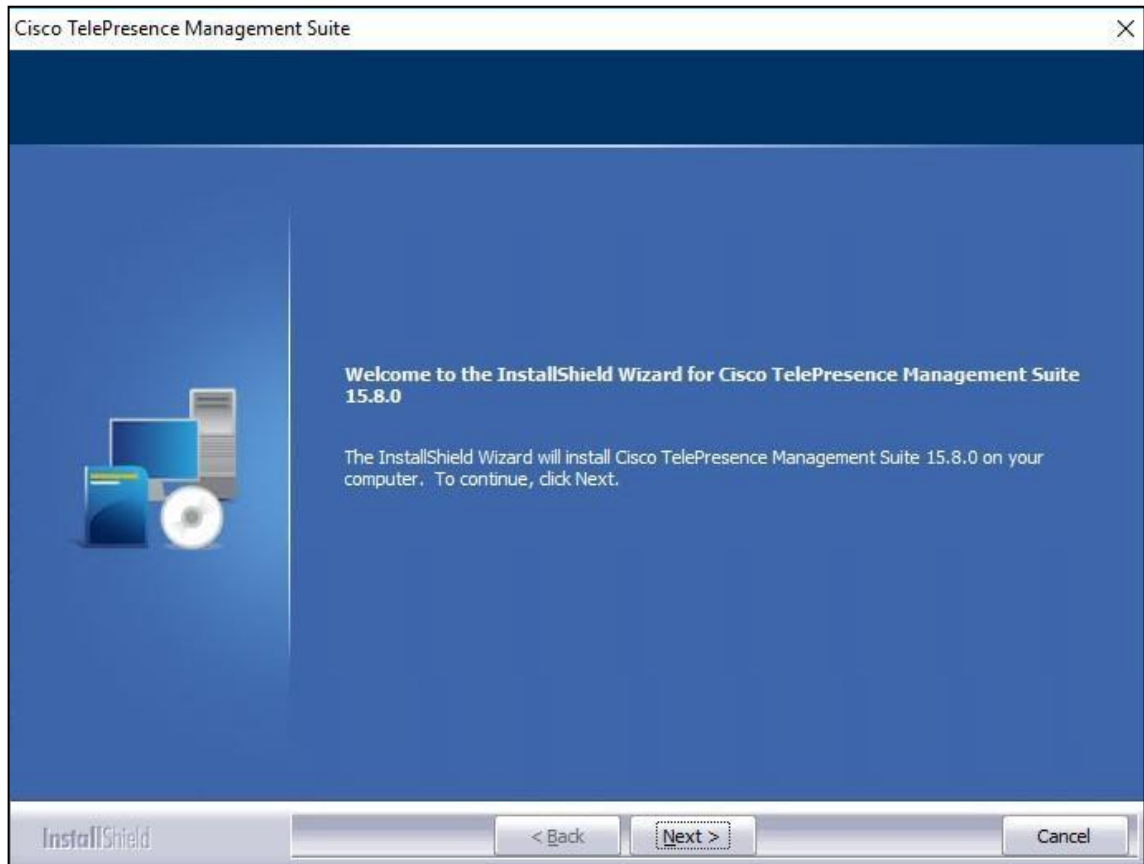
## Cisco TMS のインストールまたはアップグレード



注：両方のオプションを選択した場合、Cisco TMS がインストールされ、続いて Cisco TMS Log Collection Utility がインストールされます。

8. インストーラは、サーバーのハードウェアとソフトウェアの構成をチェックします。サーバの構成によっては、警告またはエラーメッセージが表示される場合があります。プロンプトの指示に従って、不足しているコンポーネントをインストールします。
9. 以前のバージョンの Cisco TMS が現在インストールされている場合は、アップグレードを求めるプロンプトが表示されます。
  - **【はい (Yes)】** をクリックして続行します。アップグレードにより、古いバージョンが削除され、既存の Cisco TMS データベースがアップグレードされます。
  - インストールを中止し、現在のインストールをそのままの状態にしておく場合は、**【いいえ (No)】** をクリックします。

10. **【ようこそ (Welcome)】** 画面が表示されたら、**【次へ (Next)】** をクリックして続行します。

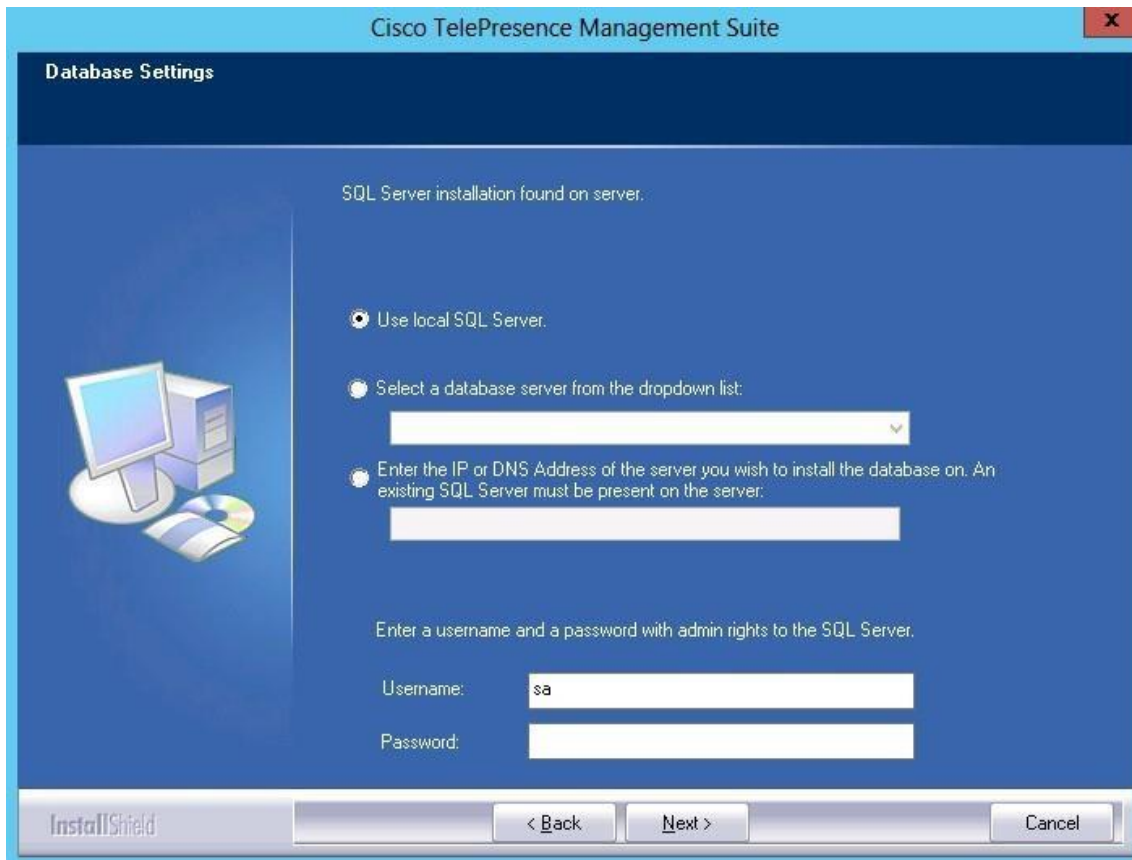


11. **【はい (Yes)】** をクリックしてライセンスに合意します。  
インストーラは、既存の SQL Server および Cisco TMS データベースを検索します。



## Cisco TMS のインストールまたはアップグレード

## データベースの作成またはアップグレード

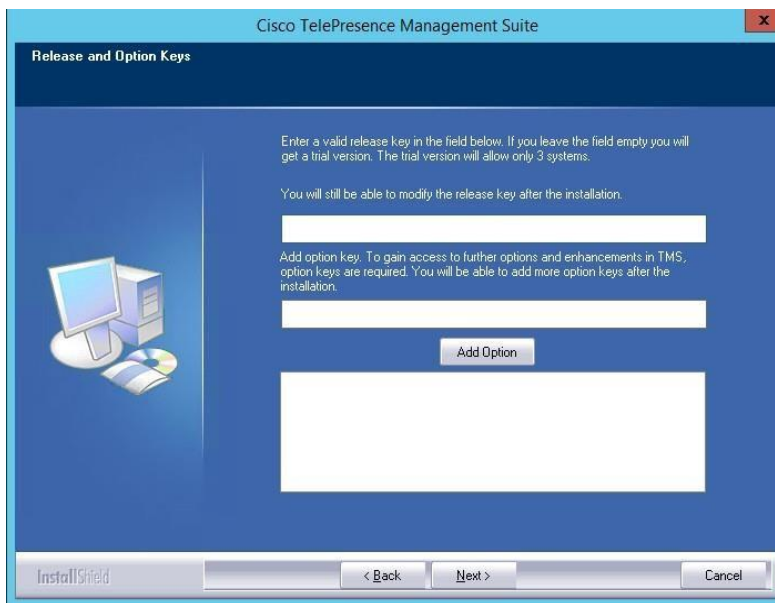


- インストーラが既存の Cisco TMS データベースが見つけず、ローカルにインストールされた SQL Server を見つけた場合は、ユーザー名とパスワードを入力してインストーラが新しいデータベースを作成できるようにします。**[Next]** をクリックします。
- 大規模展開で必要となる外部 SQL Server を使用している場合は、すべての接続の詳細を入力します。**[次へ (Next)]** をクリックします。
- インストーラによって既存の Cisco TMS データベースが見つかった場合は、以前指定した SQL Server の情報がダイアログにすでに入力されています。ユーザ名とパスワードの入力を求められたら、入力して**[次へ (Next)]** をクリックします。
  - 既存のデータベースを最新のバージョンにアップグレードし、既存の情報を保持する場合は**[はい (Yes)]** をクリックします。  
データベースをアップグレードする前に、適切なツールを使用して、データベースをバックアップすることをお勧めします。「[データベースメンテナンス計画 \(24 ページ\)](#)」も参照してください。
  - **[いいえ (No)]** をクリックする場合、同じ SQL Server を使用するには、新しい Cisco TMS データベースをインストールする前に、インストーラを停止し、手動でデータベースを削除する必要があります。

## リリース キーの追加とネットワーク設定の事前設定

ここで**[リリースキーとオプションキー (Release and Option Keys)]** ダイアログが表示され、アップグレードの場合はすべての既存のキーが表示されます。

## Cisco TMS のインストールまたはアップグレード



新規インストールまたは新しいメジャー リリースへのアップグレードを実行する場合は、新しいリリース キーが必要です。リリースキーを入力しない場合は、Cisco TMS の評価バージョンがインストールされます。これには、3 つのシステムのサポートが含まれます。

オプション キーは追加のシステム、拡張、または機能を有効にします。オプションキーは、インストール後に **【管理ツール (Administrative Tools)】 > 【構成 (Configuration)】 > 【一般設定 (General Settings)】** で追加することもできます。

リリースキーまたはオプションキーに関して質問がある場合は、Cisco リセラーまたは Cisco サポートにお問い合わせください。

1. 必要な場合はリリース キーを入力します。  
リリースキーはオプションキーを追加する前に入力する必要があります。
2. オプション キーをそれぞれ入力し、**【オプションを追加 (Add Option)】** をクリックします。  
オプション キーを追加すると検証が行われます。
3. キーの追加が終わったら、**【次へ (Next)】** をクリックします。  
**【ネットワーク設定 (Network Settings)】** 画面が表示されます。

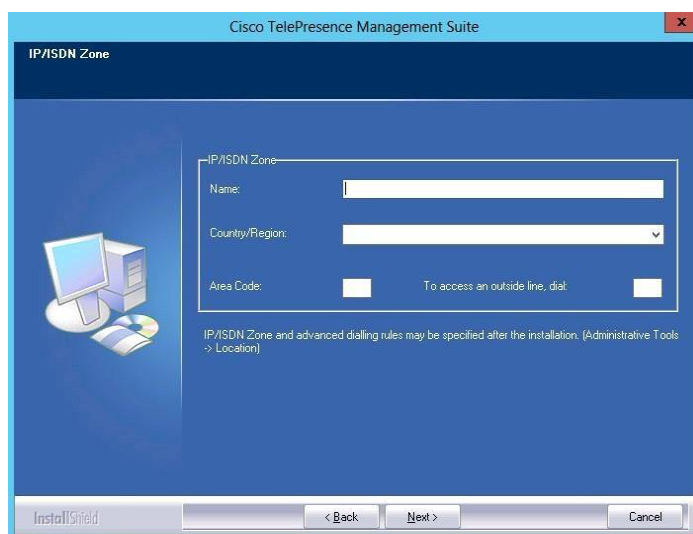
## Cisco TMS のインストールまたはアップグレード

4. ここで、Cisco TMS が基本ネットワーク構成を使用してただちに動作を開始するように、デフォルト設定を事前に設定できます。この設定はインストール後に変更できます。  
アップグレードすると、既存のデータベースの値が表示されます。

フィールド ラベル	説明
<b>TMS サーバ IPv4 アドレス (TMS Server IPv4 Address)</b>	ローカル サーバの IPv4 アドレス。
<b>TMS サーバ IPv6 アドレス (TMS Server IPv6 Address)</b>	ローカル サーバの IPv6 アドレス。IPv6 が Windows Server で有効になっていない場合、このフィールドは空白のままにします。
<b>[IP ブロードキャスト/マルチキャスト アドレス [...]] (IP Broadcast/Multicast Addresses [...])</b>	Cisco TMS で自動的にデバイスを検索するネットワークのブロードキャストアドレス (Cisco TMS が検出したシステムは、管理設定が追加された状態で Cisco TMS に自動的に追加できます)。複数のブロードキャスト アドレスをコンマで区切って入力することもできます。Cisco TMS will は、SNMP ディスカバリパケットを指定アドレスに送信してネットワークを検索します。デフォルト値は、Cisco TMS Server のネットワークのネットワークのブロードキャストアドレスです。  新規インストールでは、デフォルトで Windows SNMP Service は無効であることに注意してください。
<b>TMS でシステムの自動登録を有効化 (Enable automatic registration of systems in TMS)</b>	有効な場合は、Cisco TMS がネットワークで検出したシステムが、Cisco TMS のフォルダに自動的に、追加され、管理設定を構成します。デフォルトでは、この機能はディセーブルになっています。
<b>送信者の電子メールアドレス (Sender E-mail Address)</b>	Cisco TMS が送信するメッセージの <b>[送信者 (From)]</b> フィールドに表示する電子メール。例: videomanagement@example.com.
<b>SMTP サーバ アドレス (SMTP Server Address)</b>	Cisco TMS が電子メール送信に使用する SMTP サーバーのネットワークアドレス。必要に応じて、インストール後に追加の認証設定をセットアップできます。

5. 設定を修正したら、**[次へ (Next)]** をクリックします。  
その後、Cisco TMS は、指定された SMTP サーバーに通信して、設定を検証します。サーバーに通信できない場合は、警告が表示されます。  
新規インストールの場合、**[IP/ISDN ゾーン (IP/ISDN Zone)]** 画面が次に表示されます。

## ゾーンの事前設定とインストール フォルダの場所の設定



## Cisco TMS のインストールまたはアップグレード

ゾーンは、通話のスケジューリングや電話帳の使用の際に、電話番号およびエイリアスをルーティングするために Cisco TMS で使用される構成概念です。

インストール中に入力する情報によって、Cisco TMS に最初の IP ゾーンおよび ISDN ゾーンが作成されます。これらは基本 IP ネットワークおよび ISDN ネットワークがインストール後に動作するための初期デフォルト値として設定されます。複数のロケーションや、より複雑な構成要素を使用するネットワークでは、インストール後にその他のゾーンと構成を追加する必要があります。

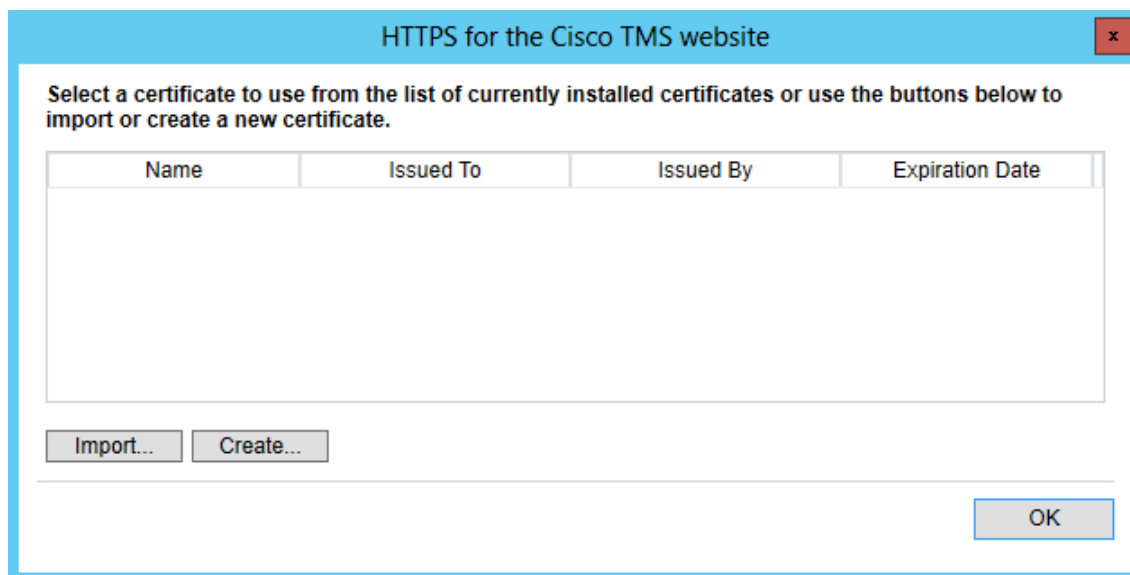
1. 次の説明に従ってゾーン情報を入力します。

フィールド ラベル	説明
名前	ゾーンのわかりやすい名前。通常は、都市や建物を表します。
国/地域	このゾーンが位置する国。
Area Code	この場所の市外局番（該当する場合）。これは ISDN ダイヤリング情報に使われます。
外線にアクセスする場合にダイヤル (To access an outside line, dial)	ISDN 回線で外線を使用する場合に必要なプレフィックス（該当する場合）。

2. 設定を変更したら、[次へ (Next)] をクリックします。  
[フォルダ設定 (Folder Settings)] 画面が表示されます。
3. Cisco TMS のインストールパスを指定し、[次へ (Next)] をクリックします。  
[暗号化キー (Encryption Key)] 画面が表示されます。
4. Cisco TMS データベース内のシステムユーザー名とパスワードのデータを暗号化する新しいキーを作成するために、[生成 (Generate)] をクリックします。または、必要に応じて、Cisco TMS の以前のインストールから既存のキーを追加します。[次へ (Next)] をクリックします。  
[ファイルのコピーの開始 (Start Copying Files)] 画面が表示されます。
5. 表示された要約のすべての設定を確認し、[次へ (Next)] をクリックします。  
インストール プロセスが始まります。

## 証明書の追加

インストールが完了したら、Cisco TMS Web サイトへの HTTPS アクセスができるようにするために、TLS 証明書をインポートするか、または作成します。テスト環境にインストールする場合を除いて、信頼できる CA からの正式な証明書を使用することを強くお勧めします。

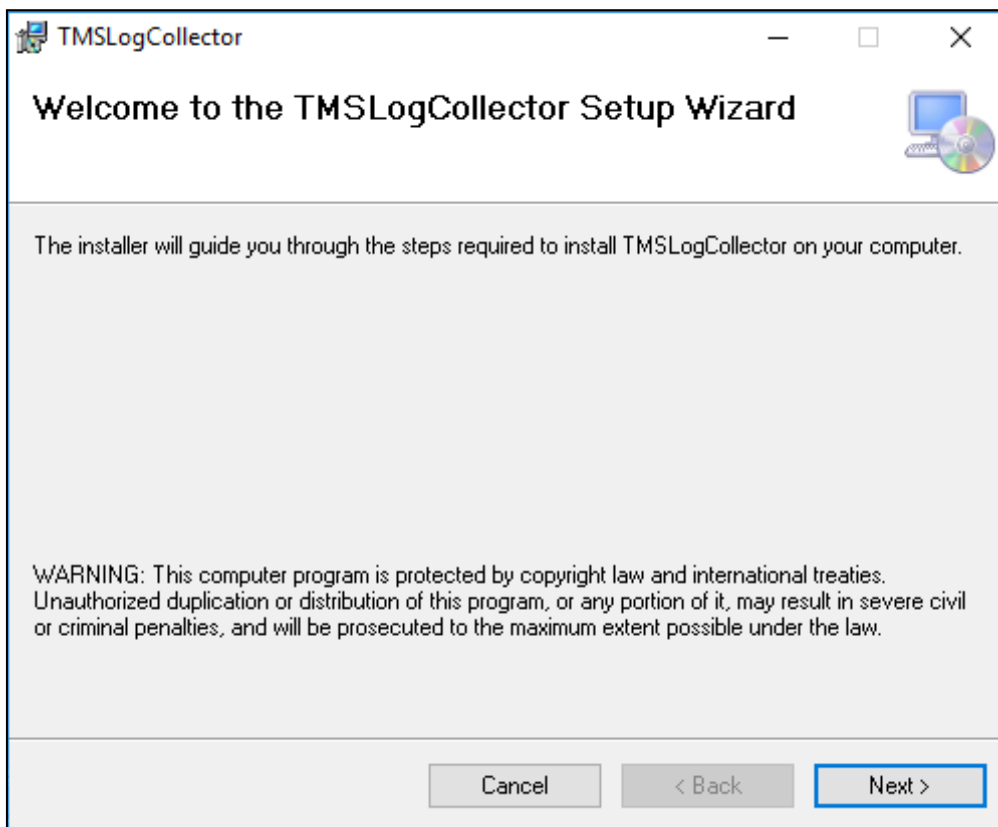


## Cisco TMS のインストールまたはアップグレード

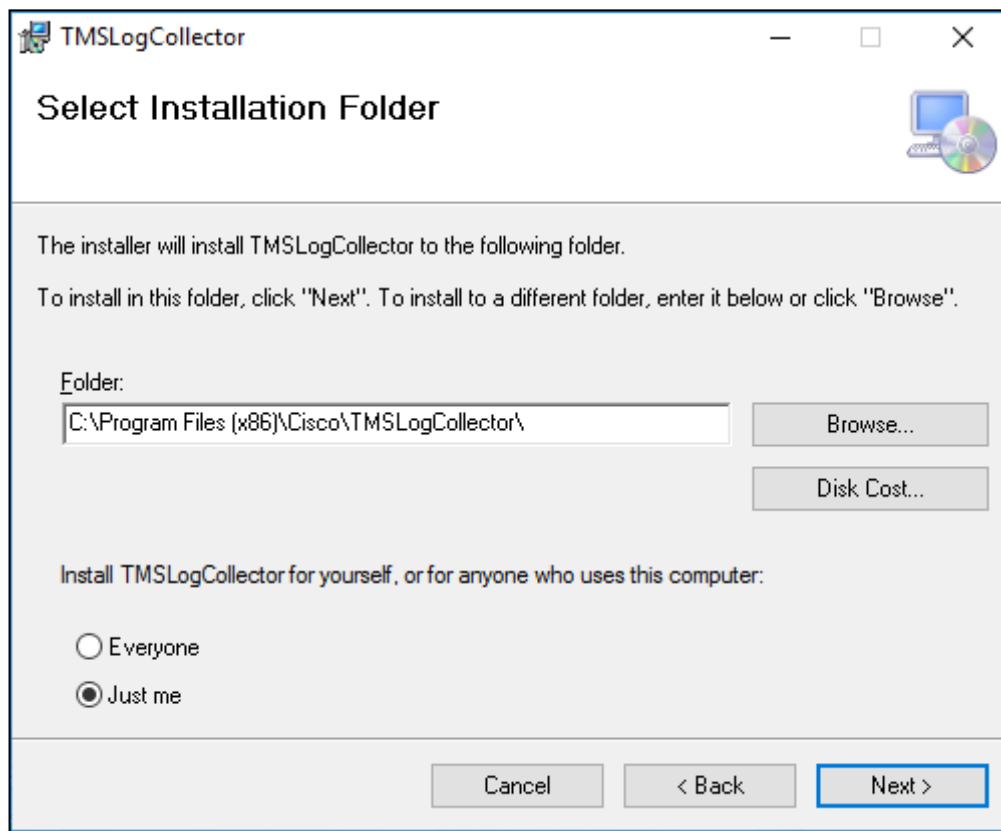
1. **【インポート (Import)】** をクリックして .pfx 形式の既存の証明書を追加するか、**【作成 (Create)】** をクリックして自己署名証明書を作成します。
2. インポートが完了したら、**【OK】** をクリックします。
3. セットアップ ウィザードを終了します。**【Finish】** をクリックします。
4. 必要な場合は、サーバをリブートするように求められます。

## Cisco TMS Log Collection Utility のインストール

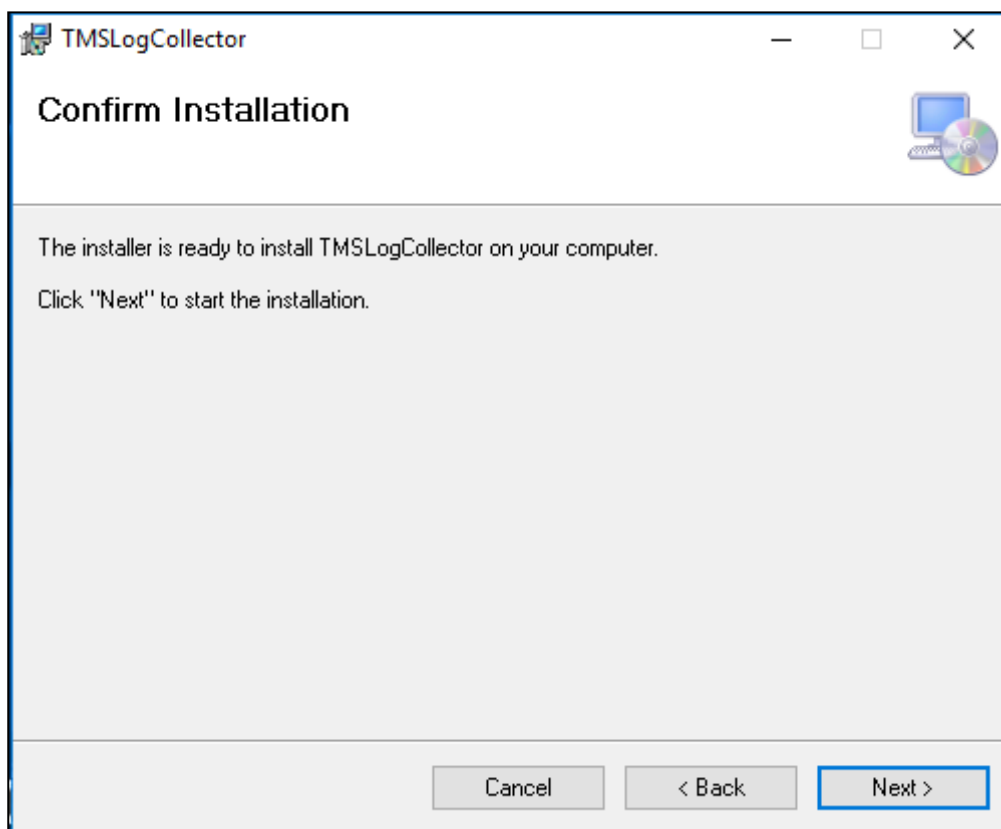
1. Cisco TMS のインストールが完了すると、Cisco TMS Log Collection Utility のインストール ダイアログボックスが表示されます。Cisco TMS Log Collection Utility のインストールの開始方法の詳細については、「[インストーラの実行 \(28 ページ\)](#)」の **ステップ 4** を参照してください。**【次へ (Next)】** をクリックして続行します。



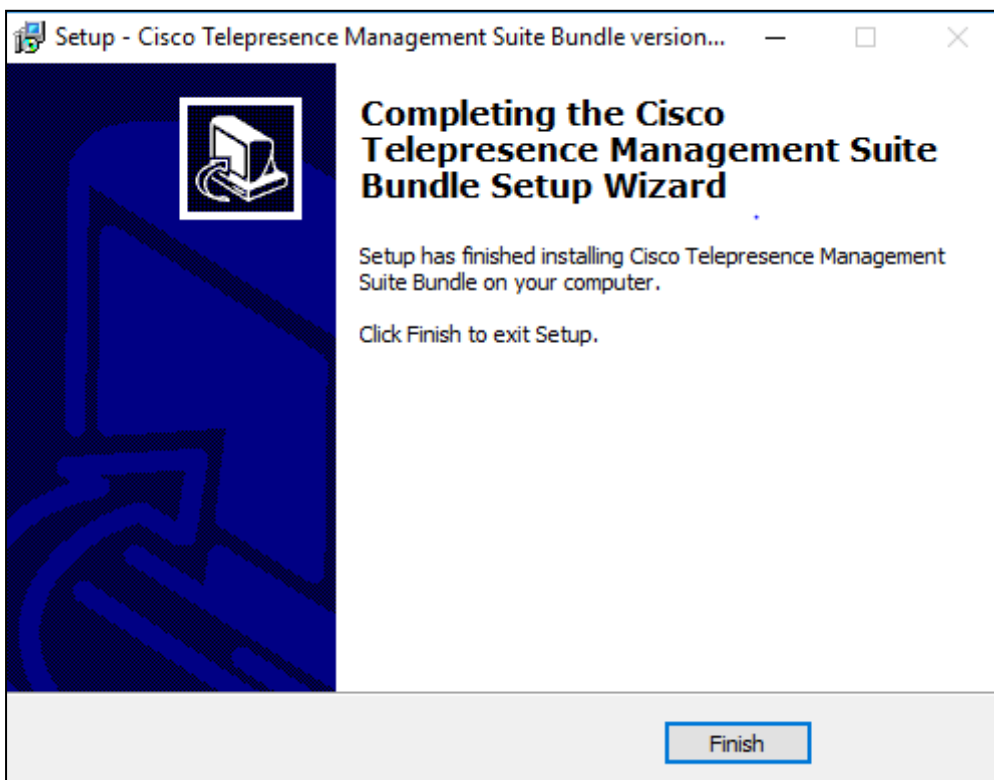
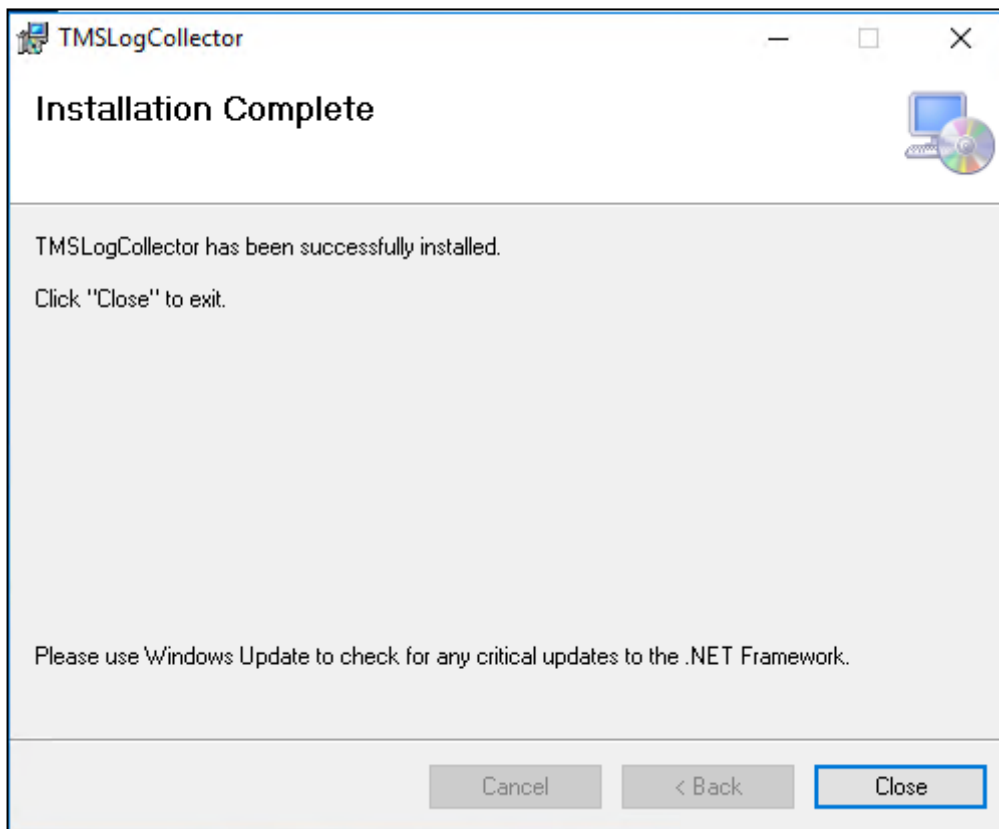
2. Cisco TMS Log Collection Utility をインストールするディレクトリ/フォルダを参照します。自分用または全員用に Cisco TMS Log Collection Utility をインストールする場合は、オプションを選択します。**【次へ (Next)】** をクリックして続行します。



3. [次へ (Next) ] をクリックしてインストールを開始します。



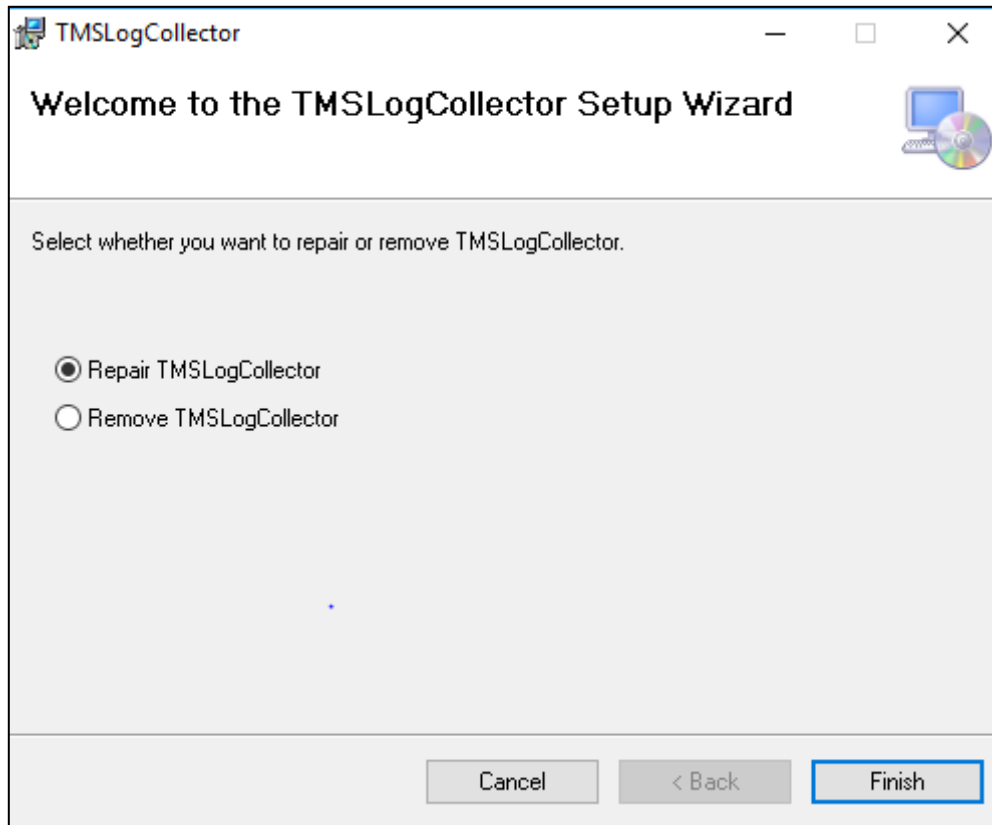
4. インストールが正常に完了したら、**[閉じる (Close)]** をクリックして終了します。





## Cisco TMS のインストールまたはアップグレード

注：両方のアプリケーションがすでにインストールされている状態で、ユーザーがインストーラパッケージを再度実行しようとすると、Cisco TMS は元の動作に従って動作します。ただし、Cisco TMS Log Collection Utility の場合、Cisco TMS Log Collection Utility を修復または削除するためのダイアログボックスが表示されます。



## Windows SNMP Service の有効化

Cisco TMS の新規インストールの場合、Windows SNMP Service はデフォルトで無効になっています。SNMP を必要とするレガシー装置を使用している場合は、インストール後にこのサービスを有効にできます。

## Cisco TMS への初回アクセス

Cisco TMS をインストールしたら、ブラウザを使用して Web インターフェイスにアクセスします。

1. 以下のいずれかを実行。
  - Windows の **[スタート (Start)]** メニューの Cisco プログラムグループにあるショートカットを使用します。
  - Web ブラウザの URL フィールドに `https://<serveraddress>/tms` と入力します。<serveraddress> には、ホスト名（推奨）か IP アドレスを入力します。ホスト名を使用すると、アクティブディレクトリによる統合認証に対応します。

## Cisco TMS のインストールまたはアップグレード

2. サーバーコンソールから Web サイトにアクセスする場合は、通常、現在ログインしているユーザー名で自動的に認証が行われ、Cisco TMS が開きます。そうでない場合は、認証情報の入力を求められます。ほとんどのブラウザでは、ログイン ウィンドウにユーザ名とパスワードの 2 つのフィールドが表示されます。ユーザ名の入力方法は、使用している Windows アカウントの種類によって異なります。

フィールド	説明	例
<b>[ドメイン ユーザー (Domain Users) ]</b>	[ユーザ名 (Username) ]は「domain\username」の形式で入力する必要があります。username@<Domain DNS name> の形式も使用できますが、あまり使用されていません	corp\firstname.lastname
<b>ローカル Windows アカウント</b>	ユーザ名は次の形式で入力する必要があります : 「machinename\username」	tms-2\administrator

3. 正常に認証されると、**[個人情報の編集 (Edit Personal Information) ]** というウィンドウがポップアップします。このウィンドウが表示されない場合は、ブラウザのポップアップブロックのアラートを見つけ、Cisco TMS のポップアップブロックを無効にします。
4. 詳細を入力し、**[個人情報を更新する (Update Your Personal Information) ]** をクリックします。





# 冗長展開の設定

Cisco TMS は、アプリケーションの可用性を向上させる冗長構成を使用した展開をサポートしています。

この章では、2 つのサポートされている冗長性シナリオでの Cisco TMS の展開に関する要件、構成、および制限について説明します。

この章は、Cisco TMS、Cisco TMS のインストール、および Windows Server オペレーティングシステムについて理解しており、コンピュータ ネットワーキングとネットワークプロトコルに関する高度な知識を持っている方を対象としています。

事前情報	44
ロード バランサを使用した展開	45
ホット スタンバイの展開	51
バージョン 14.4 以降からの冗長展開のアップグレード	54
バージョン 14.4 より前の Cisco TMS からの冗長展開のアップグレードを行う	54
ACE 構成の例	55
F5 BIG-IP の設定例	56
同期用ローカル ファイル	59

## 事前情報

### サポートされている構成

自動フェールオーバープロセスを備えた完全冗長 Cisco TMS 展開では、前面にネットワークロードバランサ (NLB) を備えた 2 台の Cisco TMS Server を設定する必要があります。新しく展開する場合、2 台の Cisco TMS Server 間における IP トラフィックのロードバランシングを行うには F5 BIG-IP ロードバランサを使用することをお勧めします。このため、このドキュメントでは、Cisco TMS を F5 BIG-IP アプライアンスとともに展開する方法について説明します。Cisco ACE 4710 Application Control Engine アプライアンスの使用もサポートされています。ACE ロードバランサを使用して、以前の冗長モデルからこの改善されたモデルへの移行についての詳細については、「[14.4 以前の Cisco TMS バージョンから冗長展開をアップグレード \(54 ページ\)](#)」を参照してください。

この章では、ホットスタンバイモデルを使用して 2 台の Cisco TMS Server を展開する方法についても説明します。

2 つの冗長性モデルのどちらを展開するかに関係なく、3 台以上の Cisco TMS Server を使用することはできません。Cisco は、冗長設定における 3 台以上の Cisco TMS Server の展開は、テストしておらず、サポートもしていません。

2 つの Cisco TMS Server を展開すると、Cisco TMS の可用性が向上しますが、Cisco TMS の拡張性は向上しません。

代替構成を使用したその他のモデルのロードバランサも Cisco TMS で動作する可能性はありますが、Cisco によるテストは行われていません。

## ライセンス

冗長 Cisco TMS 実装で利用できるライブデータベースは 1 つだけです。このため、両方のサーバーでは同じ Cisco TMS シリアル番号、および同じリリースキーとオプションキーのセットを使用します。

## 冗長展開の設定

## データベースの冗長性

Cisco TMS は、SQL データベースに大きく依存しているため、完全な耐障害性 Cisco TMS ソリューションは、SQL Server 2012 が提供する高可用性技術の 1 つも使用します。

## Cisco TelePresence Management Suite Provisioning Extension

冗長環境での Cisco TMSPE の実装については、『[プロビジョニング拡張機能展開 ガイド](#)』を参照してください。

## ロード バランサを使用した冗長展開の制限

Cisco TMS 環境に冗長性を実装する場合は、次のことに注意してください。

- システムのシステム接続の自動更新 ([**管理ツール (Administrative Tools)**] > [**構成 (Configuration)**] > [**ネットワーク設定 (Network Settings)**] > [**システムのシステム接続性の更新 (Update System Connectivity for Systems)**]) は、冗長環境では無効となります。
- 電話帳と アクティブディレクトリの同期などのタスクは、次の場合にフェールオーバーが実行されると失敗する可能性があります。
  - タスクの実行中。
  - タスクの実行がスケジュールされている直前。
- 割り当てと接続の再試行の頻度によって、会議がフェールオーバー中に影響を受けることはありません。
- 独自の予約クライアントまたはサードパーティのクライアントを使用している場合、Cisco TMSBA のバージョン 13 で導入されているクライアント セッション メカニズムを使用する必要があります。詳細については、『[Cisco TMS Booking API プログラミング リファレンス ガイド](#)』を参照してください。

## ロード バランサを使用した展開

ネットワークロードバランサ (NLB) を使用して 2 台の Cisco TMS Server (この場合は「ノード」とも呼びます) を構成すると、完全な自動フェールオーバーを備えた、真に冗長性のある Cisco TMS セットアップが実現します。

## 推奨ハードウェア

新しく展開する場合は、F5 BIG-IP ロード バランサを使用することをお勧めします。現在は Cisco ACE 4710 アプリケーション コントロール エンジン アプライアンスの使用もサポートされていますが、このロードバランサは将来のバージョンの Cisco TMS ではサポートされなくなります。

## Active Directory およびユーザ認証の要件

- 両方の Cisco TMS Server は同じ Windows ドメインのメンバーである必要があります。
- すべての Cisco TMS ユーザーは、Active Directory を使用してインポートし、認証する必要があります。
- この冗長性モデルでは、ローカル ユーザ アカウントの使用はサポートされません。

## 概要

## ノード

Cisco TMS ネットワークロードバランサ (NLB) の内部に展開されると、クラスター対応アプリケーションになります。2 台の Cisco TMS Server を同じ tmsng データベースに接続して、[**管理ツール (Administrative Tools)**] > [**構成 (Configuration)**] > [**一般設定 (General Settings)**] で冗長性を有効にした場合、片方のサーバーはただちにアクティブ ノードになり、もう片方はパッシブノードになります。アクティブにできるノードは、常に 1 つだけです。

アクティブノードの動作は、スタンドアロンの Cisco TMS Server と完全に同じです。

パッシブ ノードの動作は以下のとおりです。

- Web ページとサービスがロック ダウンされたスタンバイ モードのままになります。
- ユーザおよび管理対象システムからのすべての着信トラフィックを拒否します。

## 冗長展開の設定

ノードがパッシブである間は、Cisco TMS の全体のパフォーマンスをパッシブノードがほとんど変化させないように、tmsng データベースへのトラフィックは最小限に抑えられます。

## フェールオーバー

ノードのステータスがパッシブとアクティブ間で切り替わるプロセスは、フェールオーバーと呼ばれます。フェールオーバーは、自動的に起きる場合も、管理者によって手動で開始される場合もあります。

自動フェールオーバーは、以下のいずれかの場合に行われます。

- アクティブ ノードが、自身のサービスの応答がないか、無効化されていることを検出した場合。
- パッシブノードが、アクティブ ノードのサービスの応答がないか、無効化されていることを検出した場合。

フェールオーバーが開始されると、それまでパッシブであったノードはすぐにアクティブに変更され、同時にそれまでアクティブであったノードは、自身のサービスと Web インターフェイスをスタンバイ モードへと後退させます。この変更が NLB に検出されるまでには最大で 1 分かかる可能性があり、この間、Cisco TMS はほとんど利用不可能になります。このため、手動フェールオーバーの開始は、通常の業務時間外に限って行う必要があります。

Cisco TMS は単純な計数メカニズムを使用して、自動フェールオーバーを開始すべきかどうかを決定します。そのプロセスは次のとおりです。

1. アクティブノードとパッシブノードの両方の各 Cisco TMS サービス (IIS を含む) は、最後に機能していた時期を示すキープアライブ通知を tmsng データベースに連続的に書き込みます。
2. アクティブ ノードはこのサービスとタイムスタンプのリストを監視し、過去 1 分間に通知を送信したサービスを使用可能であると分類します。アクティブ ノードは、自身よりもパッシブ ノードの方が多くのサービスを使用中であるとみなした場合に、制御を回収してパッシブ ノードに渡します。その後、パッシブ ノードがアクティブになります。
3. フォールバック メカニズムと同様に、パッシブ ノードもタイムスタンプを監視し、アクティブ ノードがキープアライブ通知の書き込みを停止した場合にフェールオーバーを強制的に開始します。

## ネットワーク ロード バランサ

NLB は両方のノードのステータスを監視して、すべての着信トラフィックをアクティブ ノードにのみ転送します。フェールオーバーが行われた場合を除いて、着信トラフィックがパッシブノードに転送されることはありません (「[概要 \(45 ページ\)](#)」) を参照してください。

ノードのステータスを監視するには、([**管理ツール (Administrative Tools)**] > [**TMS サーバ メンテナンス (TMS Server Maintenance)**]) に表示される) 特定の URL を 5 秒ごとに両方のノードで検出するように、NLB を設定する必要があります。Cisco TMS の両方のノードが自身へのアクセス頻度の記録を保持するため、この URL の精査は別の目的にも役立ちます。ノードは、この URL へのプローブ要求の受信を停止した場合、NLB と自身の間のネットワーク リンクがダウンしたとみなして、その IIS サービスを非アクティブであるとマークします。これがアクティブ ノードで起きた場合、上記のようにフェールオーバーが作動されます。

## ネットワーク トポロジおよび管理対象システムとの通信

ユーザーおよび管理対象システムからの着信ネットワーク トラフィックは、NLB を経由して Cisco TMS Server にルーティングされます。仮想 IP アドレス (VIP) を NLB に割り当てるとともに、NLB の VIP を指す DNS レコードを作成する必要があります。その後、VIP (または関連付けられた DNS レコード) を、すべての管理対象システムの管理アドレスとフィードバック アドレスとして使用します。

NLB のホスト名と IP アドレスは、[Cisco TMS] > [**管理ツール (Administrative Tools)**] > [**構成 (Configuration)**] > [**ネットワーク設定 (Network Settings)**] > [**内部 LAN のシステムの高度なネットワーク設定 (Advanced Network Settings for Systems on Internal LAN)**] および [**パブリックインターネット上/ファイアウォールの背後のシステムの高度なネットワーク設定 (Advanced Network Settings for Systems on Public Internet/Behind Firewall)**] に入力する必要があります。

[**ネットワーク設定 (Network Settings)**] の IP アドレスとホスト名の値が変更されると、データベース スキャナ サービスがこれらの新規ネットワーク設定を管理対象のシステムに適用します。その後、システムは NLB へのトラフィックの転送を開始し、NLB はこれらの要求を Cisco TMS Server に転送します。

Cisco TMS 事態のサービスからの発信トラフィックは NLB を経由しないため、Cisco TMS のアクティブノードは、システムを管理するときに NLB をバイパスします。このため、IP プロトコルヘッダーに基づいてシステムの接続設定とパラメータを自

## 冗長展開の設定

動更新する Cisco TMS のロジックは、Cisco TMS の冗長性が有効化されると無効になります。Cisco TMS が管理対象システムと通信する方法の詳細については、『Cisco TMS 管理者ガイド』の「システム管理の概要」の章を参照してください。

冗長性のある Cisco TMS ソリューションの導入後にネットワークに重大な変更を行った場合、Cisco TMS と管理対象システム間のシステム接続がネットワークの変更後も機能していることを手動で検証する必要があります。接続を検証する必要がある変更の例としては、管理対象システムと Cisco TMS の間への新しいプロキシの導入が挙げられます。

この構成の実装方法については、「ロードバランサの展開 (45 ページ)」を参照してください。

## アーキテクチャの概要およびネットワーク構成図

## 構成例

下記の例では、次の値を使用します。

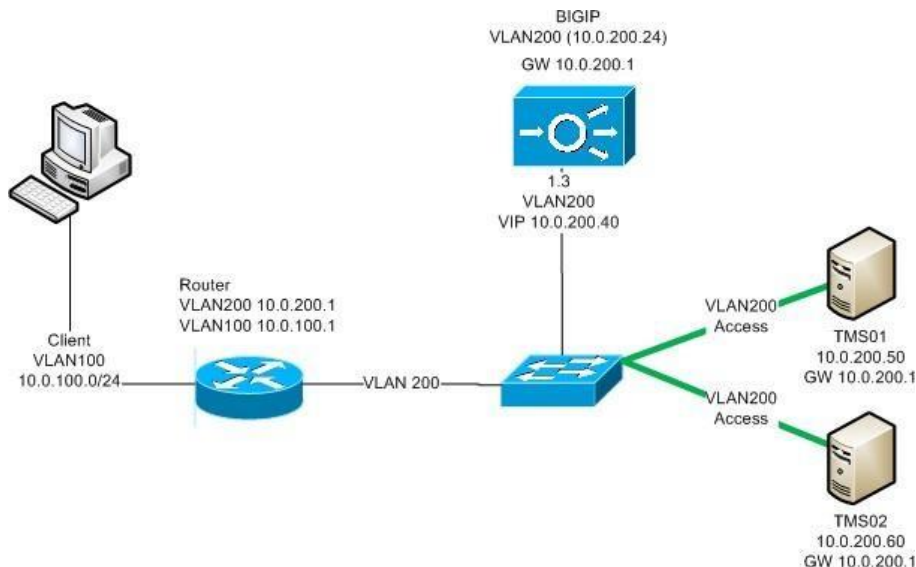
表 2 VLAN200

デバイス	IP アドレス	Hostname
F5 BIG-IP 仮想 IP アドレス	10.0.200.40	tms.example.com
tms01	10.0.200.50	tms01.example.com
tms02	10.0.200.60	tms02.example.com

表 3 VLAN100

デバイス	IP アドレス	Hostname
管理対象システムおよびユーザ	10.0.100.0/24	

- 仮想 LAN には VLAN200 と VLAN100 の 2 つがあります。
- F5 BIG-IP は VLAN200 上に設定されています。
- 2 台の Cisco TMS Server (10.0.200.50 の tms01 および 10.0.200.60 の tms02) は VLAN200 上に設定されています。
- すべてのクライアント (管理対象システムおよびユーザ) は VLAN100 上に設定されています。
- F5 BIG-IP の仮想 IP アドレスへのトラフィックはすべて、2 台の Cisco TMS Server の 1 つに転送されます。
- すべての管理対象システムとユーザーは、Cisco TMS との通信時に F5 BIG-IP の仮想 IP アドレスを使用します。
- 2 台の Cisco TMS Server は、共通の外部 tmsng データベースを共有しています。





## 冗長展開の設定

## インストールと設定

## Cisco TMS を tms01 にインストールする

1. Installing をインストールする前に、外部サーバーに SQL Server インスタンスを設定します。
2. 「[インストーラの実行 \(28 ページ\)](#)」に記載されている手順に従って、Cisco TMS を 1 つ目のノードにインストールします。
3. Cisco TMS が外部データベースサーバーを差すようにします。
4. インストール中に生成される暗号キーを書き留めておきます。
5. インストール時に HTTPS を有効にする場合は、tms.example.com [英語] に発行された証明書を使用します。
6. ログインして、Cisco TMS Web アプリケーションが正常に機能しているかを確認します。
7. **[管理ツール (Administrative Tools)] > [一般設定 (General Settings)] > [TMS の冗長性の有効化 (Enable TMS Redundancy)]** の順に選択し、**[はい (Yes)]** を選択します。

この設定を、**[はい (Yes)]** にすると、**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)] > [システムのシステム接続性の更新 (Update System Connectivity for Systems)]** の設定が自動的に無効化されるのでご注意ください。

## Cisco TMS を tms02 にインストールする

1. サービス パック レベルも含めて、tms02 のオペレーティング システムが tms01 と完全に同じであることを確認します。
2. 両方のサーバが同じタイムゾーンに設定されていること、および時計が同期されていることを確認します。
3. tms01 の設定時と同じ外部データベースサーバーとインストールディレクトリを使用して、Cisco TMS をインストールします。同じバージョンの Cisco TMS をインストールします。
4. tms01 へのインストール中に生成された暗号キーを入力します (暗号キーを上記のステップ 4 で書き留めていない場合は、**tms01** の **[TMS ツール (TMS Tools)]** の **[セキュリティ設定 (Security Settings)]** で確認できます)。
5. Cisco TMS にログインします。Cisco TMS が使用できないことを示すエラーが表示されます。

## 手動フェールオーバーのテスト

1. tms01 の IP/ホスト名にアクセスします。
2. **[管理ツール (Administrative tools)] > [TMS サーバーメンテナンス (TMS Server Maintenance)] > [TMS の冗長性 (TMS Redundancy)]** の順に選択します。
3. どちらのノードがアクティブであるかを記録し、**[アクティブ ノードのリタイア (Retire Active Node)]** をクリックします。
4. Cisco TMS Web ページを更新します。
5. *「Cisco TMS が利用できません (Cisco TMS is unavailable)」* というエラーが表示されれば成功です。
6. tms02 の IP/ホスト名にアクセスします。  
もう片方のノードがアクティブになっていることが表示されれば成功です。Cisco TMS にアクセスできます。

## ネットワーク ロード バランサの設定

第 2 ノードが動作可能になったら、ネットワーク ロード バランサを設定します。

1. HTTP 接続と HTTPS 接続、および SNMP トラップをアクティブ ノードに転送するように NLB を設定します。
2. Polycom の電話帳を動作させるために、TCP ポート 3601 をアクティブ ノードに転送するように NLB を設定します。
3. プローブ URL をプローブするように NLB を設定します。
  - a. 両方のノードの Cisco TMS で **[管理ツール (Administrative Tools)] > [TMS サーバーメンテナンス (TMS Server Maintenance)] > [TMS の冗長性 (TMS Redundancy)] > [プローブ URL (Probe URL)]** に表示される URL をプローブするように、NLB を設定します。これらの URL は、積極的 (可能であれば 5 秒ごと) にプローブする必要があります。
  - b. すべてのトラフィックをアクティブ ノード (HTTP 200 に応答する方のノード) にプッシュします。



## 冗長展開の設定

注：プローブ URL は、その他のモニタリング アプリケーションにモニタされないようにしてください。

F5 BIG-IP の構成については、「[F5 BIG-IP の設定例 \(56 ページ\)](#)」を参照してください。

## Cisco TMS の構成

アクティブ ノードで次の操作を実行します。

1. Cisco TMS アプリケーションでは、**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)]**。
2. 次の IP アドレスとホスト名を、NLB の仮想 IP アドレスとホスト名に変更します。
  - **[イベント通知 (Event Notification)] > [SNMP トラップホスト IP アドレス (SNMP Traphost IP Address)]**
  - **内部 LAN のシステムの高度なネットワーク設定**：すべてのフィールド
  - **パブリック インターネット/ファイアウォールの外側のシステムに対する高度なネットワーク設定 (AAAdvanced Network Settings for Systems on Public Internet/Behind Firewall)**

両方のノードで次の手順を実行します。

Cisco TMS Server のブラウザを使用していくつかの管理対象システムの Web インターフェイスにアクセスし、Cisco TMS Server が管理対象システムに到達できること、およびその逆も可能かどうかを確認します。

## ローカル ファイルの同期

Cisco TMS によって使用されるカスタマイズ可能なファイルの中には、tmsng データベース内ではなく Windows Server のローカル ファイルシステム内に保存されるものがあります。これらのファイルが保存されるフォルダは、2 つのサーバ間で同期させる必要があります。同期させる必要があるすべてのフォルダのリストについては、「[同期するローカル ファイル \(59 ページ\)](#)」を参照してください。

Cisco TMS は、ファイル同期プロセスを維持しません。サードパーティ製ツールを使用する必要があります。ファイル/フォルダの同期の適切な構成に関する情報については、サードパーティ製ツールのドキュメントを参照してください。

## オプション：TLS クライアント証明書の使用の有効化

TLS クライアント証明書を導入時に使用する場合、以下を確認する必要があります。

- 2 つのサーバの Cisco TMS ツールで同じオプションが選択されます。
- 2 つのサーバにインポートされた TLS 証明書が同じである。
- 2 つのサーバで同じ証明書の失効メカニズムを使用している。

詳細については、『[Cisco TMS 管理者ガイド](#)』の「Cisco TMS ツール」章を参照してください。

## フェールオーバーの動作のテスト

1. NLB の VIP を使用して Cisco TMS にログインします。
2. 手動フェールオーバーを強制実行します。
3. 1 分間待ってから、ブラウザを更新します。
4. **[管理ツール (Administrative Tools)] > [TMS サーバ メンテナンス (TMS Server Maintenance)] > [TMS の冗長性 (TMS Redundancy)]** に移動し、**[フェールオーバーのアクティビティ ログ (Failover Activity Log)]** を見て、フェールオーバーが実際に行われたことを確認します。

## Cisco TMS のアップグレード

最新のソフトウェアバージョンへの Cisco TMS のアップグレードを行うと、短時間ではあるもののユーザーが Cisco TMS を使用できなくなるので、アップグレードはメンテナンス期間中に実行します。

2 台の Cisco TMS ノードは共通のデータベースを共有しているため、常に同じソフトウェアバージョンを実行する必要があります。したがって、一度に 1 つのノードをアップグレードし、もう片方のノードをシステムとユーザに対して動作可能である状態に保つことは不可能です。

## 冗長展開の設定

1. 両方の Cisco TMS Windows Server にログインします。
2. ファイル レプリケーションを無効化して、ローカル ファイルの同期を一時的に停止します。 [SEP]
3. 両方のノードで、すべての TMS サービスおよび IIS サービスを停止します。
4. 一方のノードを新しいソフトウェア バージョンにアップグレードします。これにより、tmsng データベースがアップグレードされます。
5. このサーバーの Cisco TMS Web アプリケーションにログインして、正常に動作していることを確認します。

NLB のプローブが、アップグレードしたサーバがアクティブ ノードであると認識するようになります。ユーザーと管理対象システムは、Cisco TMS を再び使用できるようになります。

1. 2 番目の Cisco TMS ノードをアップグレードします。
2. インストーラはデータベースがアップグレード済みであることを検出し、更新されたデータベースの使用を継続するよう求めます。[はい (Yes)] を選択します。インストーラは次にバイナリを更新しますが、データベースはそのままにします。
3. アクティブサーバーの Cisco TMS Web アプリケーションにログインし、手動フェールオーバーを強制実行します。2 番目のサーバが 1 分以内にアクティブになることを確認します。
4. ファイル レプリケーションを有効化します。

ネットワーク設定がインストール プロセス中に変更されていないことを確認します。

1. Cisco TMS アプリケーションでは、[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)]。
2. 次の IP アドレスとホスト名が NLB の仮想 IP アドレスとホスト名に設定されていることを確認します。
  - [イベント通知 (Event Notification)] > [SNMP トラップホスト IP アドレス (SNMP Traphost IP Address)]
  - 内部 LAN のシステムの高度なネットワーク設定：すべてのフィールド
  - パブリック インターネット/ファイアウォール外のシステムの詳細ネットワーク設定 (Advanced Network Settings for Systems on Public Internet/Behind Firewall)

## ノードに障害が発生した場合のリカバリ

サーバ障害の場合、緊急措置は必要ありません。パッシブ ノードがダウンした場合、アクティブ ノードは通常どおりに動作を続けます。アクティブ ノードがダウンした場合、パッシブ ノードが自動的にアクティブになるとともに、NLB が障害を検出し、すべてのトラフィックを新しくアクティブになったノードに転送します。

フェールオーバーの実行には約 1 分の遅れが予想されます。この間、Web ページには「Cisco TMS に接続できません」というエラーが表示されます。

故障したノードのソフトウェアとハードウェアのトラブルシューティングを通常どおり実行し、動作可能になったらオンラインに戻します。

## 冗長展開の管理対象システムのトラブルシューティング

Cisco TMS アクティブサーバーの Wireshark トレースをキャプチャすると、NLB から入ってくるすべての着信トラフィックが表示されます。したがって、Cisco TMS と目的の管理対象システム間の通信を簡単に特定することはできません。

トラブルシューティングを開始する前に、次の手順を実行します。

1. 調査するすべてのシステムの管理アドレスを、一時的に Cisco TMS アクティブサーバーのアドレスに設定します。
2. Wireshark キャプチャを行います。
3. トレースが完了したら、すべてのシステムの管理アドレスを NLB のアドレスに戻します。

## ログ

- ログファイルは両方の Cisco TMS Server から収集する必要があります。
- ログ レベルを変更する場合は、両方のサーバで行うようにしてください。ログレベルを上げ、問題を再現してからすぐに元のログレベルに戻すなど、ごくわずかな時間だけログレベルを変更する場合はこの必要はありません。

## 冗長展開の設定

## ホット スタンバイの展開

障害に備えて追加の Cisco TMS Server をウォームスベアとして保持することは、「ホットスタンバイ」冗長性モデルと呼ばれます。これは、Cisco TMS プライマリサーバーに障害が発生した場合に手動による介入が必要になるため、フェールオーバー ソリューションではなくスイッチオーバー ソリューションです。

この冗長性モデルでは、常に 1 台の Cisco TMS Server がアクティブです。ホット スタンバイ サーバは、プライマリ サーバが故障した場合に数分以内にアクティブ化できるように、セキュリティ パッチとその他のアップグレードを使用して最新に保つ必要があります。

ホットスタンバイ冗長モデルでは tmsng データベースを外部 SQL Server に配置する必要があること、および 2 台の Cisco TMS Server が同じ Windows ドメイン内にある必要があることに注意してください。

この展開では、**[一般設定 (General Settings)] > [TMS 冗長性の有効化 (Enable TMS Redundancy)]** を使用して冗長性を有効化することはしないでください。

下記の手順では、次の例を使用します。

サーバ	DNS Name	IP アドレス
プライマリ Cisco TMS Server (tms01)	tms01.example.com	10.0.0.10
セカンダリ Cisco TMS Server (tms02)	tms02.example.com	10.0.0.11

これらの例では、IPv4 を使用することを前提としています。IPv6 も使用している場合は、IPv6 アドレスを適宜変更します。

## プライマリ Cisco TMS Server の設定

Cisco TMS をインストールする前に、次の手順を実行します。

1. 外部サーバに SQL サーバ インスタンスを設定します。
2. プライマリ サーバ tms01 の IP アドレス (10.0.0.10) を指すように、DNS レコード tms.example.com を設定します。

Cisco TMS のインストール：

1. 『Cisco TMS インストールおよびスタートアップガイド』に記載されている手順に従って、tms01 に Cisco TMS をインストールし、Cisco TMS が上記のステップ 1 で使用した外部データベースサーバーを指すように設定します。
2. インストール中に生成される暗号キーを書き留めておきます。
3. インストール時に HTTPS を有効にする場合は、tms.example.com [英語] に発行された証明書を使用します。
4. ログインして、Cisco TMS Web アプリケーションが正常に機能しているかを確認します。

すべてのユーザーと管理対象システムは、Cisco TMS への接続時に tms.example.com を使用する必要があります。サーバ自体のホスト名 (tms01.example.com) を使用することはできません。

Cisco TMS のインストールが成功したことを確認してから、次の操作を実行します。

1. Cisco TMS では、**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)]**
2. **[TMS Server の完全修飾ホスト名 (TMS Server Fully Qualified Hostname)]** と **[TMS サーバーアドレス (完全修飾ホスト名または IPv4 アドレス)]** フィールドに *tms.example.com* を入力します。

Cisco TMS にログインするときに、ローカルユーザーアカウントは使用しないでください。すべてのユーザ アカウントは、セカンダリ サーバ (tms02) にスワップする必要がある場合に使用できるように、ドメイン アカウントである必要があります。

## セカンダリ Cisco TMS Server の設定

1. サービス パック レベルも含めて、tms02 のオペレーティング システムが tms01 と完全に同じであることを確認します。
2. 両方のサーバが同じタイム ゾーンに設定されていることを確認します。タイム ゾーンが異なると、スイッチオーバーが起きた場合に、スケジュールされた会議の開始時間および終了時間が正しくないものになります。
3. tms02 で Cisco TMS インストーラを実行します。
  - a. 求められたら、外部 SQL Server の IP アドレスを入力します。

## 冗長展開の設定

- b. インストール先は tms01 上と同じディレクトリにして、tms01 上と同じログ ディレクトリを使用します。ログ ディレクトリのパスは SQL データベースではなく Windows の環境変数に保存されるため、この操作は重要です。
- c. tms01 へのインストール中に生成された暗号キーを入力します
- d. HTTPS を有効にするときに tms01 で使用した証明書と同じ証明書を使用します。
- 4. ログインして、Cisco TMS Web アプリケーションが正常に機能してるかを確認します。
- 5. tms02 で、**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)] > [内部 LAN のシステムの高度なネットワーク設定 (Advanced Network Settings for Systems on Internal LAN)]** の順に選択します。インストーラによって変更された可能性があるため、IP アドレスが tms01 (10.0.0.10) で、ホスト名が tms.example.com であることを確認します。
- 6. tms02 でサービス管理コンソールを開きます。
  - すべての Cisco TMS サービス（名前はすべて TMS から始まります）を停止します。
  - World Wide Web 発行サービスという名前のインターネット インフォメーション サービス (IIS) を停止します。
  - IIS および TMS サービスの起動タイプを [手動 (Manual)] に設定します。

これで、tms01 の障害に備えて tms02 をウォーム スペアとして動作させる準備ができました。

**[管理ツール (Administrative Tools)] > [サーバーメンテナンス (Server Maintenance)] > [TMS サービスステータス (TMS Service Status)]** では、両方のサーバーのサービスが表示されることに注意してください。リストから tms02 の停止したサービスを削除するには、**[リストのクリア (Clear List)]** をクリックします。

## ローカル ファイルの同期

Cisco TMS によって使用されるカスタマイズ可能なファイルの中には、tmsng データベース内ではなく Windows Server のローカルファイルシステム内に保存されるものがあります。これらのファイルが保存されるフォルダは、2 つのサーバー間で同期させる必要があります。同期させる必要があるすべてのフォルダのリストについては、「同期する [ローカル ファイル \(59 ページ\)](#)」を参照してください。

Cisco TMS は、ファイル同期プロセスを維持しません。サードパーティ製ツールを使用する必要があります。ファイル/フォルダの同期の適切な構成に関する情報については、サードパーティ製ツールのドキュメントを参照してください。

プライマリ サーバで障害が発生したときに 2 台のサーバをスワップする場合、tms01 と tms02 のフォルダを同期するように設定した同期メカニズムを、tms02 から tms01 に同期化するように変更します。

## オプション : TLS クライアント証明書の有効化


TLS クライアント証明書を導入時に使用する場合は、以下を確認する必要があります。

- 2 つのサーバーの Cisco TMS ツールで同じオプションが選択されます。
- 2 つのサーバにインポートされた TLS 証明書が同じである。
- 2 つのサーバで同じ証明書の失効メカニズムを使用している。

詳細については、『[Cisco TMS 管理者ガイド](#)』の「Cisco TMS ツール」章を参照してください。

## Cisco TMS のアップグレード

プライマリサーバーとセカンダリサーバーの Cisco TMS のソフトウェアバージョンは一致させる必要があります。プライマリ サーバのアップグレード後に、できるだけ早くセカンダリ サーバをアップグレードする必要があります。セカンダリサーバーのソフトウェアバージョンが古い状態でプライマリサーバーに障害が発生した場合、セカンダリサーバーを新しい Cisco TMS のソフトウェアバージョンにアップグレードするまで、サーバーをスワップできません。

1. ファイル レプリケーションを無効化して、ローカル ファイルの同期を一時的に停止します。 
2. プライマリ サーバをアップグレードします。
3. セカンダリ サーバをアップグレードします。
4. Cisco TMS ログインして、Cisco TMS Web アプリケーションが正常に機能してるかを確認します。
5. Cisco TMS アプリケーションでは、**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)]**。

## 冗長展開の設定

6. 次の IP アドレスとホスト名が、IP アドレスは 10.0.0.10、ホスト名は tms.example.com に設定されていることを確認します。
  - **[ イベント通知 (Event Notification) ] > [ SNMP トラップホスト IP アドレス (SNMP Traphost IP Address) ]**
  - **内部 LAN のシステムの高度なネットワーク設定**：すべてのフィールド
  - **パブリック インターネット/ファイアウォールの外側のシステムに対する高度なネットワーク設定 (Advanced Network Settings for Systems on Public Internet/Behind Firewall)**
7. TMS サービスを停止して、[手動 (Manual) ] に再設定します。
8. ファイル レプリケーションを有効化します。

## プライマリ サーバで障害が発生した場合のリカバリ

プライマリ サーバ tms01 で障害が発生して使用不能になった場合、数分とかからずに、セカンダリ サーバ tms02 が動作状態に変更されます。

1. tms01 をネットワークから外します。
2. tms02 の IP アドレスを、障害発生前の tms01 の IP アドレスに変更します (例：10.0.0.10) 。
3. 新しい IP アドレスで tms02 に到達可能であることを確認します。
4. Cisco TMS アプリケーションを開いて、**[構成 (Configuration) ] > [データベース接続設定の変更 (Change DB Connect Settings) ]** の順に選択します。
5. 最初に tms02 を設定してからデータベースへのパスワードが変更された可能性があるため、**[OK]** をクリックして tms02 のパスワードが正しいままであることを確認します。
6. サービス管理コンソールで次の操作を行います。
  - a. すべての TMS サービスと World Wide Web 発行サービスの起動タイプを**[自動 (Automatic) ]** に設定します。
  - b. **[サービスを開始します。(Start the services)]**

Tms02 が Cisco TMS Server で有効化されます。Cisco TMS との通信時に tms.example.com を使用するように管理対象サービスを設定済みのため、管理対象自体の再設定は必要ありません。

tms02 が正常に動作することを確認するために、次の操作を実行します。

1. 短い会議を 2 分後にスケジュールします。
2. 正常に会議が開始され、切断されることを確認します。
3. **[会議制御センター(Conference Control Center)]**を使用してこの会議を監視できることを確認します。
4. Cisco TMS がこの会議の通話詳細レコード (CDR) を生成することを確認します。

Cisco TMS がシステムと通信していることを確認するには、次の手順を実行します。

1. TMS Database Scanner Service が完全実行を完了するまで、約 20 分待機します。
2. Cisco TMS で、**[システム (Systems) ] > [システム概要 (System Overview) ]** の順に選択します。
3. 左側のツリーにあるすべてのシステムを選択し、右側のツリーで **[ネットワーク設定 (Network Settings) ] > [TMS とシステムの接続性 (TMS To System Connectivity) ]** を選択します。
4. **[表示 (View) ]** をクリックして、すべてのシステムの **[ステータス (Status) ]** が **[応答なし (NoResponse) ]** に設定されていないことを確認します。

**[管理ツール (Administrative Tools) ] > [サーバーメンテナンス (Server Maintenance) ] > [TMS サービスステータス (TMS Service Status) ]** では、両方のサーバーのサービスが表示されることに注意してください。リストから tms01 の停止したサービスを削除するには、**[リストのクリア (Clear List) ]** をクリックします。

tms01 をネットワークに接続する前に、次の操作を行います。

1. tms01 の IP アドレスを、以前の tms02 の値 (例：10.0.0.11) に変更します。
2. すべての TMS サービスと IIS を無効化します。

tms01 は問題が修復されると、tms02 がダウンした場合に備えてウォーム スペアになります。

**注：** IP アドレスを新しい値に変更する前に、tms01 をネットワークに戻さないでください。戻すと、IP アドレスの競合が発生し、Cisco TMS で予期しない動作が起こる場合があります。



## 冗長展開の設定

## バージョン 14.4 以降からの冗長展開のアップグレード

## サーバをアップグレードする前に

両方の Cisco TMS Server で次を実行します。

1. ファイル レプリケーションを無効化して、ローカル ファイルの同期を一時的に停止します。
2. すべての TMS サービスおよび IIS サービスを停止します。

## プライマリ ノードのアップグレード

1. 通常の方法で、Cisco TMS プライマリサーバーをアップグレードします。
2. **[管理ツール (Administrative Tools)] > [TMS Server メンテナンス (TMS Server Maintenance)]** の順に選択し、サーバーが **[TMS の冗長性 (TMS Redundancy)]** セクションで **[アクティブ (Active)]** として一覧されているかを確認します。**[パッシブ (Passive)]** とリストされている場合は、データが正しく更新されるまで最大で 1 分間、**[更新 (Refresh)]** を繰り返しクリックします。

## セカンダリ ノードのアップグレード

1. 通常の方法で、Cisco TMS セカンダリサーバーをアップグレードします。
2. NLB の 仮想 IP を介して、**[管理ツール (Administrative Tools)] > [TMS サーバーメンテナンス (TMS Server Maintenance)]** の順に選択し、2 つ目のサーバーが **[TMS の冗長性 (TMS Redundancy)]** セクションで、**[パッシブ (Passive)]** として表示されているか確認します。
3. **[Cisco TelePresence Management Suite (TMS) サービスのステータス (TMS Services Status)]** セクションで、パッシブノードのすべての Cisco TelePresence Management Suite (TMS) サービス (TMSPROBEURL を含む) が **[サービスはスタンバイ状態 (Service On Standby)]** と表示されていることを確認します。
4. 「手動フェールオーバーのテスト (48 ページ)」で記載されている指示に下があって、**手動フェールオーバーをテストします。**
5. 2 つの Cisco TMS ノード間のローカルファイルの複製を再度有効化します。

## バージョン 14.4 より前の Cisco TMS からの冗長展開のアップグレードを行う

バージョン 14.4 より前の Cisco TMS から 冗長 Cisco TMS 展開をアップグレードするには、ネットワークロードバランサ (NLB) の構成を変更する必要があります。アップグレードをする前に、「[冗長展開の設定 \(44 ページ\)](#)」を読み、新しい推奨 NBL セットアップについてよく理解してください。

## サーバをアップグレードする前に

両方の Cisco TMS Server で次を実行します。

1. ファイル レプリケーションを無効化して、ローカル ファイルの同期を一時的に停止します。
2. すべての TMS サービスおよび IIS サービスを停止します。
3. サーバがデフォルト ゲートウェイとして NLB を使用しないように、デフォルト ゲートウェイを変更します。
4. 管理対象システムの Web インターフェイスにアクセスするなどして、管理対象システムのネットワークに接続できることを確認します。



## プライマリ サーバのアップグレードと設定

1. 通常の方法で、Cisco TMS プライマリサーバーをアップグレードします。
2. アップグレードが完了したら、Cisco TMS Web インターフェイスにログインします。**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [一般設定 (General Settings)]** の順に選択し、**[TMS の冗長性の有効化 (Enable TMS Redundancy)]** を **[はい (Yes)]** に設定します。

## 冗長展開の設定

3. **【管理ツール (Administrative Tools)】 > 【TMS Server メンテナンス (TMS Server Maintenance)】** の順に選択し、サーバーが **【TMS の冗長性 (TMS Redundancy)】** セクションで **【アクティブ (Active)】** として一覧されているかを確認します。**【パッシブ (Passive)】** とリストされている場合は、データが正しく更新されるまで最大で 1 分間、**【更新 (Refresh)】** をクリックします。
4. **【プローブ URL (Probe URL)】** をメモします。

## プライマリサーバでの設定の更新と検証を行う

1. **「ACE 構成の例」** の説明に従って、NBL を移行します。上記ステップ 4 のプローブ URL を使用します。    
セカンダリ サーバはまだアップグレードされていないため、セカンダリ サーバのプローブはこの段階では失敗することに注意してください。 
2. プライマリサーバで **【管理ツール (Administrative Tools)】 > 【TMS サーバーメンテナンス (TMS Server Maintenance)】** の順に選択し、**【TMS サービスのステータス (TMS Services Status)】** セクションのリストに **【TMSProbeURL】** が表示されていることを確認します。**【管理ツール (Administrative Tools)】 > 【TMS サーバーメンテナンス (TMS Server Maintenance)】** の順に選択し、**【TMS サービスのステータス (TMS Services Status)】** セクションのリストに **【TMSProbeURL】** が表示されていることを確認します。
3. ブラウザで NLB の仮想 IP アドレス (VIP) を入力し、Cisco TMS に転送されることを確認します。

## セカンダリ サーバのアップグレードを行います

1. 通常の方法で、Cisco TMS セカンダリサーバをアップグレードします。
2. NLB の VIP を介して **【管理ツール (Administrative Tools)】 > 【TMS サーバーメンテナンス (TMS Server Maintenance)】** の順に選択し、**【TMS の冗長性 (TMS Redundancy)】** セクションで、2 番目のサーバーが **【パッシブ (Passive)】** と表示されていることを確認します。
3. **【Cisco TMS サービスのステータス (TMS Services Status)】** セクションで、パッシブノードのすべての Cisco TMS サービス (TMSProbeURL を含む) が **【サービスはスタンバイ状態 (Service On Standby)】** と表示されていることを確認します。
4. **「フェールオーバー動作のテスト (49 ページ)」** の指示に従って、手動フェールオーバーをテストします。
5. 2 つの Cisco TMS ノード間のローカルファイルの複製を再度有効化します。

## ACE 構成の例

次の例では、ロードバランサが Cisco TMS を使って ACE 構成をする際の詳細を示しています。この構成を適用すると、新しい冗長性モデルで正しく機能するようになります。

次に例を示します。

```
probe http PROBE-HTTP-TMS
  port 80
  interval 2
  faildetect 1
  passdetect interval 2
  request method head url /tms/public/IsAlive.aspx?guid=<TMS_REDUNDANCY_GUID>
  expect status 200 200
  open 1
  rserver host TMS01
  ip address 10.0.200.50
  inservicer
  server host TMS02
  ip address 10.0.200.60
```

## 冗長展開の設定

```

inservice
serverfarm host SFARM-TMS
failaction purge
probe PROBE-HTTP-TMS
rserver TMS01
inservice
rserver TMS02
inservice
class-map match-any L4-CLASS-TMS
2 match virtual-address 10.0.200.40 tcp eq 443
3 match virtual-address 10.0.200.40 tcp eq 80
4 match virtual-address 10.0.200.40 udp eq 162
5 match virtual-address 10.0.200.40 tcp eq 3601
policy-map type loadbalance first-match L7-POLICY-TMS
class class-default serverfarm SFARM-TMS
policy-map multi-match L4-POLICY-TMS
class L4-CLASS-TMS
loadbalance vip inservice
loadbalance policy L7-POLICY-TMS
loadbalance vip icmp-reply
nat dynamic 1 vlan 200
interface vlan 200
no ipv6 normalization
no ipv6 icmp-guard
ip address 10.0.200.24 255.255.255.0
no normalization
no icmp-guard
access-group input ALL
access-group output ALL
nat-pool 1 10.0.200.30 10.0.200.30 netmask 255.255.255.255 pat
service-policy input L4-POLICY-TMS
no shutdown

```

## F5 BIG-IP の設定例

次に例を示します。

```

ltm default-node-monitor {
rule /Common/icmp and /Common/snmp_dca
}
ltm node /Common/TMS01 {
address 10.0.200.50
description "TMS NODE 01"
monitor /Common/icmp
}
ltm node /Common/TMS02 {

```



## 冗長展開の設定

```
address 10.0.200.60
description "TMS NODE 02"
monitor /Common/icmp
}
ltm pool /Common/pl-TMS {
members {
/Common/TMS01:0 {
address 10.0.200.50
}
/Common/TMS02:0 {
address 10.0.200.60
}
}
monitor /Common/mn-TMS-HTTPS
}
ltm virtual /Common/vs-TMS-HTTP {
description "TMS Virtual Server for HTTP"
destination /Common/10.0.200.40:80
ip-protocol tcp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
/Common/VLAN200
}
vlans-enabled
}
ltm virtual /Common/vs-TMS-HTTPS {
description "TMS Virtual Server for HTTPS"
destination /Common/10.0.200.40:443
ip-protocol tcp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
```

## 冗長展開の設定

```
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
/Common/VLAN200
}
vlans-enabled
}
ltm virtual /Common/vs-TMS-PLCM {
description "TMS Virtual Server for Polycom"
destination /Common/10.0.200.40:3601
ip-protocol tcp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
vlans {
/Common/VLAN200
}
vlans-enabled
}
ltm virtual /Common/vs-TMS-SNMPTRAP {
description "TMS Virtual Server for SNMPTRAP"
destination /Common/10.0.200.40:162
ip-protocol udp
mask 255.255.255.255
pool /Common/pl-TMS
profiles {
/Common/fastL4 { }
}
source 0.0.0.0/0
source-address-translation {
type automap
}
translate-address enabled
translate-port enabled
```

## 冗長展開の設定

```

vlangs {
/ Common/VLAN200
}
vlangs-enabled
}
ltm virtual-address /Common/10.0.200.40 {
address 10.0.200.40
arp enabled
icmp-echo enabled
mask 255.255.255.255
traffic-group /Common/traffic-group-1
}
ltm monitor https /Common/mn-TMS-HTTPS {
adaptive disabled
cipherlist DEFAULT:+SHA:+3DES:+kEDH
compatibility enabled
defaults-from /Common/https
destination *:443
interval 5
ip-dscp 0
recv 200
recv-disable 503
send "HEAD /tms/public/IsAlive.aspx?guid=<TMS_REDUNDANCY_GUID> HTTP/1.0\r\n"
time-until-up 0
timeout 16
}

```

**注：**

1. Polycom デバイスがない場合は、ポート **3601** を構成する必要はありません。
2. SNMP の使用を無効にするより高いセキュリティモードを有効にしている場合は、**SNMPTRAP** ポートを構成する必要はありません。
3. https のみを許可すると、http が削除される可能性があります。

## 同期用ローカル ファイル

Cisco TMS のインストール中に、冗長展開を使用する場合に 2 台のサーバー間で同期する必要のあるカスタマイズ可能ファイルが追加されます。

このようなファイルには、Cisco TMS にアップロード可能なソフトウェアおよびイメージ、Cisco TMS により作成されたイメージなどが含まれます。

デフォルトのインストールでのファイルの場所は次のとおりです。

**C:\Program Files (x86)\TANDBERG\TMS\Config\System\**

**C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\**

**注：**ディレクトリは初めて使用するときには作成されるため、これらのディレクトリはノード間のファイル複製の設定時に存在しない可能性があります。

# Cisco TMS の移動またはアンインストール

この章では、Cisco TMS を新サーバーに移動する手順と旧サーバーからすべてのコンポーネントを削除する手順について説明します。

新しいサーバーに Cisco TMS を移動する	60
Cisco TMS のアンインストール	65
Cisco TMS データベースを外部 SQL Server に移動する	66
TMS Log Collector のアンインストール	66

## 新しいサーバーに Cisco TMS を移動する

サーバーの使用を停止する場合でも、導入を拡大してより高いハードウェア機能が必要になる場合でも、Cisco TMS のインストールを別のサーバーに移行する際は以下の手順に従ってください。

### ご使用になる前に

- 新サーバのネットワーク構成は変更せず、可能であれば同じ DNS ホスト名と IP アドレスを使用することをお勧めします。こうすることで移行後に必要な管理タスクを最小限に抑えることができます。
- ファイアウォール上で、旧サーバ用に開放されているポートが同じく新サーバ用にも開放されていることを確認してください。
- Cisco TMSPE が Cisco TMS Server にインストールされている場合は、同時に移動する必要があります。

## アプリケーションおよびデータベースの移行

### インストール データのコピー

ローカルまたはリモートのデータベースとともに Cisco TMS を移行する前に、以下の作業を行ってください。

1. インストールプロセスで新サーバーに入力する暗号キーのコピーを作成します。Cisco TMS Server で、[TMS ツール (TMS Tools)] を開き、[セキュリティ設定 (Security Settings)] > [暗号化キー (Encryption Key)] の順に選択します。ノートパッド ファイルにコピーします。
2. 同じ IP アドレスを維持し、外部認証局の TLS クライアント証明書を使用する場合は、新サーバーで使用するためのコピーを作成します。新サーバのホスト名が変わる場合は、新しい証明書を生成する必要があります。

### SQL は、ローカルで Cisco TMS Server に保管されます

両方のサーバーで、同じバージョンの Cisco TMS を使用する必要があります。また、同じタイムゾーンを使用する必要があります。

1. Cisco TMS サーバーのすべての Cisco TelePresence Management Suite (TMS) サービスと IIS を停止します。
  - a. サービス管理コンソールを開きます。
  - b. すべての Cisco TMS サービス（名前はすべて TMS から始まります）を停止します。
  - c. World Wide Web 発行サービスという名前のインターネット インフォメーション サービス (IIS) を停止します。

## Cisco TMS の移動またはアンインストール

2. SQL Server Management Studio Express を使用して、SQL データベースをバックアップし、**tmsng.bak** ファイルを新規 Cisco TMS Server にコピーします。
  - a. **tmsng** データベースを右クリックします。
  - b. [タスク (Tasks) ] > [バックアップ... (Back Up...)] の順に選択します。 > [データベース (Database...)] を選択します。
  - c. バックアップ先のパスをメモし、[OK] をクリックします。
  - d. バックアップ先から新しいサーバー上に **tmsng.bak** ファイルをコピーします。
3. 新しいサーバーに同じバージョンの Cisco TMS をインストールします。
  - a. [データベースをこのサーバにインストール (Install the database on this server)] を選択します。
  - b. リリース キーやオプション キーは入力しないでください。
  - c. 旧サーバーの **IP アドレス**を入力します。
  - d. 旧サーバーの**暗号キー**を入力します。
4. SQL Server Management Studio Express を使用して SQL データベースを復元します。
  - a. **tmsng** データベースを右クリックします。
  - b. [タスク (Tasks) ] > [復元 (Restore) ] > [データベース (Database) ] を選択します。
  - c. [復元するバックアップ セットのソースと場所を指定 (Specify the source and location of backup sets to restore) ] で [デバイスから (From device) ] を選択し、**tmsng.bak** ファイルを保存した場所を参照します。
  - d. [データベースの復元 - tmsng (Restore Database - tmsng) ] ウィンドウに戻るまで [OK] をクリックします。
  - e. [復元するバックアップ セットを選択 (Select the backup sets to restore) ] で該当するバックアップ ファイルの横の [復元 (Restore) ] 列のチェックボックスをオンにします。[OK] をクリックします。
5. Cisco TMS Web アプリケーションを開き、アプリケーションが動作しているかと、各場所にあるすべてのデータを確認します。
6. 必要に応じて、元のサーバ上でローカルに保存された次のカスタマイズ可能なフォルダを、新サーバ上の同じ場所にコピーします。これらのフォルダは初回使用時に作成されるため、手動による作成が必要になることがあります。デフォルトのインストールでのファイルの場所は次のとおりです。
  - C:\Program Files (x86)\TANDBERG\TMS\Config\System\
  - C:\Program Files (x86)\TANDBERG\TMS\Data\GenericEndpoint\
  - C:\Program Files (x86)\TANDBERG\TMS\Data\SystemTemplate\
  - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\
  - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\
  - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

## SQL データベースがリモート サーバにある場合

この場合、データベースがインストール中にアップグレードされるので、同じバージョンの Cisco TMS を使用する必要はありません。

1. Cisco TMS サーバーのすべての Cisco TelePresence Management Suite (TMS) サービスと IIS を停止します。
  - a. サービス管理コンソールを開きます。
  - b. すべての Cisco TMS サービス (名前はすべて TMS から始まります) を停止します。
  - c. World Wide Web 発行サービスという名前のインターネット インフォメーション サービス (IIS) を停止します。
2. 新しいサーバーに Cisco TMS をインストールし、インストール時既存の外部 SQL データベースを差すように指定します。
3. Cisco TMS Web アプリケーションを開き、アプリケーションが動作しているかと、各場所にあるすべてのデータを確認します。

## Cisco TMS の移動またはアンインストール

4. 必要に応じて、元のサーバ上でローカルに保存された次のカスタマイズ可能なフォルダを、新サーバ上の同じ場所にコピーします。これらのフォルダは初回使用時に作成されるため、手動による作成が必要になることがあります。デフォルトのインストールでのファイルの場所は次のとおりです。
  - C:\Program Files (x86)\TANDBERG\TMS\Config\System\
  - C:\Program Files (x86)\TANDBERG\TMS\Data\GenericEndpoint\
  - C:\Program Files (x86)\TANDBERG\TMS\Data\SystemTemplate\
  - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\
  - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\
  - C:\Program Files (x86)\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

## 新しいネットワーク構成での移行

一部のケースでは、移行の一環として、Cisco TMS Server の IP アドレスやホスト名まで変更する必要がある場合があります。

その場合は新サーバに Cisco TMS をインストールした後、データベースに接続されていること、すべてのデータが存在することを確認し、次の手順を実行します。

- **[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)]** の順に選択し、**[内部 LAN のシステムの高度なネットワーク設定 (Advanced Network Settings for Systems on Internal LAN)]** および **[パブリックインターネット上またはファイアウォール内側のシステム向けの高度なネットワーク設定 (Advanced Network Settings for Systems on Public Internet/Behind Firewall)]** に Cisco TMS Server の新しい IP アドレスとホスト名を入力します。
- **[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [ネットワーク設定 (Network Settings)] > [システム上の管理設定の強制 (Enforce Management Settings on Systems)]** の順に選択し、**[今すぐ適用 (Enforce Now)]** をクリックします。
- サーバのホスト名が変わり、Active Directory アカウントではなくローカル ユーザ アカウントを使用する場合は、**[TMS ツール (TMS Tools)] > [ユーティリティ (Utilities)] > [ユーザ ドメインの変更 (Change User Domain)]** を使用してユーザ ドメインを変更します。ローカル ユーザ アカウントを使用する場合、新サーバではこれらを手動で作成し直す必要があります。
- Polycom システムの場合は、SNMP の **[コンソール IP アドレス (Console IP Address)]** を Cisco TMS Server の新しい IP アドレスやホスト名に手動で変更し、各システムをリブートします。
- Cisco TMSXE を使用している場合は、構成ツールを開き、必要に応じて Cisco TMS 接続の詳細を変更します。
- Cisco TMSXN を使用している場合は、Domino Administrator を開き、必要に応じて Cisco TMS 用に作成したリソース予約データベースで **[ホスト名 (Host name)]** を変更します。
- リモート システムの場合、各システムの **[外部マネージャ アドレス (External Manager Address)]** を新しい IP アドレスまたはホスト名に手動で変更します。

## アプリケーションの移行後

移行後、元のサーバで Cisco TMS に関するサービスを再度アクティブにしないでください。

サーバをデコミッションしない場合、Cisco TMS を元のサーバから削除することを強く推奨します。「[サーバーからすべての Cisco TMS 情報を削除する \(65 ページ\)](#)」を参照してください。

## Cisco TMSXE の移動

Cisco TMSXE を新サーバに移行する方法については、『[Cisco TMSXE 導入ガイド](#)』を参照してください。

非常に小規模な展開を除き、Cisco TMSXE を Cisco TMS と同じサーバにインストールしないでください。詳細については、インストール ガイドのベスト プラクティスのセクションを参照してください。

## Cisco TMS の移動またはアンインストール

## Cisco TMSPE の移動

Cisco TMSPE は常に Cisco TMS Server にインストールされており、Cisco TMS を移動したらすぐに移動する必要があります。

Cisco TMS と同様に、Cisco TMSPE データベースはローカルまたはリモートの場合があります。

## ローカル データベース

Cisco TMSPE を移動するには、次の手順を実行します。

1. 元のサーバで プロビジョニング拡張機能 Windows サービスを停止します。
2. 上記の Cisco TMS で手順に従って、tmspe データベースをコピーして復元します。詳細については、「[SQL データベース を Cisco TMS Server にローカルで保管する](#) (60 ページ)」を参照してください。
3. Cisco TMSPE を新しいサーバにインストールし、インストーラが新しい tmspe データベースの場所を指すように指定します。
4. Cisco TMS のネットワーク構成が変更された場合は、**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [プロビジョニング拡張機能の設定 (Provisioning Extension Settings)] > [Cisco TMS 設定 (Cisco TMS Settings)]** の順に選択します。  
**[ホスト名 (Hostname)]** が localhost でない場合は、新しい Cisco TMS アドレスを反映するように更新する必要があります。

## リモートデータベース

Cisco TMSPE を移動するには、次の手順を実行します。

1. 元のサーバで プロビジョニング拡張機能 Windows サービスを停止します。
2. 新サーバに Cisco TMS をインストールし、インストーラにリモートデータベースの場所を指定します。

3. Cisco TMS のネットワーク構成が変更された場合は、**[管理ツール (Administrative Tools)] > [構成 (Configuration)] > [プロビジョニング拡張機能の設定 (Provisioning Extension Settings)] > [Cisco TMS 設定 (Cisco TMS Settings)]** の順に選択します。  
**[ホスト名 (Hostname)]** が localhost でない場合は、新しいアドレスを反映するように更新する必要があります。

## データベースを外部 SQL Server に移動する

データベースを外部 SQL Server に移動するには、次の手順を実行します。

1. Cisco TMS Server のすべての Cisco TMS と IIS を停止します。

- a. サービス管理コンソールを開きます。
- b. すべての Cisco TMS サービス（名前はすべて **TMS** から始まります）を停止します。
- c. World Wide Web パブリッシング サービスという名前のインターネット インフォメーション サービス (IIS) を停止します。

2. SQL Server Management Studio を使用して、SQL データベースをバックアップし、**tmsng.bak** ファイルを外部 SQL Server にコピーします。

Cisco TMSPE がインストールされていて、Cisco TMSPE、tmspe\_vmr、および tms\_userportal データベースにリストされている場合は、それらのデータベースのバックアップを作成します。

- a. **tmsng** データベースを右クリックします。
- b. **[タスク (Tasks)] > [バックアップ... (Back Up...)]** の順に選択します。 > **[データベース (Database...)]** を選択します。
- c. バックアップ先のパスをメモし、**[OK]** をクリックします。
- d. バックアップ先から外部サーバーの任意の場所に **tmsng.bak** ファイルをコピーします。
- e. 該当する場合は、Cisco TMSPE データベース作成手順と同じ手順に従います。
3. SQL Server Management Studio を使用して、**tmsng** という同じ名前の新しいデータベースを作成する
  - a. **[データベース (Databases)] > [新しいデータベース (New Database)]** の順に選択し、右クリックします。
  - b. データベースに **tmsng** と入力し、**[OK]** をクリックします。
  - c. 該当する場合は、同じ手順に従って Cisco TMSPE データベースを作成します。
4. SQL Server Management Studio を使用して SQL データベースを復元する：
  - a. **tmsng** データベースを右クリックします。
  - b. **[タスク (Tasks)] > [復元 (Restore)] > [データベース... (Database...)]** の順に選択します。
  - c. **[復元するバックアップセットのソースと場所を指定 (Specify the source and location of backup sets to restore)]** で **[デバイスから (From device)]** を選択し、**tmsng.bak** ファイルを保存した場所を参照します。
  - d. **[データベースの復元 - tmsng (Restore Database - tmsng)]** ウィンドウに戻るまで **[OK]** をクリックします。
  - e. **[復元するバックアップセットを選択 (Select the backup sets to restore)]** で該当するバックアップファイルの横の **[復元 (Restore)]** 列のチェックボックスをオンにします。
  - f. **[ページの選択 (Select a page)]** で、**[オプション (Options)]** をクリックし、**[既存のデータベースを上書き (置き換えあり) (Overwrite the Existing database (WITH REPLACE))]** チェックボックス をオンにしたら、**[OK]** をクリックします。
  - g. 該当する場合は、同じ手順に従って Cisco TMSPE データベースを作成します。
5. TMS ツールを使用して Cisco TMS データベース接続設定を変更する
  - a. TMS サーバーで、TMS ツールアプリケーションを起動します。
  - b. **[構成 (Configuration)] > [Cisco TMS データベース接続 (Cisco TMS Database Connection)]** の順に選択します。
  - c. **[データベースサーバー/インスタンス (Database Server/Instance)] > [認証情報を入力 (Enter Authentication information)]** の順に選択し、新規外部 SQL Server 情報を入力したら、**[保存 (Save)]** をクリックします。
  - d. Cisco TMSPE をインストールする場合は、**[Cisco TMSPE Da データベース接続 (Cisco TMSPE Database Connection)]** をクリックし、ステップ C を実行します。



## Cisco TMS の移動またはアンインストール

6. Cisco TMS Server ですべての Cisco TMS サービスと IIS を開始します。

- a. サービス管理コンソールを開きます。
- b. すべての Cisco TMS サービス（名前はすべて **TMS** から始まります）を開始します。
- c. World Wide Web パブリッシングサービスという名前のインターネット インフォメーション サービス (IIS) を開始します。

## Cisco TMS のアンインストール

このセクションでは、Cisco TMS アプリケーションの削除方法について説明します。通常の状態では、Cisco TMS の古いバージョンは、Cisco TMS インストーラから自動削除されるのでご注意ください。

Cisco TMS をアンインストールすると、Cisco TMS アプリケーション、Web サイトおよびサービスが削除されます。カスタマー データ、ログ、データベースおよびデータベース サーバは、将来のアップグレードに備えて、完全に保持されます。

アンインストール ウィザードでは、SQL Server はいっさい変更されません。データベースサーバーを含むすべての Cisco TMS 情報をサーバーから完全に削除する場合は、次のセクションを参照してください。

Cisco TMS アプリケーションを削除するには、次の手順を実行します。

1. **[開始 (Start)]** メニューまたは画面のシスコプログラムグループで *[Cisco TMS をアンインストール (Uninstall Cisco TMS)]* を選択するか、Windows のコントロールパネルで **[プログラムの追加と削除 (Add/Remove Programs)]** を選択します。  
[ようこそ (Welcome)] ウィンドウに、アンインストールスクリプトで Cisco TMS は削除されるが、データベースとデータベースサーバーは個別に削除する必要があるという説明が表示されます。
2. **[Next]** をクリックします。  
ウィザードによって、Cisco TMS のサービス、Web サイト、およびアプリケーションデータが削除されます。

Cisco TMS アプリケーションの削除を完了します。

## サーバーからのすべての Cisco TMS 情報を削除する

アンインストールウィザードは、Cisco TMS のみをサーバーから削除します。これにより、Cisco TMS を今後簡単に再インストールまたはアップグレードできます。

**注意：**

- これらの手順では、SQL Server が その他アプリケーションではなく、Cisco TMS でインストールされ、正常に削除できることを前提としています。SQL Server が他のアプリケーションによって使用されている場合は、SQL Server またはそのプログラム フォルダを削除しないでください。
- 次の手順を実行すると、すべての Cisco TMS データを削除できます。ご使用の Cisco TMS インストール情報を保存したい場合は、先に進まないでください。

Cisco TMS とデータをサーバーから完全に削除するには、次の手順を実行します。

1. 前の項の手順を使用して、Cisco TMS アンインストールウィザードを実行します。
2. Cisco TMSPE をインストールする場合は、[「Cisco TelePresence Management Suite 導入ガイド」](#) を参照して、アンインストールしてください。
3. Cisco TMS インストールを使用してプログラムフォルダを削除します。デフォルトの場所は **C:\Program Files (x86)\TANDBERG\TMS** です。
4. **[スタート (Start)]** メニューの **[ファイル名を指定して実行 (Run)]** を選択して「regedit」と入力し、**[OK]** をクリックして Windows レジストリ エディタを開きます。
5. アイコンを使用して左側のツリーを展開して、Hive (フォルダ) **HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Tandberg\TANDBERG Management Suite** を検索します。
6. **TANDBERG Management Suite** フォルダアイコンを右クリックして、**[削除 (Delete)]** をクリックします。確認のために **[Yes]** をクリックします。
7. レジストリ エディタを閉じます。

## Cisco TMS の移動またはアンインストール

8. リモート SQL Server を使用している場合、Microsoft SQL 管理者に問い合わせ、Cisco TMS が使用する Microsoft SQL から **tmsng** という名前のデータベースを停止するように依頼します。
9. Cisco TMS が排他的に使用する SQL Server のローカルコピーがある場合は、次の手順を実行して削除します。
  - a. Windows コントロールパネルの **【プログラムの追加と削除 (Add/Remove Programs)】** を開きます。
  - b. リストのインストールに応じて関連するバージョン番号 (2012/ 2014/2016/2017) の「Microsoft SQL Server」を検索し、**【削除 (Remove)】** を選択します。
  - c. SQL インストールेशनによって使用されていたプログラム フォルダを削除します。デフォルトの場所は、**C:\Program Files\Microsoft SQL Server** です。

これで、Cisco TMS、データベース、顧客が保存したすべてのデータの削除が完了されます。

## Cisco TMS データベースを外部 SQL Server に移動する

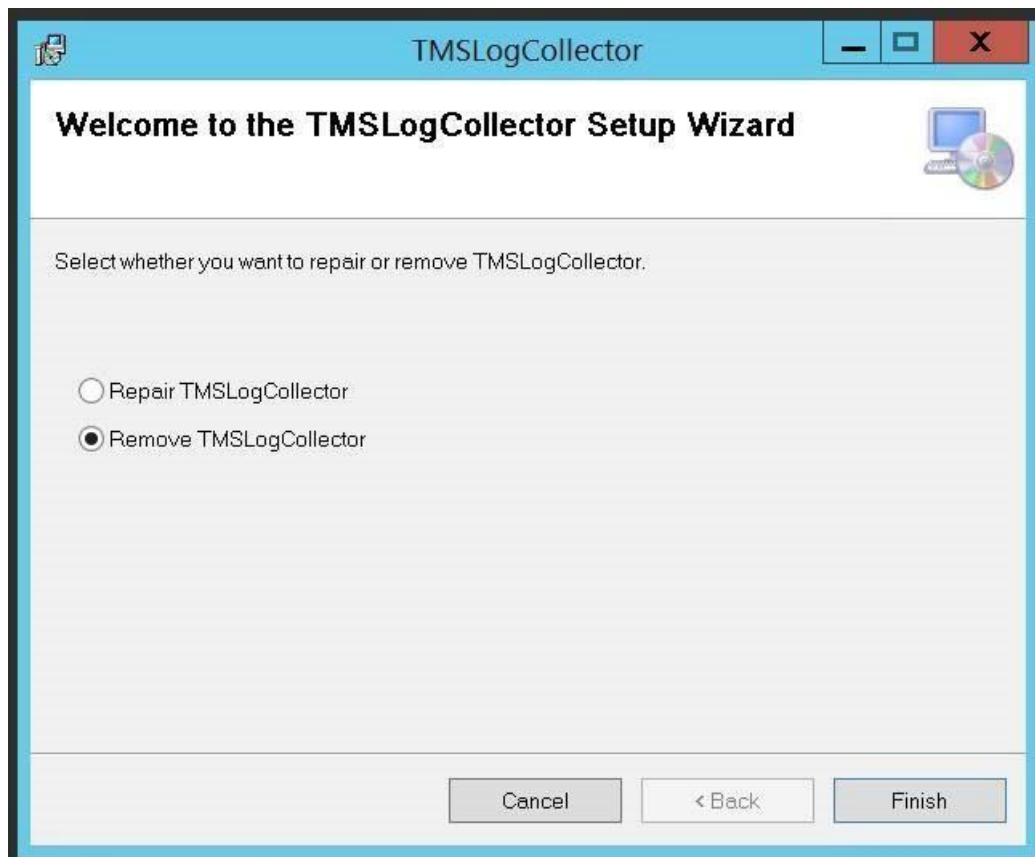
手順に従って、Cisco TMS データベースを外部 SQL Server に移動します。

1. Cisco TMS サーバーのすべての Cisco TelePresence Management Suite (TMS) サービスと IIS を停止します。
  - a. サービス管理コンソールを開きます。
  - b. すべての Cisco TMS サービス (名前はすべて TMS から始まります) を停止します。
  - c. World Wide Web 発行サービスという名前のインターネット インフォメーション サービス (IIS) を停止します。
2. SQL Server Management Studio Express を使用して SQL データベースのバックアップを作成し、**tmsng.bak** ファイルを新 SQL Server にコピーします。
  - a. **tmsng** データベースを右クリックします。
  - b. **【タスク (Tasks)】 > 【バックアップ... (Back Up...)】** の順に選択します。 > **【データベース (Database...)】** を選択します。
  - c. バックアップ先のパスをメモし、**【OK】** をクリックします。
  - d. バックアップ先から新サーバー上に **tmsng.bak** ファイルをコピーします。
3. SQL Server Management Studio Express を使用して SQL データベースを復元します。
  - a. **tmsng** データベースを右クリックします。
  - b. **【タスク (Tasks)】 > 【復元 (Restore)】 > 【データベース (Database)】** を選択します。
  - c. **【復元するバックアップセットのソースと場所を指定 (Specify the source and location of backup sets to restore)】** で **【デバイスから (From device)】** を選択し、**tmsng.bak** ファイルを保存した場所を参照します。
  - d. **【データベースの復元 - tmsng (Restore Database - tmsng)】** ウィンドウに戻るまで **【OK】** をクリックします。
  - e. **【復元するバックアップ セットを選択 (Select the backup sets to restore)】** で該当するバックアップ ファイルの横の **【復元 (Restore)】** 列のチェックボックスをオンにします。 **【OK】** をクリックします。
4. Cisco TMS Server に移動し、TMS ツールを開きます。
5. **【構成 (Configuration)】 > 【Cisco TMS データベース接続 (Cisco TMS Database Connection)】** の順に選択し、**【データベースサーバー/インスタンス (Database Server\Instance)】** テキストフィールドにデータベースサーバーとインスタンスを入力します。 **【保存 (Save)】** をクリックします。
6. すべての TMS サービスと IIS を開始します。
7. Cisco TMS Web アプリケーションを開き、アプリケーションが動作しているかと、各場所にあるすべてのデータを確認します。

## TMS Log Collector のアンインストール

1. **TLCSetup** をダブルクリックします  
または  
**【コントロール (Control)】** パネル > **【プログラムのインストール (Uninstall Programs)】 > 【TMS Log Collector】 > 【アンインストール (Uninstall)】** の順に選択します。

2. **[TLC Logsetup を削除 (Remove TLC Logsetup) ]** を選択します。



3. **[Finish]** をクリックします。

注：アンインストール手順では、TMS Log Collector のログファイルは削除されません。削除は手動で行う必要があります。

## トラブルシューティング

## トラブルシューティング

## インストールのタイムアウト

Cisco TMS をアップグレードするときのデフォルトのデータベースのタイムアウト値は 30 分です。この値は、インストーラの内部データベース操作のそれぞれに適用されます。数年分の通話履歴やシステム データを含む大規模導入では、一部の操作は完了までに 30 分以上かかる場合があります。

このタイムアウト値はコマンドライン オプションを使用して設定できます。60 分のタイムアウト値を使用するには、コマンドラインから次のようにインストーラを実行します。

```
TMS15.13.5.exe /z"sqltimeout 60"
```

必要に応じて、60 をさらに大きい値に置き換えることができます。

デフォルト値の 30 分を使用し、最初のアップグレードの試みが失敗した場合にのみタイムアウト値を増やすことを推奨します。

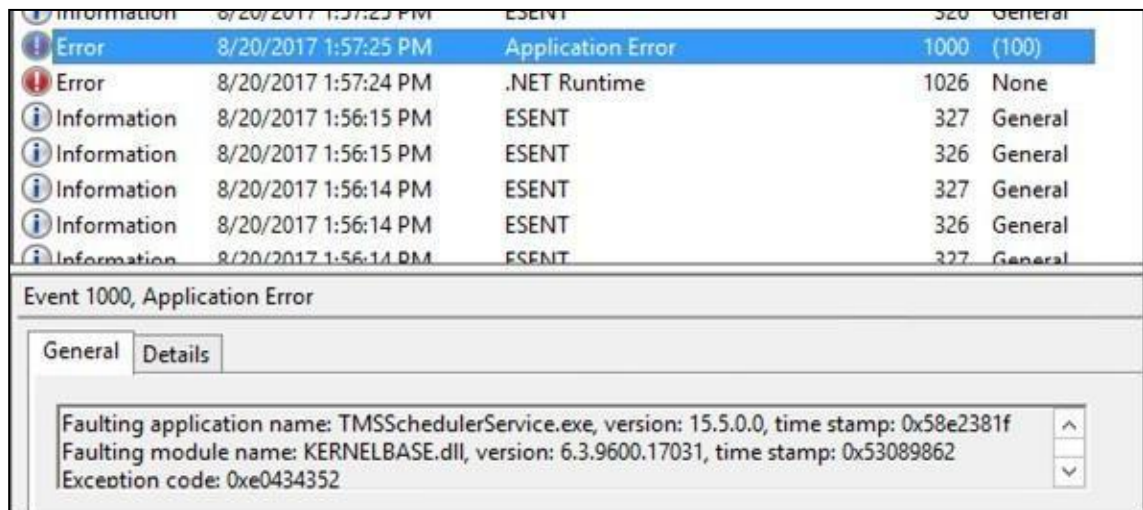
## Windows OS ソフトウェアを 2008R2 から 2012R2 にアップグレードすると、「TMSSchedulerService」が停止します

Cisco TMS 15.5 バージョン以下の Windows OS ソフトウェアを 2008R2 から 2012R2 にアップグレードすると、**TMSSchedulerService** が停止することがあります。

## トラブルシューティングの手順

この問題のトラブルシューティングを行うには、次の手順を実行する必要があります。

1. イベントビューア ([スタートメニュー (Startmenu) ]>> [イベントビューア (Event Viewer) ]>> [Windows ログ (Windows Logs) ]>> [アプリケーション (Application) ]) で確認すると、次のエラーメッセージが表示されます。



2. これらのメッセージは、Windows のアップグレードの後に .Net framework 4.5 がクラッシュしたため、**TMSSchedulerService** が停止したことを示しています。

## ソリューション

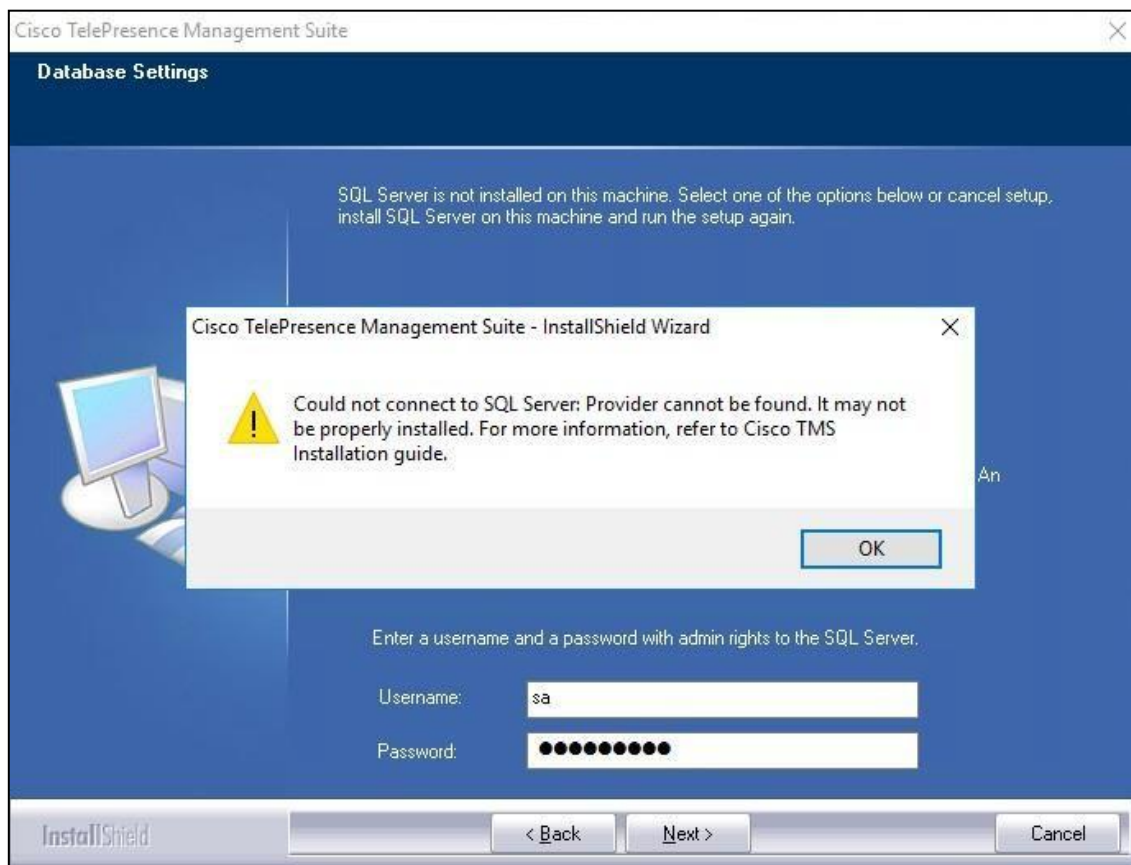
次の手順を実行して問題を解決します。

## トラブルシューティング

1. 次の Microsoft リンクから **KB3186539** Windows Update パッチをダウンロードしてインストールし、サーバーを再起動します。  
<https://www.catalog.update.microsoft.com/Search.aspx?q=KB3186539>
2. 正常に更新されると、.Net Framework 4.7 がアクティブになり、**TMSSchedulerService** が完全に機能することに注意してください。

## SQL Server 接続の問題により、Cisco TMS のインストールまたはアップグレードが終了した

SQL Server プロバイダーが見つからない場合、SQL Server 接続の問題により、Cisco TMS のインストールまたはアップグレードが中止されます。次のエラー メッセージが表示されます。



## トラブルシューティングの手順

この問題のトラブルシューティングを行うには、次の手順を実行する必要があります。

1. デフォルトでは、Windows Server のインストールには SQL Native Client は含まれていません。
2. 同じ Windows Server 上に SQL と Cisco TMS アプリケーションの両方がある展開では、SQL Server のインストールがそれをカバーするため、Cisco TMS は SQL Native Client のインストールを明示的に要求しません。

## 解決策

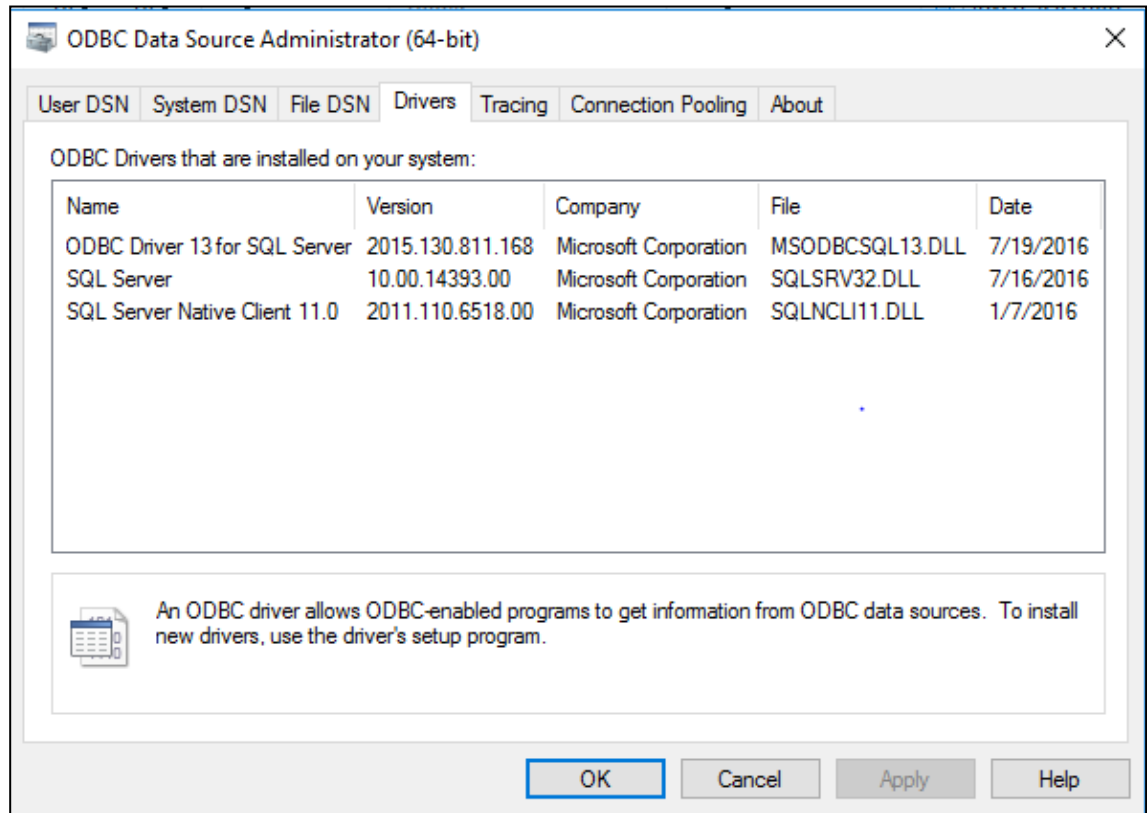
次の手順を実行して問題を解決します。

## トラブルシューティング

1. SQL と TMS アプリケーションが異なる Windows Server にある展開では、管理者は TMS アプリケーションをインストールする前に SQL Native Client 11 をインストールする必要があります。

- SQL ネイティブクライアントは、次のリンクからダウンロードできます。
  - SQL Server 2012 - <https://www.microsoft.com/en-us/download/details.aspx?id=50402>
  - SQL Server 2016 (13.0.1601.5 以降) - <https://www.microsoft.com/en-us/download/details.aspx?id=56833>

Microsoft リンク機能バックのバージョンは **13.0.1601.5** であり、SQL Server Native Client が Windows Server にインストールされている場合、インストールされているバージョンは **2011.110.6518.00** であることに注意してください。

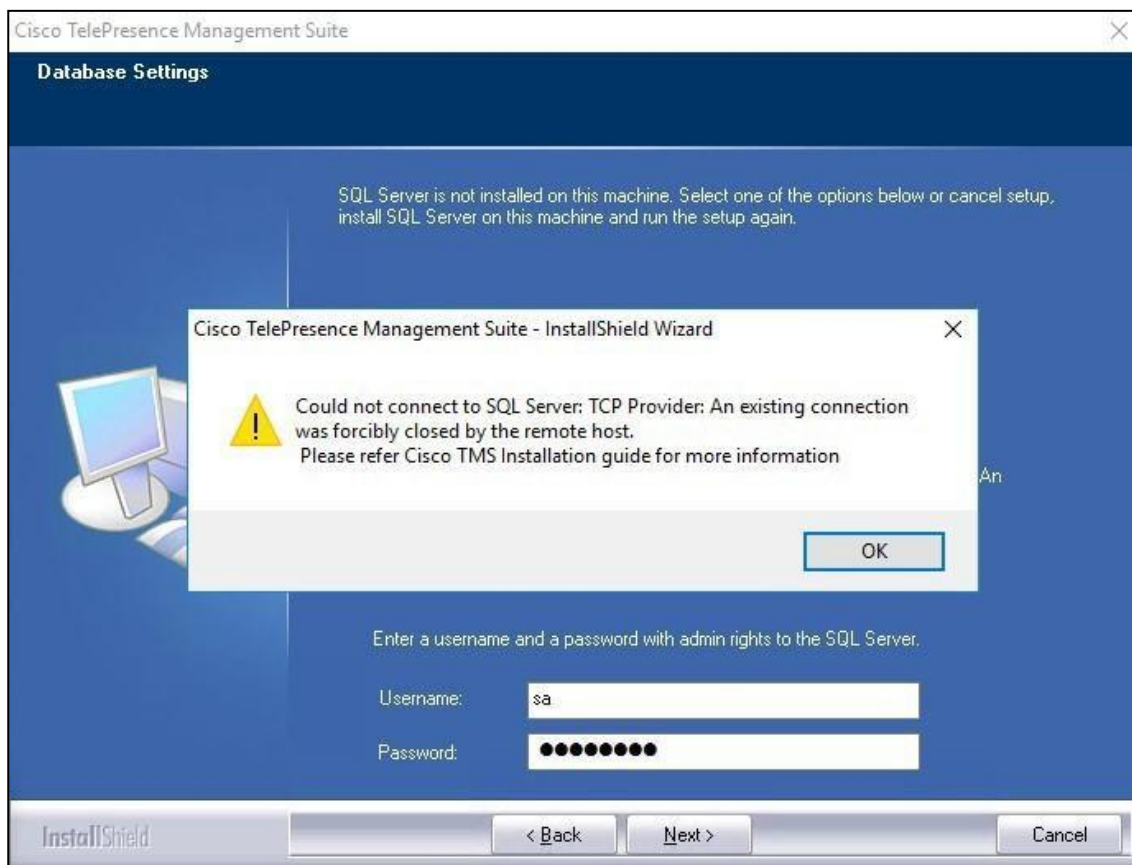


TLSv1.0 が無効になっている場合、Windows Server 2016/2012R2 での Cisco TMS のインストールまたはアップグレードが終了する

TLS バージョン 1.0 が無効になっている場合、Windows Server 2016/2012R2 での Cisco TMS のインストールまたはアップグレードは中止されます。次のエラー メッセージが表示されます。



## トラブルシューティング



## トラブルシューティングの手順

この問題のトラブルシューティングを行うには、次の手順を実行する必要があります。

1. (HKey\_Local\_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols) TLSv1.0 が無効になっている場合は、Windows レジストリを確認します。

## 解決策

次の手順を実行して問題を解決します。

1. 次の SQL Server Native Client をダウンロードしてインストールします。
  - SQL Server 2012  
<https://www.microsoft.com/en-us/download/details.aspx?id=50402>
  - SQL Server 2016 (13.0.1601.5 以降)  
<https://www.microsoft.com/en-us/download/details.aspx?id=56833>



# 付録

付録 1 : IIS モジュールを必要最低限に制限する	72
付録 2 : スпам防止の IIS リクエストの構成	73
Cisco TMS バンドル	77

## 付録 1 : IIS モジュールを必要最低限に制限する

IIS では、セキュリティを最高の状態に保つために、サーバーにインストールして有効にするコンポーネントを管理者が微調整できるモジュラーシステムがあります。サーバーをさらに制限したいと考えている管理者のために、Cisco TMS の必須モジュールの一覧を以下に示します。モジュールは、サイト レベルまたはサーバ レベルのいずれかで制御されます（一部はサーバ レベルのみです）。下記の手順では、サーバ レベルで変更を加えることを想定しています。

モジュールを削除する前に、コマンド `%windir%\system32\inetsrv\appcmd.exe add backup "TMS".` を使用して、IIS 構成をバックアップすることを推奨します。

後でバックアップを復元する必要がある場合は、コマンド `%windir%\system32\inetsrv\appcmd.exe restore backup "TMS"` を使用します。

IIS の有効化モジュールを変更するには、次の手順を実行します。

1. インターネット インフォメーション サービス (IIS) マネージャを開きます。
2. 左側のセクションのツリーから、サーバ名をクリックします。
3. 中央のセクションの [IIS] で [モジュール (Modules)] をダブルクリックします。  
インストールされているマネージド モジュールとネイティブ モジュールの一覧が表示されます。
4. モジュールを削除するには、そのエントリを右クリックするか、エントリを選択したら、[操作 (Actions)] パネルに移動し、[削除 (Remove)] を選択します。

次のモジュールは Cisco TMS に必要なので、**削除しない**でください。

- **AnonymousAuthenticationModule**
- **BasicAuthenticationModule**
- **DefaultDocumentModule**
- **DefaultAuthentication**
- **DigestAuthenticationModule**
- **HttpCacheModule**
- **HttpLoggingModule (推奨)**
- **HttpRedirectModule**
- **IsapiFilterModule**
- **ProtocolSupportModule**
- **RequestFilteringModule**
- **Session**
- **StaticCompressionModule**
- **StaticFileModule**
- **WindowsAuthentication**
- **WindowsAuthenticationModule**

Cisco Systems, Inc. [www.cisco.com](http://www.cisco.com)



## 付録 2：スパム防止の IIS リクエストの構成

システムからの非常に多くの同時着信リクエストのスパム攻撃に対して、Cisco TMS の安定性を守り、保護するため、サーバーで IIS スパム保護を構成することをお勧めします。

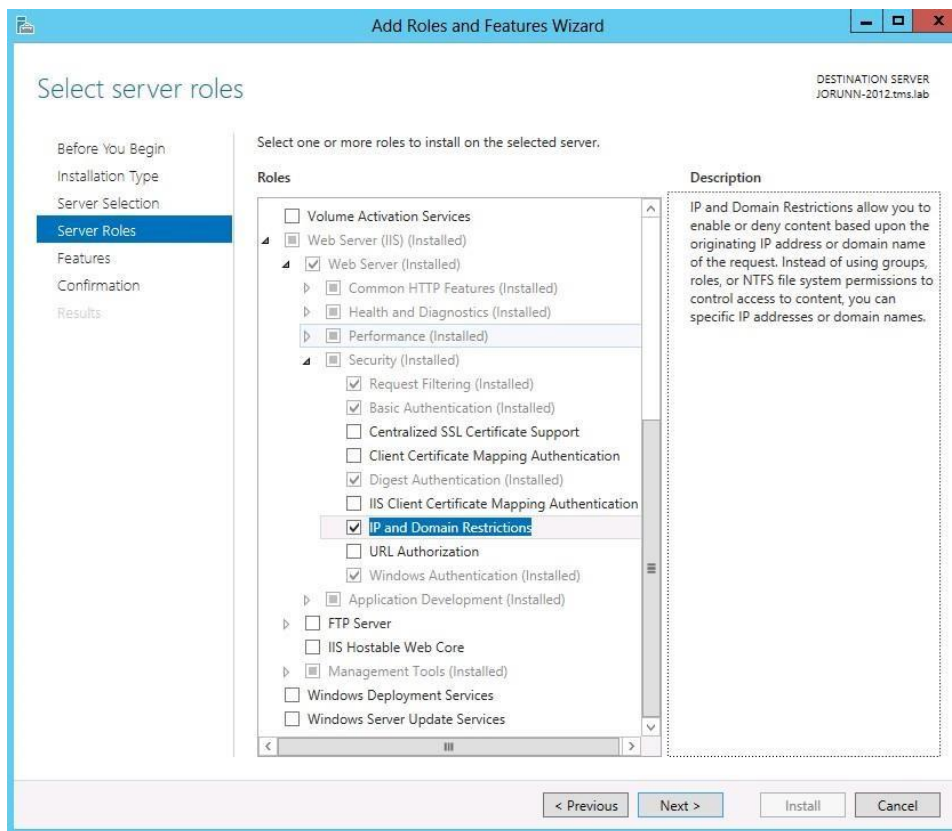
推奨される値での設定手順を次に示します。

### IIS 8 および 8.5

サーバーが IIS 8 と 8.5 で実行されている場合は、以下の手順を実行します。

#### IP と ドメイン制限ロールの有効化

1. [サーバー マネージャー (Server Manager)] を開きます。
2. スタート ページで[役割と機能の追加 (Add Roles and Features)] をクリックします。ロールと機能の追加ウィザードの [はじめる前に (Before you begin)] 画面が表示されます。
3. 説明されているサーバとパスワードの前提条件が満たされていることを確認し、[次へ (Next)] をクリックします。**[インストールタイプ (Installation type)]** 画面を表示します。
4. **[職務 (Role-based)]** または **[機能ベース (feature-based)]** インストールを選択し、**[次へ (Next)]** をクリックします。  
**[サーバー選択 (Server selection)]** 画面が表示されます。
5. **[サーバープールからサーバーを選択 (Select a server from the server pool)]** オプションを選択し、正しいサーバーが選択されているかを確認したら、**[次へ (Next)]** をクリックします。  
**[サーバーロールを選択 (Select server roles)]** 画面が表示されます。



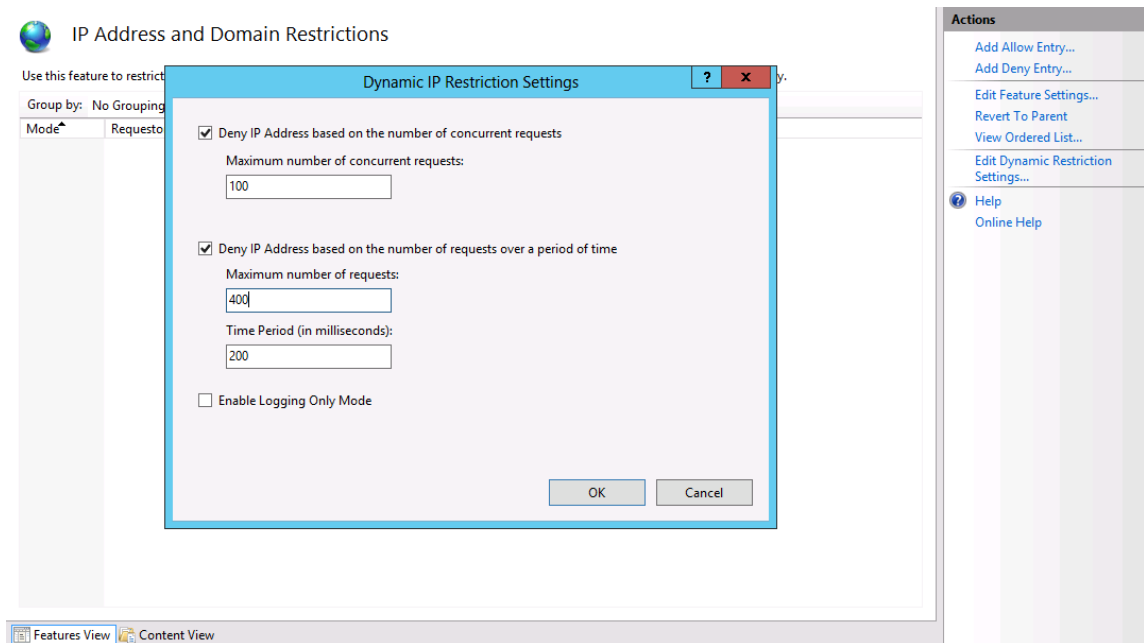
## 付録

6. [ロール (Roles) ] ペインで、[Web サーバー (IIS) (Web Server (IIS)) ] > [Web サーバー (Web Server) ] > [セキュリティ (Security) ] の順に展開し、[IP およびドメイン制限 (P and Domain Restrictions) ] をオンしたら、[次へ (Next) ] をクリックします。  
[機能 (Features) ] 画面が表示されます。
7. [Next] をクリックします。  
[確認 (Confirmation) ] 画面が表示されます。
8. [インストール (Install) ] をクリックします。  
インストールが完了したらウィザードを閉じます。

## デフォルトサイトへの Dynamic IP Restriction の構成

IIS マネージャで次の手順を実行します。

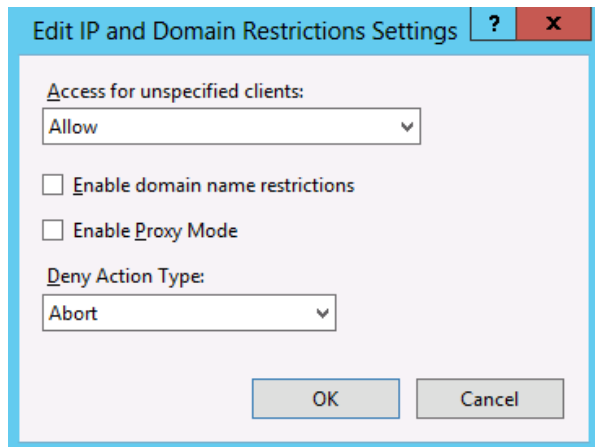
1. 左側のパネルで、[既定の Web サイト (Default Website) ] に移動し、エントリをクリックして [既定の Web サイトホーム (Default Web Site Home) ] を表示します。
2. [IIS] セクションの [IP アドレスおよびドメインの制限 (IP Address and Domain Restrictions) ] をダブルクリックします。
3. 右の [操作 (Actions) ] パネルの [動的制限設定の編集 (Edit Dynamic Restriction Settings) ] をクリックします。  
[Dynamic IP Restriction] ダイアログが開きます。



4. このダイアログで以下を行います。
  - a. [同時要求の数に基づいて IP アドレスを拒否する (Deny IP Address based on the number of concurrent requests) ] をオンにし、最大数を 100 に設定します。
  - b. [一定時間の要求数に基づいて IP アドレスを拒否する (Deny IP Address based on the number of requests over a period of time) ] をオンにします。  
要求の最大数を 400 に、時間 (ミリ秒) を 200 に設定し、[OK] をクリックします。

## 付録

5. 右の [操作 (Actions)] パネルの [機能設定の編集 (Edit Feature Settings)] をクリックします。  
[IP およびドメイン制限設定の編集 (Edit IP and Domain Restriction Settings)] ダイアログが表示されます。



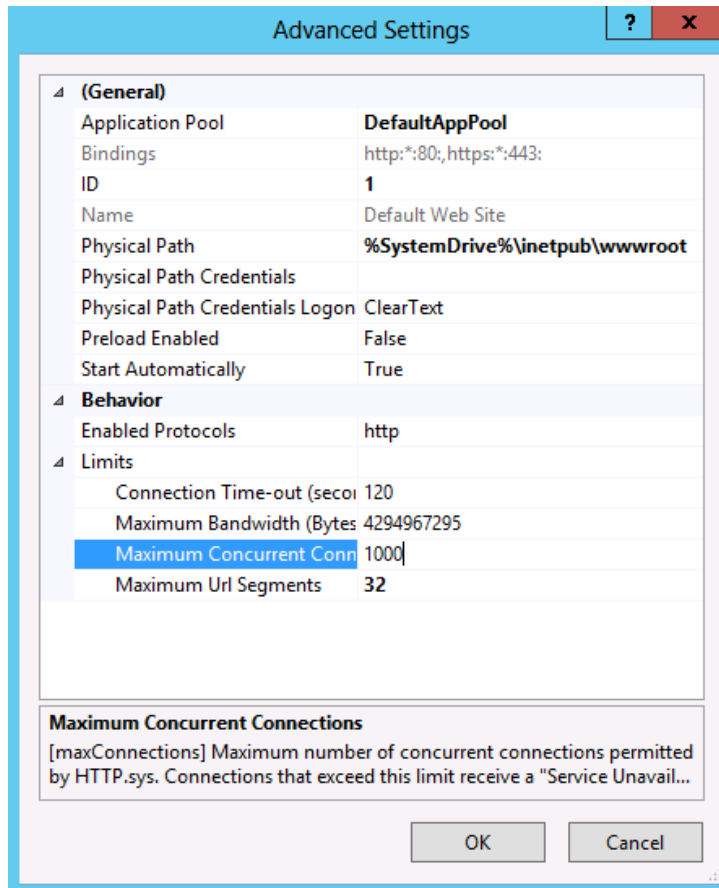
6. [拒否のアクションタイプ (Deny Action Type)] を [中止 (Abort)] に設定します。
7. [OK] をクリックします。

## 合計接続数の制限

IIS マネージャで次の手順を実行します。

## 付録

1. 左側のパネルで、**【既定の Web サイト (Default Website)】** に移動し、エントリをクリックして **【既定の Web サイトホーム (Default Web Site Home)】** を表示します。
2. 右側のパネルの **【詳細設定 (Advanced Settings)】** をクリックします。  
**【詳細設定 (Advanced Settings)】** ダイアログが表示されます。



3. **【動作 (Behavior)】 > 【制限 (Limits)】** で **【最大同時接続数 (Maximum Concurrent Connections)】** を 1000 に設定します。
4. **【OK】** をクリックして保存します。
5. IIS Manager を閉じます。

## IIS 7

お使いのサーバーで IIS バージョン 7 を実行している場合は、以下の手順を実行します。

## IIS 拡張機能のインストール

スパム攻撃の保護を構成する前に、IIS.NET から Dynamic IP Restrictions をダウンロードし、サーバー (<http://www.iis.net/downloads/microsoft/dynamic-ip-restrictions>) にインストールする必要があります。

このダウンロードは Microsoft Web Platform Installer を使用します。

## デフォルトサイトへの Dynamic IP Restriction

IIS マネージャーで次の手順を実行します。

1. 左側のパネルで、**【既定の Web サイト (Default Website)】** に移動し、エントリをクリックして **【既定の Web サイトホーム (Default Web Site Home)】** を表示します。

## 付録

2. **[動的 IP 制限 (Dynamic IP Restrictions)]** をダブルクリックします。
3. **[同時要求の数に基づいて IP アドレスを拒否する (Deny IP addresses based on the number of concurrent requests)]** をオンにし、最大数を 100 に設定します。
4. **[一定時間の要求数に基づいて IP アドレスを拒否する (Deny IP addresses based on the number of requests over a period of time)]** をオンにします。  
要求の最大数を 400 に、時間 (ミリ秒) を 200 に設定します。
5. **[拒否のアクションタイプ (Deny Action Type)]** ドロップダウンから **[要求を中止 (接続の終了) (Abort Request (Close Connection))]** を選択します。
6. **[適用 (Apply)]** をクリックして、変更内容を保存します。

IIS マネージャを開いたままにし、合計同時接続数の制限に移ります。

## 合計接続数の制限

IIS マネージャで次の手順を実行します。

1. 左側のパネルで、**[既定の Web サイト (Default Website)]** に移動し、エントリをクリックして **[既定の Web サイトホーム (Default Web Site Home)]** を表示します。
2. 右側のパネルの **[詳細設定... (Advanced Settings...)]** をクリックします。
3. **[動作 (Behavior)]** > **[接続制限 (Connection Limits)]** で **[最大同時接続数 (Maximum Concurrent Connections)]** を 1000 に設定します。
4. **[OK]** をクリックして保存します。
5. IIS Manager を閉じます。

詳細については、IIS.NET の項目 [Using Dynamic IP Restrictions](#) を参照してください。

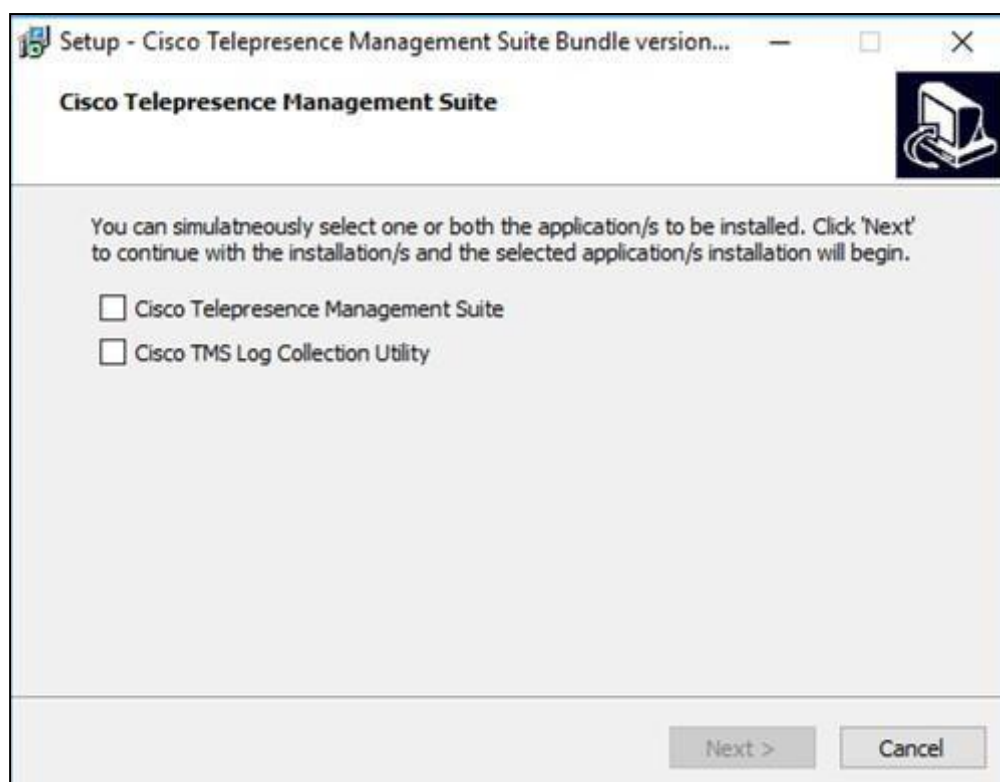
## Cisco TMS バンドル

Cisco TMS は、Cisco TMS Log Collection Utility ツールにバンドルされたインストーラを提供します。

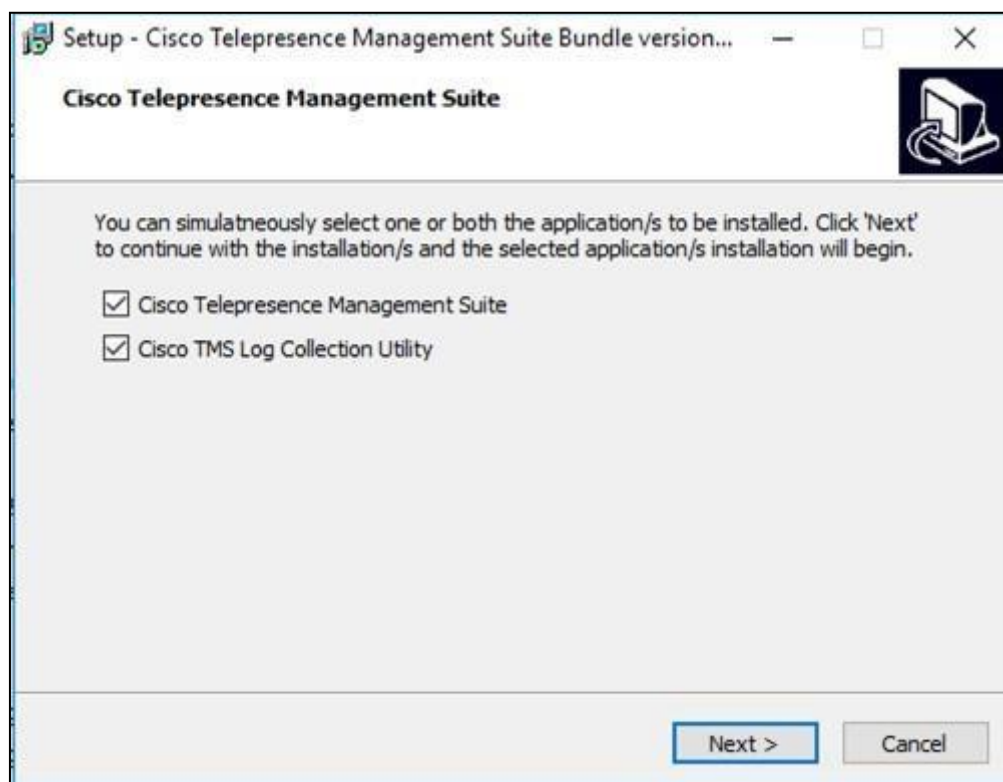
## インストーラの実行

1. すべてのアプリケーションを終了し、ウィルス スキャン ソフトウェアやその他ソフトウェアなどインストールの実行を妨げる恐れのあるソフトウェアを無効にします。
2. **Cisco TMS.zip** アーカイブをフォルダに展開します。
3. **Cisco TMS** の実行可能ファイルを管理者として実行します。
4. インストーラは、サーバーのハードウェアとソフトウェアの構成をチェックします。サーバーの構成によっては、警告またはエラーメッセージが表示される場合があります。プロンプトの指示に従って、不足しているコンポーネントをインストールします。
5. インストーラパッケージを実行すると、次の 2 つのオプションを含むダイアログボックスが表示されます。
  - a. Cisco TelePresence Management Suite (TMS)。
  - b. Cisco TMS Collection Utility。

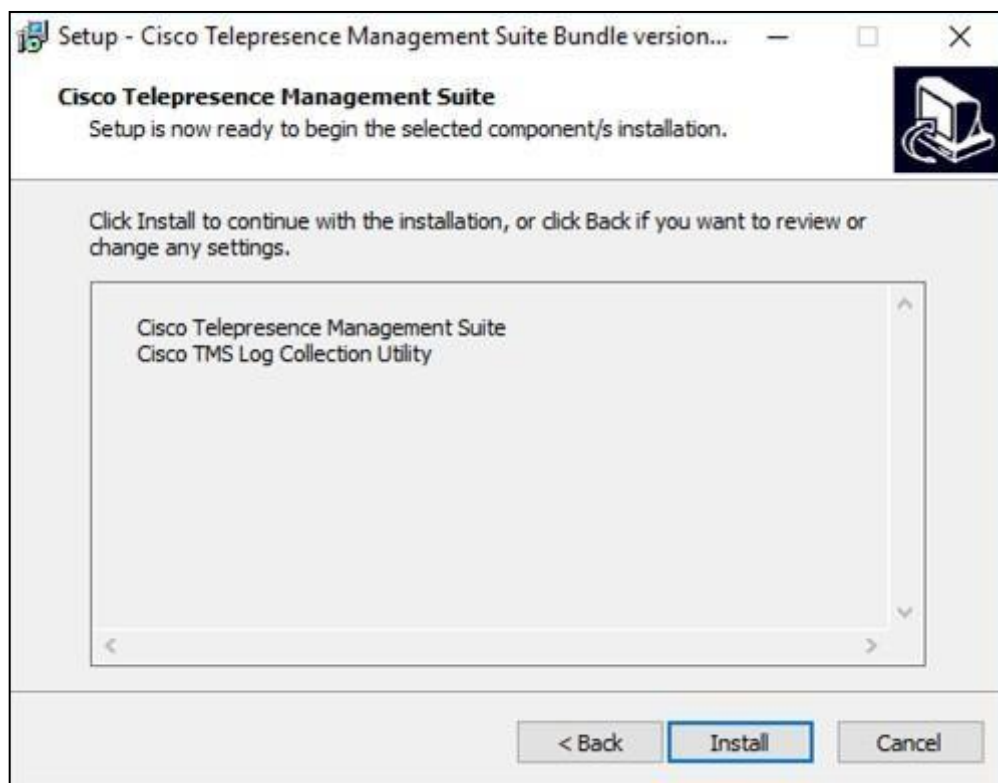
注：いずれか 1 つのアプリケーションを選択した場合、その特定のアプリケーションのみがインストールされます。



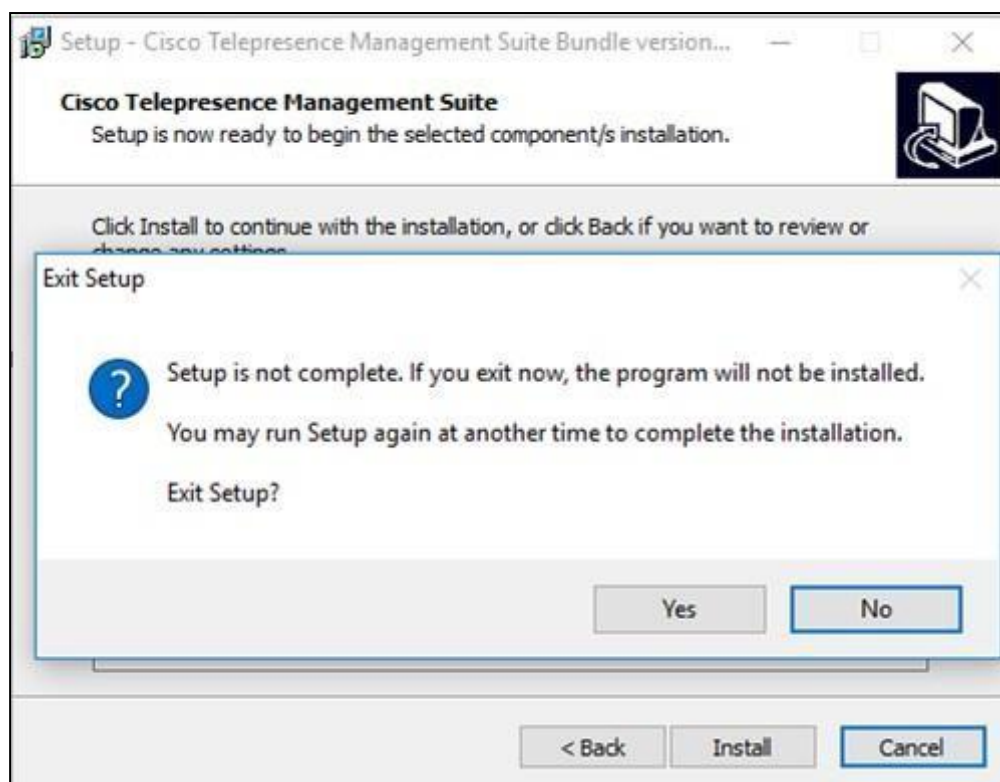
6. 選択に基づいて、アプリケーションの両方またはいずれかを選択できます。



7. **[次へ (Next)]** をクリックしてインストールを続行します。
8. **[インストール (Install)]** をクリックして、選択したアプリケーションをインストールします。

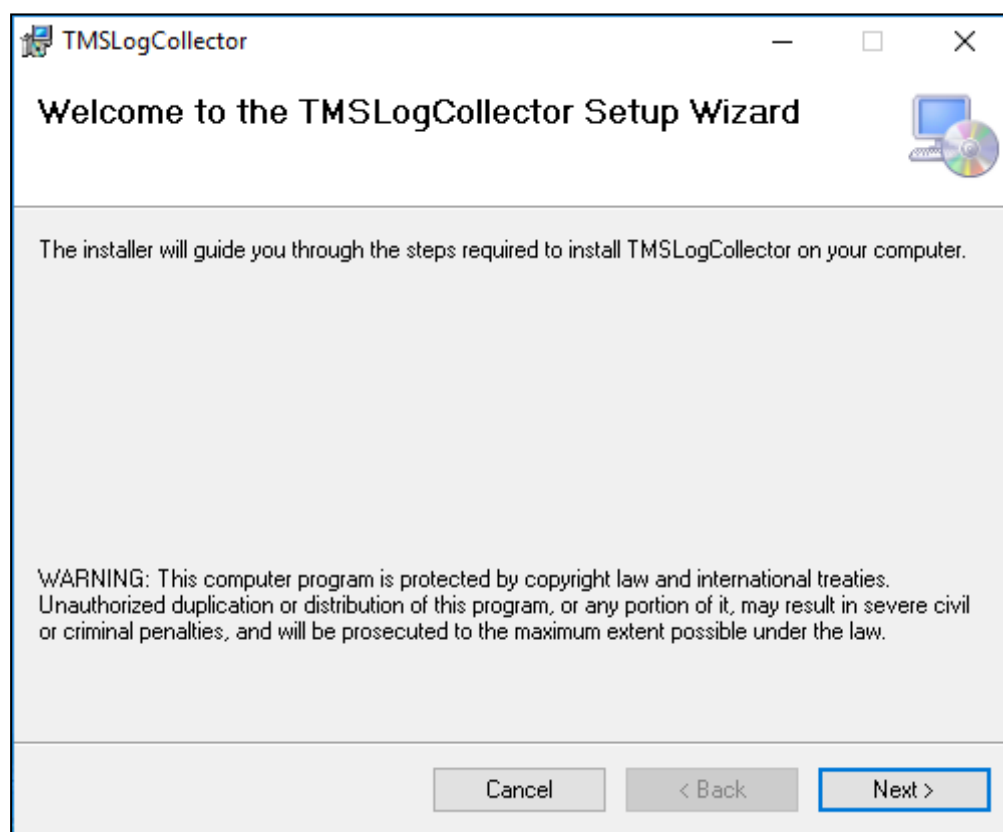


注：インストールプロセスを中止するために **[キャンセル (Cancel)]** をクリックすると、インストールの終了を確認するダイアログボックスが表示されます。

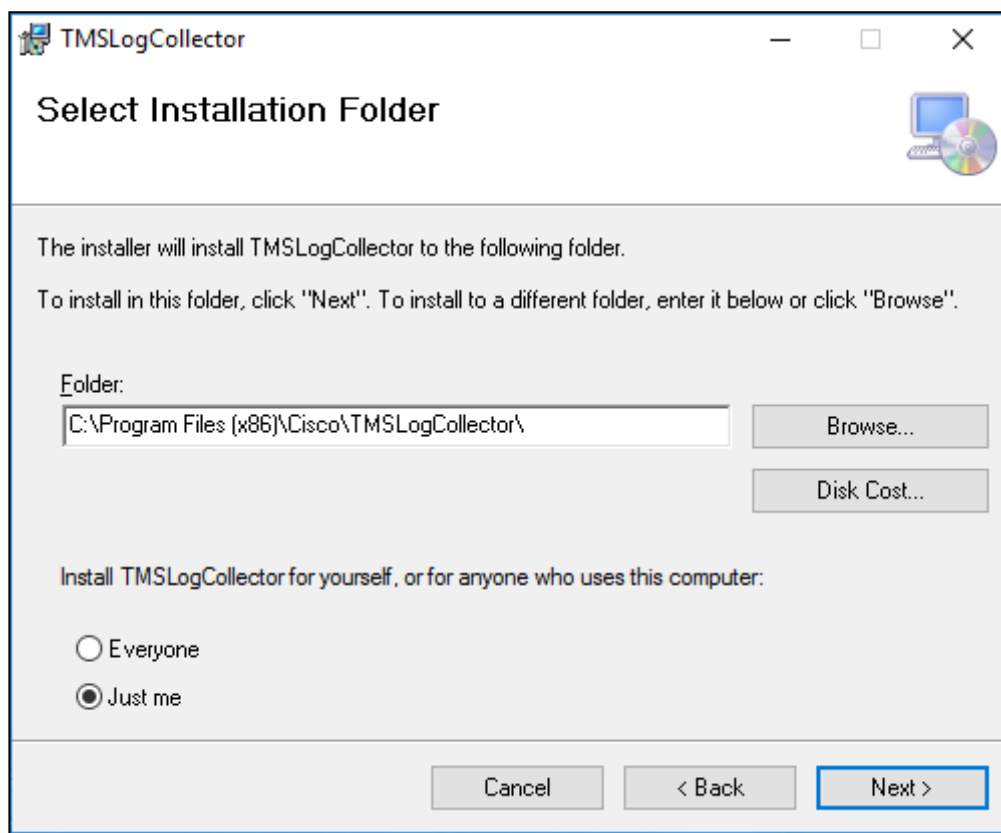


9. Cisco TMS のインストールについては、『Cisco TMS 設置ガイド』の「インストーラの実行」セクションのステップ 5 に記載されている手順に従ってください。
10. Cisco TMS のインストールが完了すると、TLCU のインストールが続行されます。[次へ (Next)] をクリックして続行します。

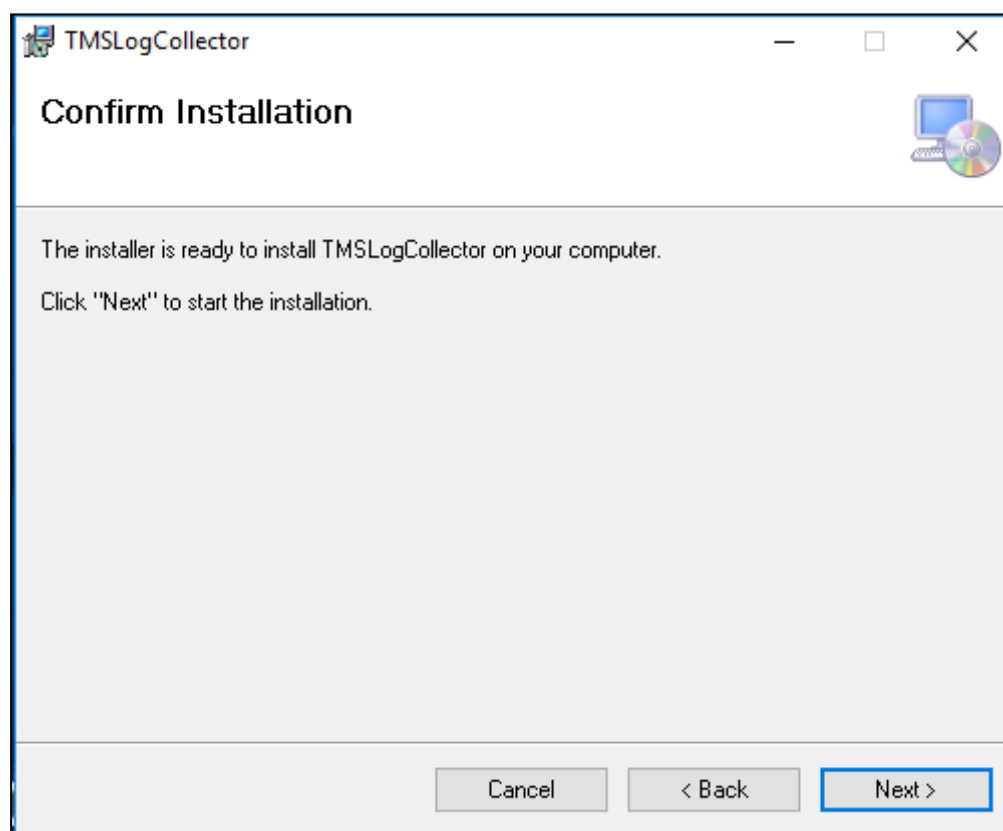




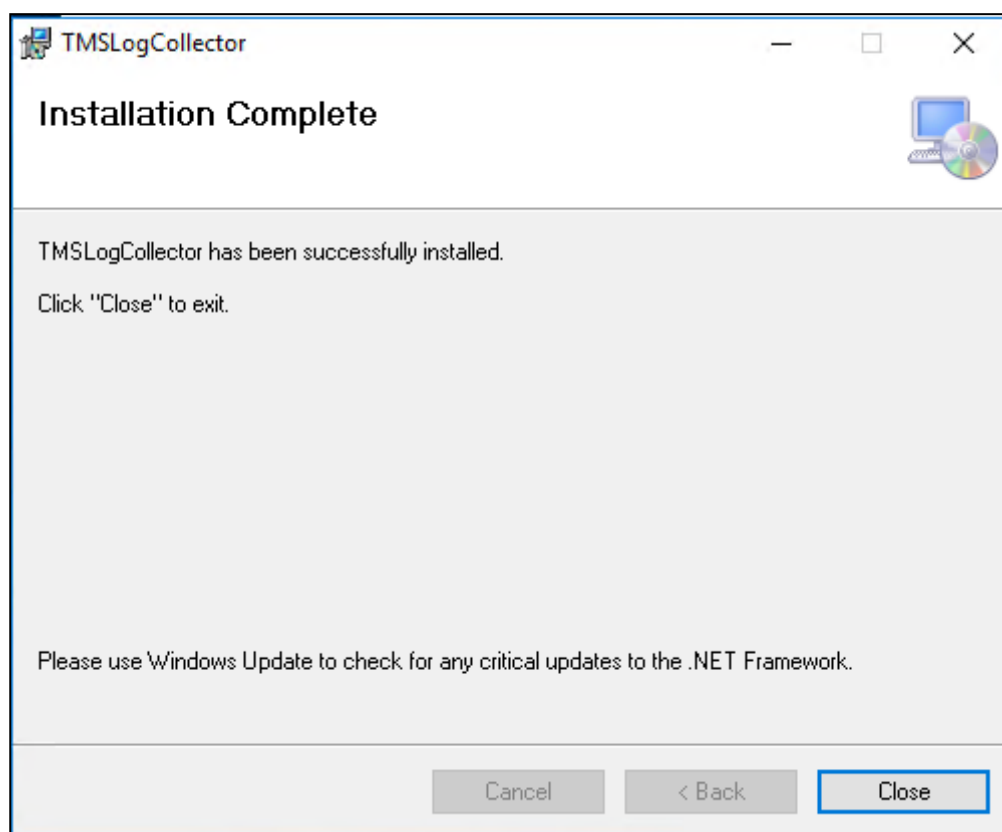
11. 自分用または全員用に TLCU をインストールする場合は、オプションを選択します。[次へ (Next)] をクリックして続行します。



12. [次へ (Next) ] をクリックしてインストールを開始します。



13. インストールが正常に完了したら、**【閉じる (Close)】**をクリックして終了します。



14. 両方のアプリケーションがすでにインストールされていて、ユーザーがインストーラパッケージを再度実行しようとする  
ると、TMS は元の動作に従って動作します。つまり、最初にアンインストールしてから、パッケージを再度インストー  
ルする必要があります。また、TLCU の場合、TLCU を修復または削除するためのダイアログボックスが表示されます。



## 注意事項

## 注意事項

### アクセシビリティ通知

シスコは、利用しやすい製品およびテクノロジーの設計および提供に取り組んでいます。

Cisco TelePresence Management Suite の Voluntary Product Accessibility Template (VPAT) は、ここで入手可能です。

[http://www.cisco.com/web/about/responsibility/accessibility/legal\\_regulatory/vpats.html#telepresence](http://www.cisco.com/web/about/responsibility/accessibility/legal_regulatory/vpats.html#telepresence) [英語]

アクセシビリティの詳細については、次を参照してください。

[www.cisco.com/web/about/responsibility/accessibility/index.html](http://www.cisco.com/web/about/responsibility/accessibility/index.html) [英語]

## Cisco の法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本書に組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または黙示のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

印刷版と複製ソフトは公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。住所、電話番号、FAX 番号はシスコの Web サイト ([www.cisco.com/go/offices](http://www.cisco.com/go/offices)) をご覧ください。

© 2014– 2023 Cisco Systems, Inc. All rights reserved.

## Cisco の商標または登録商標

Cisco および Cisco ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の国における登録商標または商標です。シスコの商標の一覧については、<http://www.cisco.com/jp/go/trademarks> をご覧ください。Third-party trademarks mentioned are the property of their respective owners. 「パートナー」という言葉が使用されていても、シスコと他社の間にパートナーシップ関係が存在することを意味するものではありません。(1721R)