Cisco TMS へのシステム フィードバックが、ネットワークまたは Web サーバによってブロックされます。

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[Cisco TMS へのシステム フィードバックが、ネットワークまたは Web サーバによってブロックされます。](#)

概要

このドキュメントでは、ネットワークまたは Web サーバによってブロックされた Cisco TelePresence Management Suite（TMS）へのフィードバックの問題をトラブルシューティングする方法について説明します。

前提条件

要件

Cisco TMS に関する基本的な知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、Cisco TMS に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

Cisco TMS へのシステム フィードバックが、ネットワークまたは Web サーバによってブロックされます。

Cisco TMS は、システムから送信されるフィードバックで通知されるシリアル番号、MAC アドレス、および IP アドレスに基づき、接続してくるエンドポイントを確認します。Cisco TelePresence およびサードパーティ システムのほとんどは、このフィードバックを匿名 HTTP または HTTPS 接続で送信しますが、認証を要求する Web プロキシがネットワーク上に存在すると、接続がブロックされる場合があります。この場合、プロキシの管理者に連絡して、Cisco TMS 宛てのトラフィックに対する例外を追加してもらう必要があります。

また、ファイアウォールがシステムから Cisco TMS への新しい接続をブロックするように設定されている場合も、ファイアウォールによって Cisco TMS へのフィードバックがブロックされます。

> **ヒント**：Cisco TMS サポート ドキュメントで、システムのタイプごとに利用可能にする必要があるポートとプロトコルについて概説しています。

よくある接続失敗の別の例として、Cisco TMS がインストールされた後、管理者が手動でインターネット インフォメーション サービス (IIS) を変更して Web ディレクトリへの匿名アドレスを無効にした場合も、接続が失敗します。

> **注**：匿名アクセスは Cisco TMS の特定の部分に対してのみオープンになり、システムはフィードバックの送信時にユーザ名とパスワードを使用しません。したがって、匿名アクセスを無効にしてはなりません。

IIS の誤った設定を修正するには、Cisco TMS をアンインストールしてから再インストールします。データベースの状態はそのままで、インストーラによって Web サイトのプロパティが適切に復元される限り、データ損失は発生しません。