



TS エージェントのインストールと設定

- [TS エージェントのインストールまたはアップグレード](#) (1 ページ)
- [TS エージェント設定インターフェイスの開始](#) (2 ページ)
- [TS エージェントの設定](#) (2 ページ)
- [REST VDI ロールの作成](#) (19 ページ)

TS エージェントのインストールまたはアップグレード

始める前に

- [サーバおよびシステム環境要件](#)の説明に従って、TS エージェントがお使いの環境でサポートされていることを確認してください。
- [現在のユーザセッションの終了](#)の説明に従って、現在のすべてのユーザセッションを終了してください。

ステップ 1 管理者特権を持つユーザとしてサーバにログインします。

ステップ 2 サポートサイトから、TS エージェントパッケージをダウンロードします。TSAgent-1.3.0.exe

(注) サイトから更新プログラムを直接ダウンロードします。ファイルを電子メールで転送すると、破損することがあります。

ステップ 3 [TSAgent-1.3.0.exe] を右クリックし、[管理者として実行 (Run as Administrator)] を選択します。

ステップ 4 [インストール (Install)] をクリックして、TS エージェントをインストールまたはアップグレードするための指示に従います。

TS エージェントを使用する前に、コンピュータを再起動する必要があります。

次のタスク

- [TS エージェント サービス コンポーネントの状態の表示](#)の説明に従って、TS エージェントが実行されていることを確認します。

- TS エージェントプロセスの開始と停止の説明に従って、TS エージェントを起動します。
- TS エージェントの設定 (2 ページ) の説明に従って、TS エージェントを設定します。

以前のバージョンの TS エージェントからアップグレードし、Citrix Provisioning を使用している場合は、アップグレード後に [予約ポート (Reserve Port(s))] フィールドに 6910 と入力する必要があります。



(注) TS エージェント インストーラによって .NET Framework の失敗が報告された場合、Windows Update を実行し、TS エージェントのインストールを再試行してください。

TS エージェント設定インターフェイスの開始

cite

TS エージェントのショートカットがデスクトップ上にある場合は、ショートカットをダブルクリックします。そうでない場合、TS エージェント設定インターフェイスを起動するには、次の手順を使用します。

ステップ 1 管理者特権を持つユーザとしてサーバにログインします。

ステップ 2 C:\Program Files (x86)\Cisco\Terminal Services Agent を開きます。

ステップ 3 TS エージェントのプログラム ファイルを表示します。

(注) このプログラムファイルは、表示専用です。これらのファイルは削除、移動、または変更しないでください。

ステップ 4 TSAgentApp ファイルをダブルクリックして、TS エージェントを開始します。

TS エージェントの設定

TS エージェントを設定するには、TS エージェントインターフェイスを使用します。変更を有効にするには、変更を保存してサーバを再起動する必要があります。

始める前に

- Firepower システムに接続する場合は、『*Firepower Management Center Configuration Guide*』の説明に従って、お使いのサーバがモニタするユーザをターゲットにした Active Directory レルムを 1 つ以上設定し、有効化します。
- Firepower システムに接続する場合は、REST VDI 特権を持つユーザ アカウントを設定します。

REST VDI ロールの作成 (19 ページ) の説明に従って、Firepower Management Center 内に REST VDI ロールを作成する必要があります。

- Firepower システムにすでに接続しており、かつ別の Firepower Management Center に接続するように TS エージェントの設定を更新する場合は、新しい設定を保存する前に、現在のすべてのユーザセッションを終了する必要があります。詳細については、[現在のユーザセッションの終了](#)を参照してください。
- TS エージェント サーバと Firepower システムの時計を同期させます。
- [TS エージェントの設定フィールド \(4 ページ\)](#) の説明に従って、設定フィールドを確認し、理解してください。

-
- ステップ 1** [TS エージェント設定インターフェイスの開始 \(2 ページ\)](#) の説明に従って、TS エージェントをインストールしたサーバで、TS エージェントを開始します。
- ステップ 2** [構成 (Configure)] をクリックします。
- ステップ 3** タブ ページの [全般設定 (General Settings)] セクションに移動します。
- ステップ 4** [最大ユーザセッション (Max User Sessions)] の値を入力します。
- ステップ 5** ポート変換および通信に使用する [サーバ NIC (Server NIC)] を選択します。
- サーバの IP アドレスが後で変更された場合は、設定を保存し、変更を有効にするためにサーバを再起動するように求められます。
- ステップ 6** [システム ポート (System Ports)] および [ユーザ ポート (User Ports)] の値を入力します。有効な設定では、システム ポートとユーザ ポートの範囲が重複しません。
- ステップ 7** [予約ポート (Reserve Port(s))] の値をコンマ区切りのリストとして入力します。
- [予約ポート (Reserve Port(s))] には、Citrix MA クライアントのポート (2598) 、Citrix Provisioning のポート (6910) 、Windows ターミナルサーバのポート (3389) に想定される値が自動的に設定されます。Citrix MA クライアントと Windows ターミナル サーバのポートは、除外する必要があります。
- Citrix Provisioning を使用していて、以前の TS エージェントバージョンからアップグレードする場合は、このフィールドに 6910 と入力する必要があります。
- ステップ 8** タブの [Firepower Management Center REST API 接続 (Firepower Management Center REST API Connection)] 設定セクションに移動します。
- ステップ 9** [ホスト (Host)]、[ホスト名/IP アドレス (Hostname/IP Address)]、および [ポート (Port)] の値を入力します。
- Firepower Management Center には、[ポート (Port)] 443 が必要です。ISE/ISE-PIC には、[ポート (Port)] 9094 が必要です。
- ステップ 10** [ユーザ名 (Username)] と [パスワード (Password)] を入力します。
- ステップ 11** 必要に応じ、2 番目の行のフィールドで手順 9 と 10 を繰り返し、スタンバイ (フェールオーバー) 接続を設定します。
- ステップ 12** [テスト (Test)] をクリックして、TS エージェントとシステムの間 REST API 接続をテストします。

プライマリとセカンダリの Firepower Management Center を設定している場合は、セカンダリへのテスト接続が失敗します。これは想定されている動作です。TS エージェントは、アクティブな Firepower Management Center と常に通信します。プライマリがダウンして非アクティブの Firepower Management Center になった場合、TS エージェントは、セカンダリの（アクティブになった） Firepower Management Center と通信します。

ステップ 13 [保存 (Save)] をクリックして、デバイスのリポートを確認します。

TS エージェントの設定フィールド

TS エージェントの設定には、次のフィールドを使用します。

全般設定

表 1: 全般設定フィールド

フィールド	説明	例
[予約ポート (Reserve Port(s))]		通常、次のいずれかです。 <ul style="list-style-type: none">• 2598、3389 (Citrix MA クライアントおよび Windows ターミナル サーバのポート)• 2598、3389、6910 (Citrix MA クライアント、Windows ターミナルサーバ、および Citrix Provisioning のポート)

フィールド	説明	例
	<p>TS エージェントに無視させるポート。除外したいポートをコンマ区切りのリストとして入力します。</p> <p>[予約ポート (Reserve Port(s))]には、Citrix MA クライアントのポート (2598) 、Citrix Provisioning のポート (6910) 、Windows ターミナルサーバのポート (3389) のデフォルト値がTS エージェントによって自動的に設定されます。正しいポートを除外しないと、これらのポートを必要とするアプリケーションが失敗する可能性があります。</p> <p>TS エージェントの [予約ポート (Reserve Port(s))]フィールドで指定する値は、Citrix Provisioning の [最初と最後のUDP ポート番号 (First and Last UDP port numbers)]のポートのいずれかと一致する必要があります。</p> <p>注意 正しいポートを指定しないと、クライアントの起動に失敗します。</p> <p>(注) お使いのサーバ上のプロセスが [システムポート (System Ports)]の範囲にならないポートを使用またはリスンしている場合、そのポートは、[予約ポート (Reserve Port(s))]フィールドを使用して手動で除外する必要があります。</p>	

フィールド	説明	例
	<p>(注) サーバにクライアントアプリケーションがインストールされていて、そのアプリケーションが特定のポート番号を使用するソケットにバインドするよう設定されている場合、[予約ポート (Reserve Port(s))]フィールドを使用して、そのポートを変換から除外する必要があります。</p>	
最大ユーザセッション (Max User Sessions)	<p>TS エージェントにモニタさせるユーザセッションの最大数。単一のユーザが一度に複数のユーザセッションを実行する場合があります。</p> <p>このバージョンのTS エージェントは、デフォルトで29のユーザセッションをサポートし、最大199のユーザセッションをサポートします。</p>	29 (このバージョンのTS エージェントがサポートする最大値)

フィールド	説明	例
サーバ NIC (Server NIC)		Ethernet 2 (192.0.2.1) (サーバ上の NIC)

フィールド	説明	例
	<p>このバージョンの TS エージェントでは、ポート変換およびサーバシステム間の通信に、単一のネットワーク インターフェイス コントローラ (NIC) を使用することができます。サーバに有効な NIC が 2 つ以上存在する場合、TS エージェントは、設定の際に指定されたアドレスに対してのみポートの変換を実行します。</p> <p>TS エージェントは、このフィールドに、TS エージェントがインストールされているサーバの各 NIC の IPv4 アドレスおよび/または IPv6 アドレスを自動的に設定します。有効な NIC には必ず、IPv4 もしくは IPv6 のアドレスが 1 つだけ、または各タイプのアドレスが 1 つずつあります。有効な NIC が同じ種類のアドレスを複数持つことはできません。</p> <p>(注) サーバの IP アドレスが変更された場合は、設定を保存し、変更を有効にするためにサーバを再起動するように求められます。</p> <p>(注) サーバに接続されているデバイスで、ルータアドバタイズメントメッセージを無効にする必要があります。ルータアドバタイズメントが有効になっていると、デバイスがサーバ上の NIC に複数の IPv6</p>	

フィールド	説明	例
	アドレスを割り当て、TSエージェントで使用するNICを無効にしてしまう可能性があります。	

フィールド	説明	例
システム ポート (System Ports)		[開始 (Start)] を 10000 に設定し、[範囲 (Range)] を 5000 に設定

フィールド	説明	例
	<p>システム プロセスに使用するポートの範囲。TS エージェントは、このアクティビティを無視します。[開始 (Start)] ポートを設定し、範囲を開始する場所を指定します。[範囲 (Range)] の値を設定し、個々のシステム プロセスに割り当てるポートの数を指定します。</p> <p>シスコが推奨する [範囲 (Range)] の値は、5000 以上です。TS エージェントでシステム プロセス用のポートが頻繁に不足する場合は、[範囲 (Range)] の値を大きくします。</p> <p>(注) システムプロセスが指定された [システムポート (System Ports)] の範囲外のポートを要求する場合は、そのポートを [除外ポート (Exclude Port(s))] フィールドに追加します。システムプロセスによって使用されるポートを [システムポート (System Ports)] の範囲に指定するか除外するかしないと、システムプロセスが失敗する可能性があります。</p> <p>TS エージェントは、次の数式を使用して、[終了 (End)] の値を自動的に設定します。</p> $([Start\ value] + [Range\ value]) - 1$ <p>入力の結果、[終了 (End)] の</p>	

フィールド	説明	例
	値が [ユーザ ポート (User Ports)] の [開始 (Start)] の値を超える場合、[開始 (Start)] および [範囲 (Range)] の値を調整する必要があります。	

フィールド	説明	例
ユーザ ポート (User Ports)	<p>ユーザ用に指定するポートの範囲。[開始 (Start)]ポートを設定し、範囲を開始する場所を指定します。[範囲 (Range)]の値を設定し、個々のユーザセッションにおける TCP または UDP 接続に割り当てるポートの数を指定します。</p> <p>(注) ICMP トラフィックは、ポートがマッピングされずに渡されます。</p> <p>シスコが推奨する [範囲 (Range)]の値は、1000 以上です。TS エージェントでユーザ トラフィック用のポートが頻繁に不足する場合は、[範囲 (Range)]の値を大きくします。</p> <p>(注) 使用されているポートの数が [範囲 (Range)]の値を超えると、ユーザ トラフィックがブロックされます。</p> <p>TS エージェントは、次の数式を使用して、[終了 (End)]の値を自動的に設定します。</p> $[\text{Start value}] + ([\text{Range value}] * [\text{Max User Sessions value}]) - 1$ <p>入力の結果、[終了 (End)]の値が 65535 を超える場合、[開始 (Start)]および [範囲 (Range)]の値を調整する必要があります。</p>	<p>[開始 (Start)]を 15000 に設定し、[範囲 (Range)]を 1000 に設定</p>

フィールド	説明	例
エフェメラル ポート	TS エージェントがモニタできるように、エフェメラルポートの範囲（ダイナミックポートとも呼ばれる）を入力します。	[開始 (Start)] を 49152 に設定し、[範囲 (Range)] を 16384 に設定

フィールド	説明	例
不明なトラフィック通信		適用対象外

フィールド	説明	例
	<p>[許可 (Permit)] をオンにして、TS エージェントがシステムポート経由のトラフィックを許可できるようにします。ただし、TS エージェントはポートの使用状況を追跡しません。システムポートは、ローカルシステムアカウントまたは他のローカルユーザアカウントによって使用されます (ローカルユーザアカウントはTS エージェントサーバにのみ存在します。対応する Active Directory アカウントはありません)。このオプションを選択すると、次のタイプのトラフィックを許可できます。</p> <ul style="list-style-type: none"> • ブロックされるのではなく、ローカルシステムアカウント (サーバメッセージブロック (SMB) など) によって実行されるトラフィックを許可します。ユーザが Active Directory に存在しないため、Firepower Management Center はこのトラフィックを不明なユーザからのトラフィックとして識別します。 <p>このオプションを有効にすると、ローカルシステムアカウントを使用してTS エージェントサーバにログインしている場合、Firepower Management Center との接続を正常にテストできます。</p> <ul style="list-style-type: none"> • ユーザまたはシステムセッションがその範囲内の使用可能なすべての 	

フィールド	説明	例
	<p>ポートを使い果たすと、TS エージェントはエフェメラルポート経由のトラフィックを許可します。このオプションは、トラフィックを有効にしません。Firepower Management Center は、不明なユーザからのトラフィックとして識別します。</p> <p>これは、ドメインコントローラの更新、認証、Windows Management Interface (WMI) クエリなど、システムの健全性を維持するためにシステムポートが必要な場合に特に役立ちます。</p> <p>システムポートのトラフィックをブロックするには、オフにします。</p>	

REST API 接続の設定

プライマリのシステムアプライアンスに加え、必要に応じてスタンバイ（フェールオーバー）のシステムアプライアンスの接続を設定することができます。

- システムアプライアンスがスタンドアロンの場合、REST API 接続フィールドの2番目の行は空白のままにします。
- システムアプライアンスをスタンバイ（フェールオーバー）アプライアンスとともに展開している場合、1番目の行はプライマリアプライアンスへの接続の設定に、2番目の行はスタンバイ（フェールオーバー）アプライアンスへの接続の設定に使用します。

表 2: REST API 接続設定用のフィールド

フィールド	説明	例
ホスト名/IP アドレス (Hostname/IP Address)	システムアプライアンスのホスト名または IP アドレス。	192.0.2.1

フィールド	説明	例
ポート (Port)	システムが REST API 通信に使用するポート。(Firepower Management Center では、通常はポート 443 が使用されます)。	443
ユーザ名とパスワード	接続のためのクレデンシャル。 <ul style="list-style-type: none"> • Firepower システムでは、Firepower Management Center で REST VDI 特権を持つユーザのユーザ名とパスワードが必要です。このユーザの設定に関する詳細については、『<i>Firepower Management Center Configuration Guide</i>』を参照してください。 	n/a

REST VDI ロールの作成

TS エージェントを Firepower Management Center に接続するには、お使いの Firepower ユーザが REST VDI ロールを持っている必要があります。REST VDI は、デフォルトでは定義されていません。ロールを作成し、TS エージェントの設定に使用するユーザに割り当てる必要があります。

ユーザおよびロールの詳細については、『*Firepower Management Center Configuration Guide*』を参照してください。

-
- ステップ 1** Firepower Management Center にロール作成の権限を持つユーザとしてログインします。
- ステップ 2** [システム (System)] > [ユーザ (Users)] をクリックします。
- ステップ 3** [ユーザロール (User Roles)] タブをクリックします。
- ステップ 4** [ユーザロール (User Roles)] タブ ページで、[ユーザロールの作成 (Create User Role)] をクリックします。
- ステップ 5** [名前 (Name)] フィールドに、REST VDI と入力します。
 ロール名では、大文字と小文字が区別されません。
- ステップ 6** [メニューベースのアクセス許可 (Menu-Based Permissions)] セクションで、[REST VDI] をオンにし、[REST VDI の変更 (Modify REST VDI)] もオンになっていることを確認します。

ステップ7 [保存 (Save)]をクリックします。

ステップ8 ロールを TS エージェントの設定に使用するユーザに割り当てます。
