BigFix Remote Console ユーザー・ガイド

目次

第 1 章. Remote Control コンソール・ユーザー・ガイド

このガイドは、エンタープライズ全体でワークステーションおよびサーバーとのリモート・コントロール・セッションを確立するために必要なコンポーネントをデプロイして構成するために、BigFix® コンソールを使用する必要があるユーザーを対象としています。このユーザーズ・ガイドでは、Remote Control の主要コンポーネントの一部、これらを BigFix® コンソールからインストールして構成する方法、およびリモート・コントロール・セッションを確立する際のこれらの使用について説明します。

Remote Control で使用される用語の定義

Remote Control で使用される共通の用語の定義。

リモート・コントロール・セッション

環境内のコンピューターと接続を確立して、コンピューターをリモートで監視したりアクティブに制御したりすること。セッションでは、コントローラー・ユーザーのキーボードおよびマウスが、リモート・システムのプライマリー・キーボードおよびマウスになります。リモート・コントロール・セッションで使用できるオプションには、チャット、ガイダンス、リブート、ファイル転送などの機能があります。リモート・コントロール・セッションについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

P2P セッション

コントローラーとターゲットの間に直接確立されるリモート・コントロール・セッション。コントローラー・ユーザーはコントローラー・コンポーネントをローカルで開始し、リモートで制御するターゲットを指定します。セッションには、ターゲットで設定されているローカル・プロパティーが使用されます。詳しくは、『ターゲット構成およびサーバー構成の管理』を参照してください。セッション中のコントローラー UI の使用について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

管理対象リモート・コントロール・セッション

コントローラー・ユーザーが Remote Control サーバーからセッションを開始するリモート・コントロール・セッション。コントローラー・コンポーネントが開始され、ターゲットに接続して、セッション要求を送信します。ターゲットはサーバーと接続して要求を認証し、セッションのポリシーおよび許可を取得します。管理対象リモート・コントロール・セッションのポリシーおよび権限について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。ターゲットがサーバーに到達できない場合、セッションは拒否されます。

セッション・ポリシー

セッション・ポリシーは、コントローラー・ユーザーによって実行可能なアクションと、リモート・コントロール・セッション中にターゲット・システム上で使用可能な機能を定義します。P2P セッションでは、ポリシーは、ターゲットに定義されているローカル・プロパティーによって決定されます。管理対象セッションでは、ユーザーとターゲット・グループの関係から解決されるポリシーと権限によって、実行できるアクションが決定されます。管理対象リモート・コントロール・セッションのポリシー

および権限の導出方法について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

Remote Control コンソール

Remote Control には、インストール環境内のワークステーションおよびサーバーのリモートでの制御とモニタリングに必要となるコンポーネントを提供する、多数の機能が含まれています。

BigFix® コンソールのナビゲーション・ツリーはすべての BigFix® 製品で使用でき、Remote Control のすべての機能の中心的なコマンドとして機能します。ナビゲーション・ツリーからは、ネットワーク内のターゲット・システムの制御と管理に関連したすべてのレポート、ウィザード、Fixlet メッセージ、分析、およびタスクに簡単にアクセスできます。

コンポーネント

BigFix® コンソールの内容は、以下の 4 つの部分に編成されます。

ドメイン・ペイン

ナビゲーション・ツリーとすべてのドメインのリストを含みます。

ナビゲーション・ツリー

サイト・コンテンツを格納するノードとサブノードのリストを含みます。

リスト・ペイン

タスクおよび Fixlet のリストを含みます。

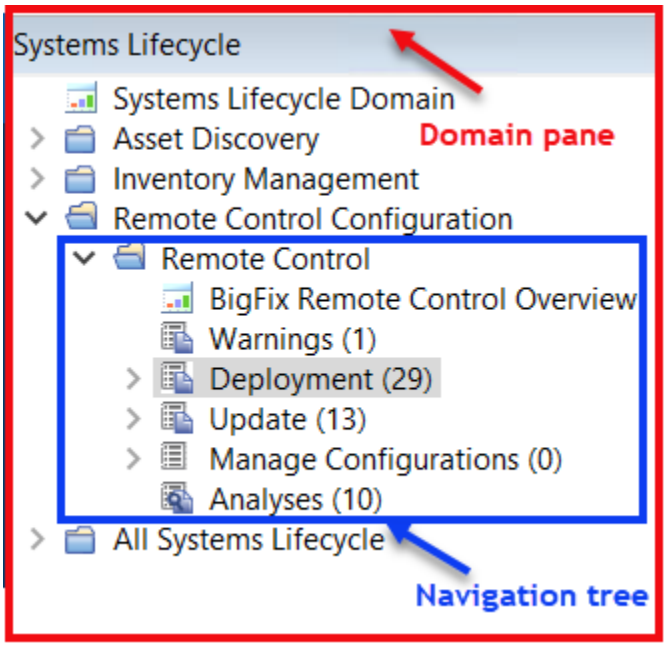
作業域

Fixlet およびダイアログが表示される作業ペインです。

BigFix® コンソールのコンテキストでは、製品またはサイトはカテゴリー別またはドメイン別にグループ化されます。例えば Remote Control は、「システム・ライフサイクル」ドメイン内部に含まれるサイトの 1 つです。

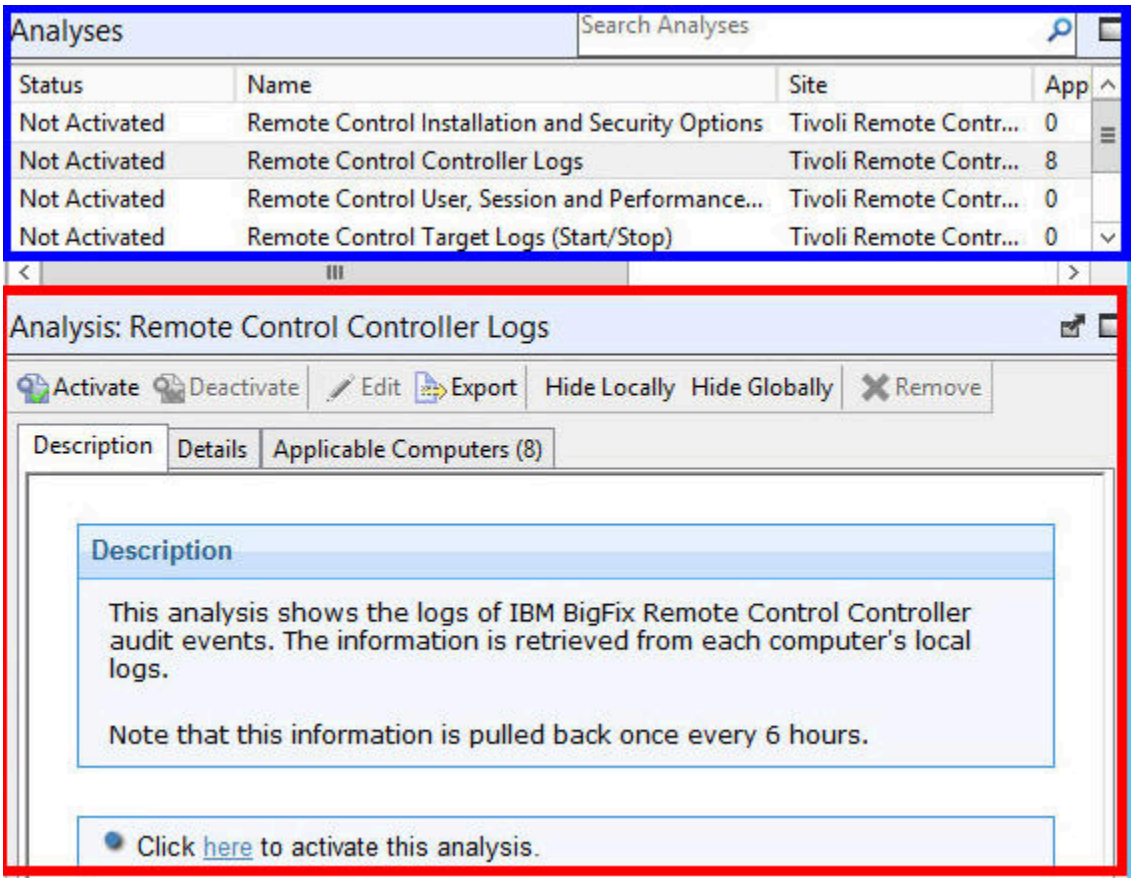
ドメイン・ペインはコンソールの左側の領域で、ナビゲーション・ツリーとすべてのドメインのリストを含みます。ナビゲーション・ツリーは、サイト・コンテンツを格納するノードとサブノードのリストを含みます。

「システム・ライフサイクル」ドメインをクリックして、そのドメインに関連付けられたサイトのリストを表示します。



赤色の線で囲んだ外側の領域は、ドメイン・ペイン全体 (ナビゲーション・ツリーおよびドメインのリスクを含む) を表しています。青色の線で囲んだ内側の領域には、Remote Control サイトのナビゲーション・ツリーのみが含まれています。

Remote Control のタスクは、上部および下部のタスク・ペインでソートされます。これらはコンソールの右側に配置されます。

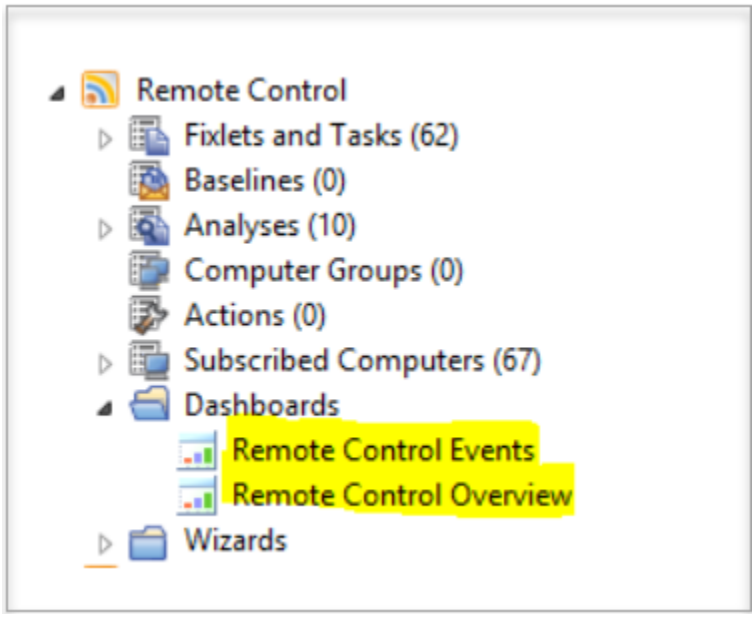


上部ペインは、リスト・ペインと呼ばれ、「ステータス」、「名前」、「サイト」、「適用可能なコンピューターの数」などのタイプによってデータをソートする列を含みます。下部ペイン (作業域) には Fixlet タスク・ペインが表示されます。このペインから、デプロイメント内のコンテンツをカスタマイズするために特定のアクションを実行するように指示されます。

ダッシュボードの概要

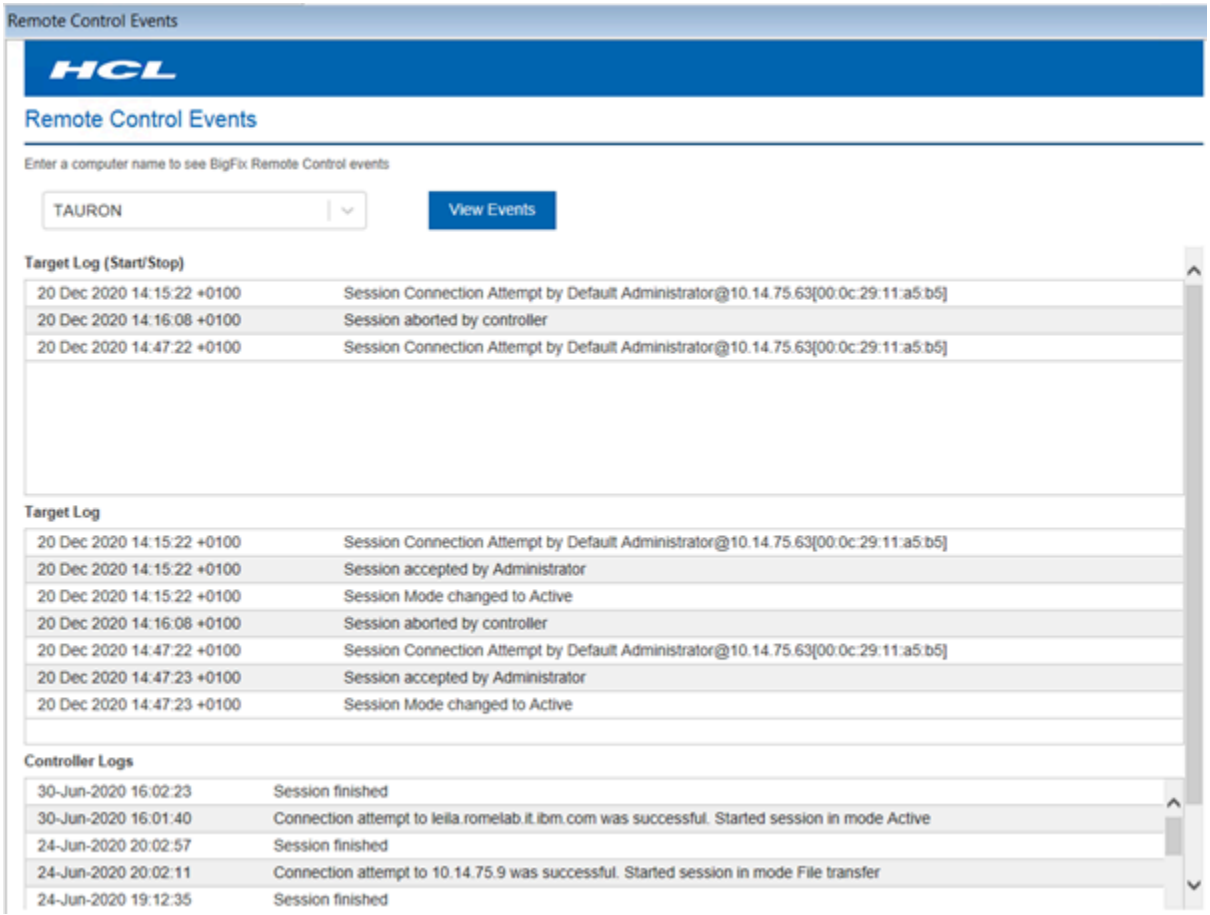
Remote Control では、いくつかの便利なダッシュボード、コントローラーから収集されたログ・データや指定したコンピューターに関するターゲット・ログを表示するための **Remote Control イベント**、および環境内の Remote Control コンポーネントのデプロイメントの配布と、実行されるターゲット・デプロイメントの種類の配布を表示する **Remote Control の概要**を提供します。

Remote Control ナビゲーション・ツリーの上部からこれらのダッシュボードにアクセスするには、**「Remote Control イベント」**または**「Remote Control の概要 :」**を選択します。



Remote Control イベントの表示

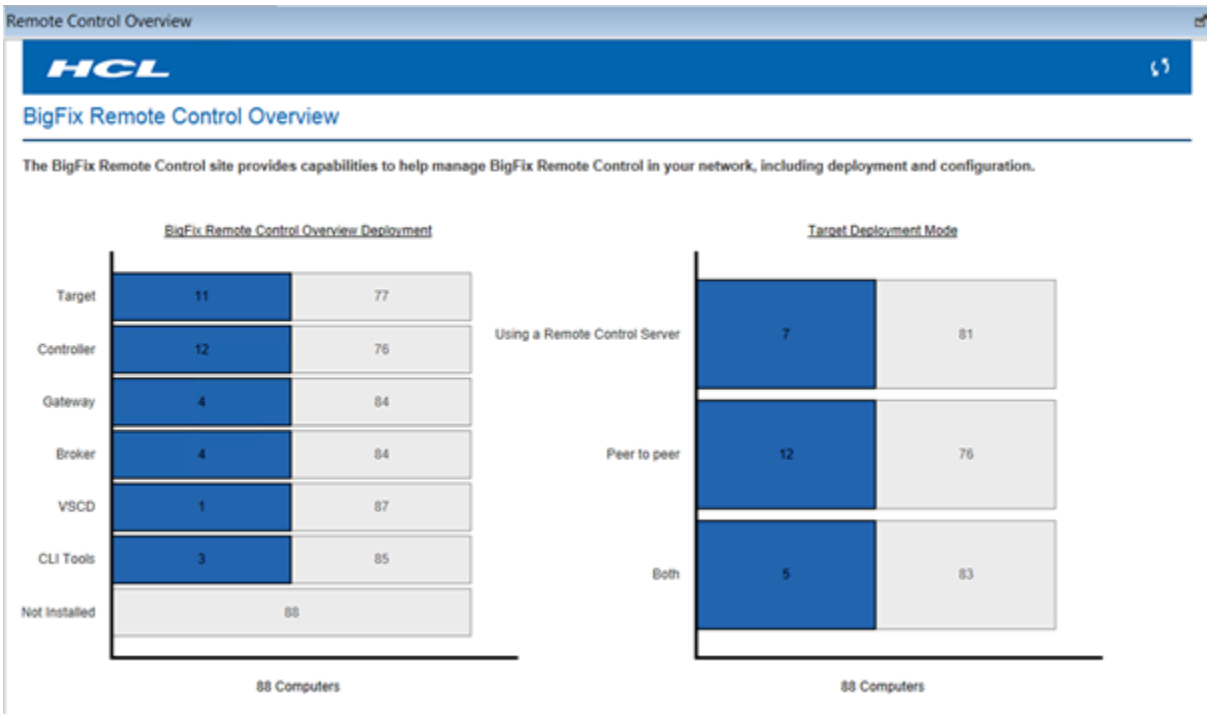
「Remote Control イベント」ダッシュボードには、コントローラーから収集されたログ・データと、指定したコンピューターに関するターゲット・ログを示す 3 つのセクションがあります。



インストール分布データの表示

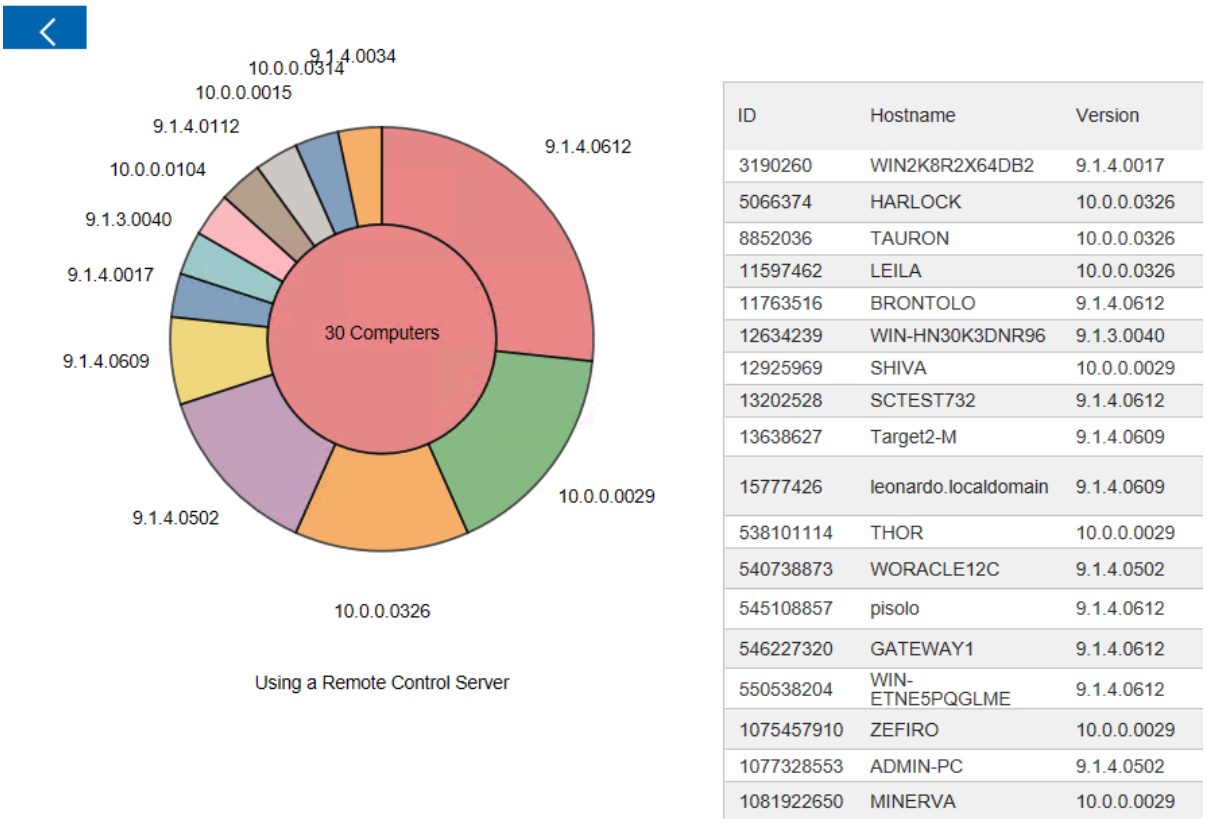
「Remote Control の概要」ダッシュボードには、Remote Control のインストールの分布と、ターゲット・インストール・タイプの分布を表示する 2 つの別々のセクションが含まれています。

「Remote Control の概要デプロイメント」セクションには、各種の Remote Control コンポーネントがインストールされた、環境内のコンピューターの数が表示されます。



「ターゲットのデプロイメント・モード」セクションには、環境内のコンピューター上で実行されたターゲット・インストール・タイプの分布が表示されます。ターゲット・インストールのさまざまなタイプについて詳しくは、Remote Control コンポーネントのデプロイを参照してください。

- 最新のデプロイメント分布データを表示するには、更新アイコン  を使用します。
- ロードされた統計の結果を確認するには、青いバーをクリックします。コンピューターのバージョン、インストールされているコンポーネントのバージョンなどの詳細を表示できます。



- コンポーネントをバージョンでさらに絞り込むには、目的の円グラフの項目をクリックします。
- 完全な統計に戻るには、グラフの中央にある円をクリックします。
- メインページに戻る場合は、「戻る」ボタン  をクリックします。

Remote Control 内の機能

Remote Control ナビゲーション・ツリーには、一連の Fixlet、タスク、およびウィザードが表示されています。これらの機能を使用して、環境でリモート・コントロール・セッションを実行するために必要なコンポーネントのインストール、構成、および更新を行います。これらのコンポーネントからデータを収集することもできます。

Remote Control コンポーネントのデプロイ

Remote Control ナビゲーション・ツリーの**「デプロイメント」**ノードには、オペレーティング・システム固有のサブノードがあります。これらのサブノードの中に、リモート・コントロール・セッションを確立するために必要なコンポーネントをインストールできます。また、コマンド・ラインを使用してターゲットに接続するために使用できるユーティリティーもインストールできます。ご使用のオペレーティング・システムに該当するノードを選択します。

注: Remote Control コンポーネントは、インストール・ファイルを使用してインストールすることもできます。詳しくは、*BigFix® Remote Control* インストール・ガイド を参照してください。

コントローラー

Remote Control サーバーへのアクセス権限を持っていない場合は、リモート・コントロール・セッションを開始するコンピューター上にコントローラー・コンポーネントをインストールする必要があります。

ターゲット

ターゲット・コンポーネントは、リモート・コントロール・セッション時に制御されるコンピューター上にインストールする必要があります。Remote Control では、2 つの方法でターゲット・コンポーネントをインストールできます。P2P セッションまたは管理対象セッションのターゲットをインストールできます。この 2 つのセッション・タイプについては、Remote Control で使用される用語の定義で説明されており、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」では、より詳細に説明されています。

注: Remote Control サーバーを使用する方法では、ご使用の環境に Remote Control サーバーをインストールする必要があります。

CLI ツール

コマンド・ライン・ツールには、コマンド・ラインから実行できる 2 つのユーティリティーが含まれています。これらのユーティリティーを使用すると、ターゲットとのリモート・コントロール・セッションを開始したり、ターゲット・ユーザーによる操作なしにターゲット・システムでコマンドを実行したりできます。これらのツールは、Remote Control サーバー・インターフェースにアクセスせずにターゲットに接続する場合に役立ちます。また、これらをスクリプトで使用して、複数のコマンドを自動的に実行することもできます。

注: CLI ツールをインストールするには、アクセス権限がある Remote Control サーバーの URL が必要です。

ゲートウェイ

ターゲット、コントローラー、およびサーバーが、相互に直接接続できない別々のネットワーク上にある場合は、ゲートウェイ・サポートをインストールし、構成することができます。ゲートウェイ・サポートを使用して、これらの接続が確立されるようにネットワークを構成します。

ブローカー

インターネット上の企業ネットワークの外側にあるターゲットを使用する場合は、ブローカー・コンポーネントをインストールします。ブローカー・コンポーネントは、インターネット経由のリモート・コントロール・セッションでコントローラーとターゲットの間に接続を確立するために使用されます。

Windows® システムでのコンポーネントのデプロイ

Windows デプロイメント・ノードには、Windows® オペレーティング・システム環境で以下のコンポーネントをインストールまたは削除するために使用できる一連のタスクが用意されています。

- ターゲット・ソフトウェアおよびコントローラー・ソフトウェア
- CLI ツール
- ゲートウェイ・サポート
- ブローカー・サポート

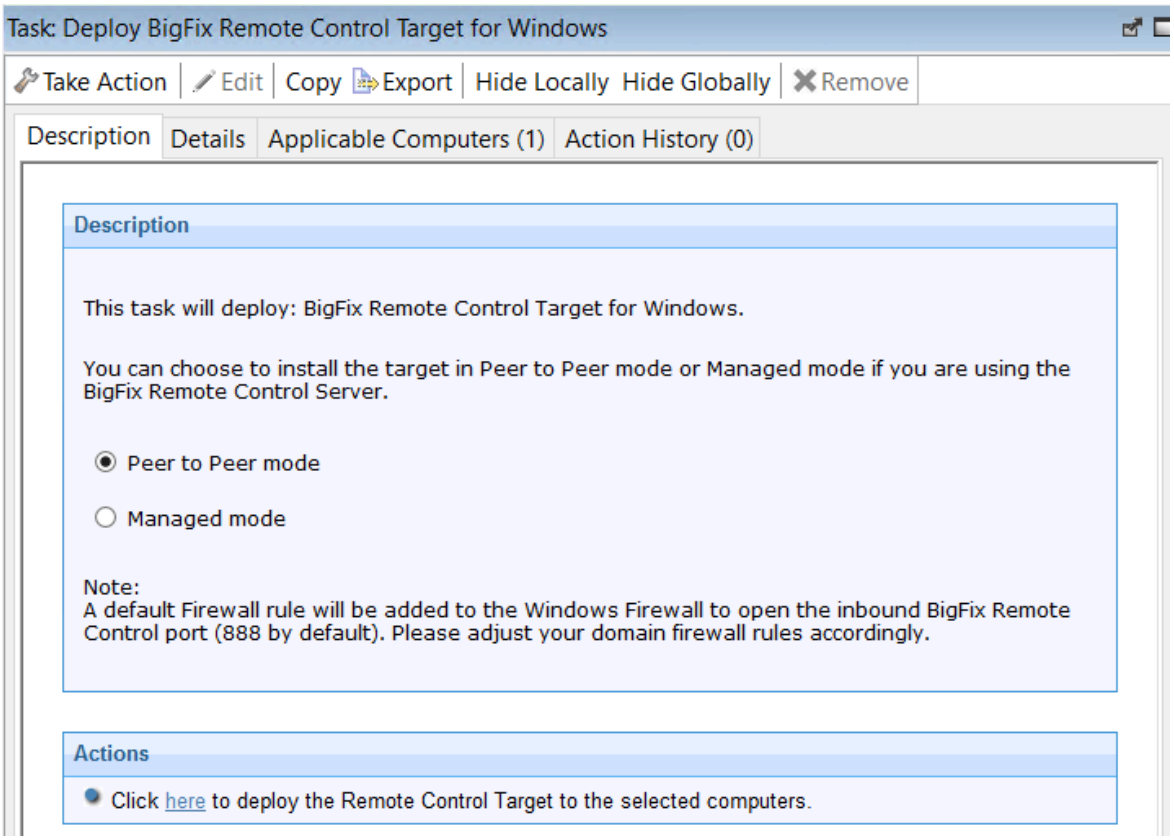
Windows® ターゲットのデプロイ

「Remote Control ターゲット (Windows 版) のデプロイ」タスクを使用して、ターゲット・ソフトウェアを Windows® コンピューターにインストールします。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーで、**「デプロイメント」 > 「Windows」**をクリックします。
2. **「Remote Control ターゲット (Windows 版) のデプロイ」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。

   関連するインストール方法を決定し、記載された指示に従ってくださ



   い。

   P2P モード

このインストール方法を使用すると、Remote Control サーバーを必要とせずに、コントローラーとターゲットの間に直接リモート・コントロール・セッションを確立できます。このインストール方法では、Remote Control サーバー URL の指定を求めることなくターゲットがインストールされます。リモート・コントロール・セッションを確立するときには、このインストール方法により設定されたローカル・ターゲット・ポリシーが使用されます。ターゲットのインストール・プロパティーについて詳しくは、ターゲット構成およびサーバー構成の管理を参照してください。

「アクションの実行」ペインの「対象」タブで、Remote Control ターゲットをデプロイするコンピューターを決定するための関連オプションを選択します。

「OK」。

概要画面にタスクの進行状況が表示され、タスク完了時にはステータス *complete* が表示されます。

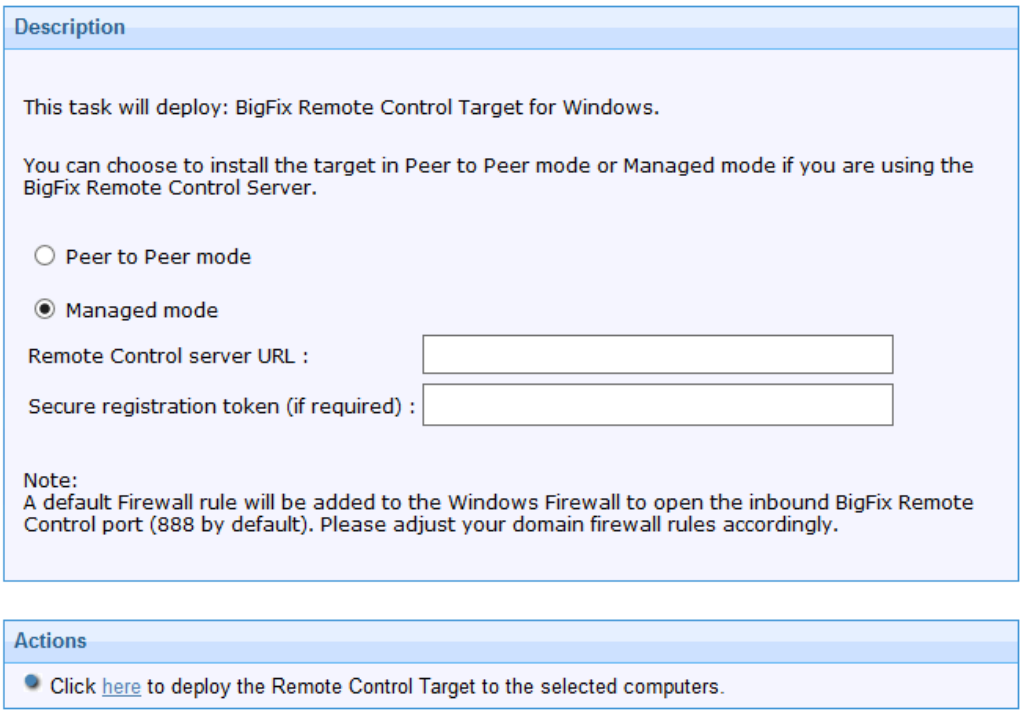
注: ターゲットを将来 Remote Control サーバーに登録する場合は、Remote Control ターゲット・ウィザードを使用します。構成タスクを作成して、関連サーバーのサーバー URL を指定します。選択したターゲットでこのタスクを実行すると、ターゲットが再構成され、サーバーに接続できるようになります。ターゲット構成タスクについて詳しくは、Remote Control ターゲット構成タスクの作成を参照してください。セキュア登録機能がサーバー上で有効になっている場合、セキュア登録トークンをターゲットに配布できます。詳しくは、『ターゲットへのセキュア登録トークンの配布』を参照してください。

管理対象モード

ターゲットを Remote Control サーバーに登録し、サーバーから起動されたリモート・コントロール・セッションに参加させるには、このインストール・オプションを選択します。このインストール方法では、Remote Control サーバー URL を指定する必要があります。このターゲットに対して、リモート・コントロール・セッションが要求された場合は、要求を認証するため、指定されたサーバーへの接続が行われます。要求が認証されると、セッションに対するポリシーが Remote Control サーバーからターゲットに渡され、セッションが確立されます。ターゲットのインストール・プロパティーについて詳しくは、ターゲット構成およびサーバー構成の管理を参照してください。

Remote Control サーバーの URL を入力します。

セキュア登録機能がサーバー上で有効になっている場合、有効なセキュア登録トークンを入力します。



「アクションの実行」ペインの「ターゲット」タブで、Remote Control ターゲットをデプロイするコンピューターを決定するための関連オプションを選択します。

「OK」。

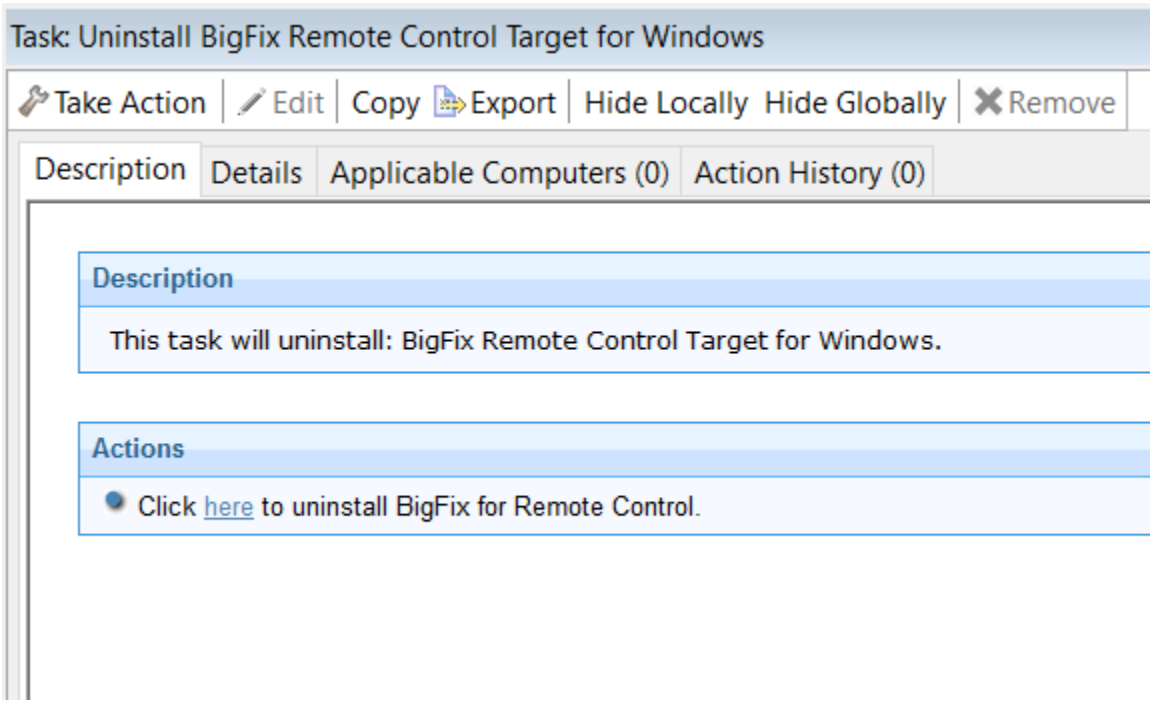
概要画面にタスクの進行状況が表示され、タスク完了時にはステータス *complete* が表示されます。

Windows® ターゲットの削除

「Remote Control ターゲット (Windows 版) のアンインストール」タスクを使用すると、ターゲット・ソフトウェアが既にインストールされている Windows® コンピューターからターゲット・ソフトウェアを削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Windows」**をクリックします。
2. **「Remote Control ターゲット (Windows 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ペインの「対象」タブで、Remote Control ターゲットを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

注: ターゲットが削除された後、一部のファイルは自動的に削除されない場合があります。これらのファイルは、ターゲットのインストールの一部として作成されました。それらのファイルは `C:\ProgramData\BigFix\Remote Control\` にあります。

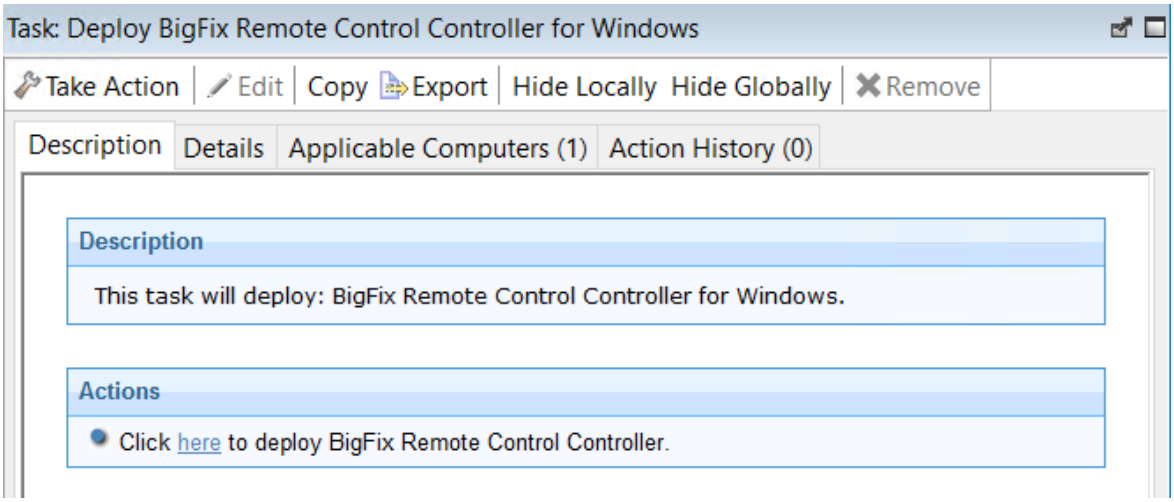
Windows® コントローラーのデプロイ

「Remote Control コントローラー (Windows 版) のデプロイ」タスクを使用すると、コントローラー・ソフトウェアを Windows® コンピューターにインストールできます。

注: リモート・コントロール・セッションを BigFix® コンソールから開始するには、コンソールがインストールされているのと同じコンピューターにコントローラーをデプロイします。ただし、コントローラーがインストールされたとき、セッションを開始するメニュー項目の表示権限があるのは、インストール対象のコンピューターにログオンしている現行ユーザーのみです。メニュー項目は他のユーザーに表示されません。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Windows」**をクリックします。
2. **「Remote Control コントローラー (Windows 版) のデプロイ」**をクリックします。
3. **「タスク」**ペインで、説明を確認し、**「アクション」**ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「ターゲット」タブで、コントローラーをデプロイするターゲットを決定するために必要なオプションを選択します。
5. **「OK」**。

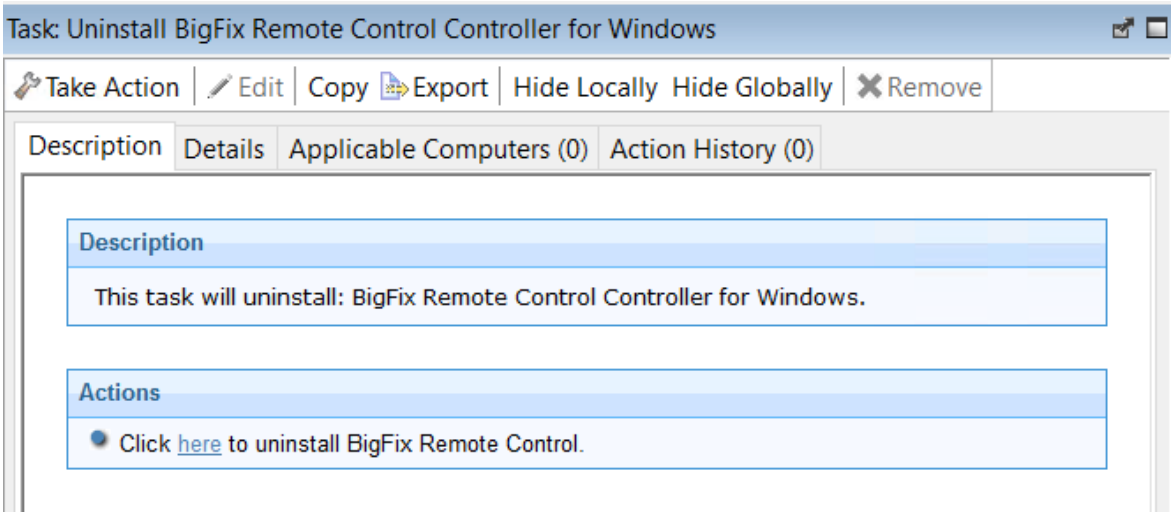
概要画面にタスクの進行状況が表示されます。

Windows® コントローラーの削除

「Remote Control コントローラー (Windows 版) のアンインストール」タスクを使用すると、コントローラー・ソフトウェアが既にインストールされている Windows® コンピューターからコントローラー・ソフトウェアを削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Windows」**をクリックします。
2. **「Remote Control コントローラー (Windows 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「ターゲット」タブで、Remote Control コントローラーを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

Windows® CLI ツールのデプロイ

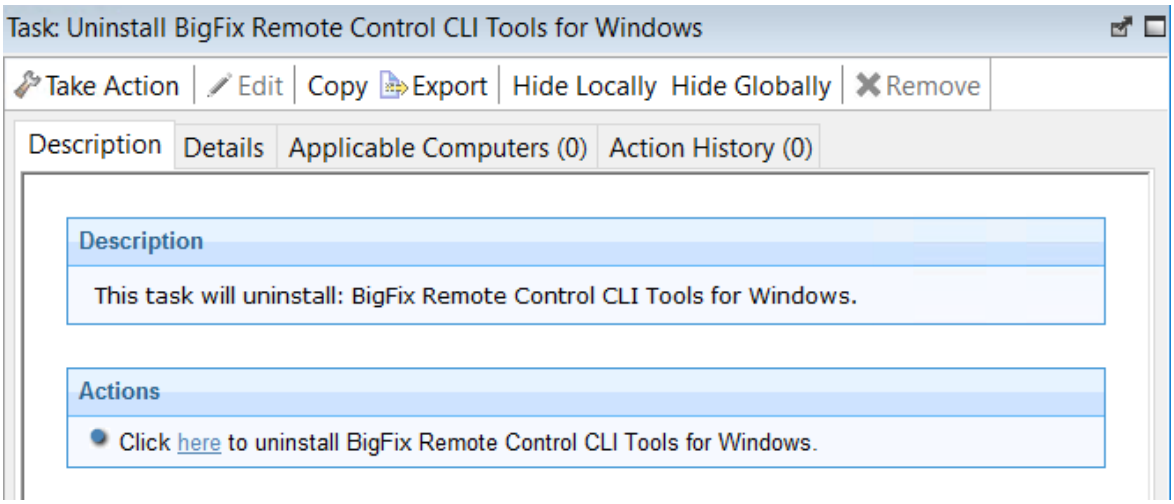
「Remote Control CLI ツール (Windows 版) のデプロイ」タスクを使用すると、CLI ツールを Windows® コンピューターにインストールできます。CLI ツールを使用して、コマンド・ラインからセッションを開始します。ツールを使用して、リモート・ターゲットでコマンドを実行することもできます。

このタスクを開始するには、以下のステップを実行します。

注:

1. ターゲット・ソフトウェアをインストールすると、CLI ツールもインストールされます。そのため、**「Remote Control CLI ツール (Windows 版) のデプロイ」** Fixlet を使用して、ターゲット・ソフトウェアがインストールされていないコンピューターにのみ CLI ツールをインストールします。
2. このタスクを適用するには、アクセス権限がある Remote Control サーバーの URL が必要です。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Windows」**をクリックします。
2. **「Remote Control CLI ツール (Windows 版) のデプロイ」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. Remote Control サーバーの URL を入力し、**「OK」**をクリックします。
5. 「アクションの実行」ペインの「対象」タブで、CLI ツールをデプロイするターゲットを決定するために必要なオプションを選択します。
6. **「OK」**。

概要画面にタスクの進行状況が表示されます。

デプロイメント・タスクを実行したときに選択したターゲットの `\Program Files\BigFix\Remote Control \Target` ディレクトリーに、2 つの CLI ユーティリティーがインストールされます。

`wrc.exe`

このツールを使用して、ターゲットとのリモート・コントロール・セッションを開始します。

`wrcmdpcr.exe`

このツールを使用して、ターゲットでコマンドを実行します。コマンドからの出力は、コマンドを実行したコンピューターで表示されます。

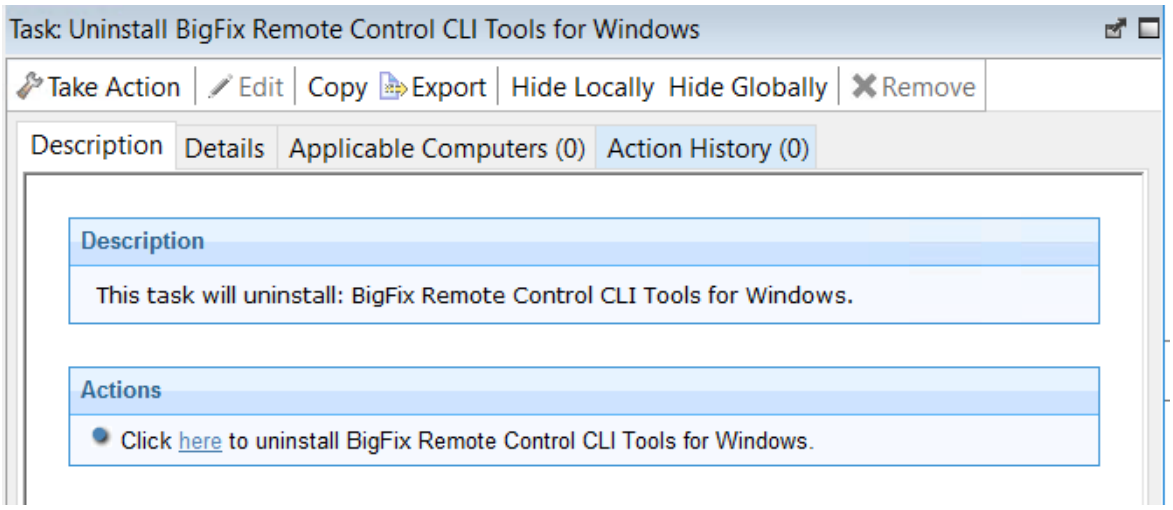
コマンド・ライン・ツールの使用方法について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

Windows® CLI ツールの削除

「Remote Control CLI ツール (Windows 版) のアンインストール」タスクを使用すると、CLI ツールが既にインストールされている Windows® コンピューターから CLI ツールを削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Windows」**をクリックします。
2. **「Remote Control CLI ツール (Windows 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「ターゲット」タブで、CLI ツールを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。CLI ツールが、選択されたターゲットから削除されます。

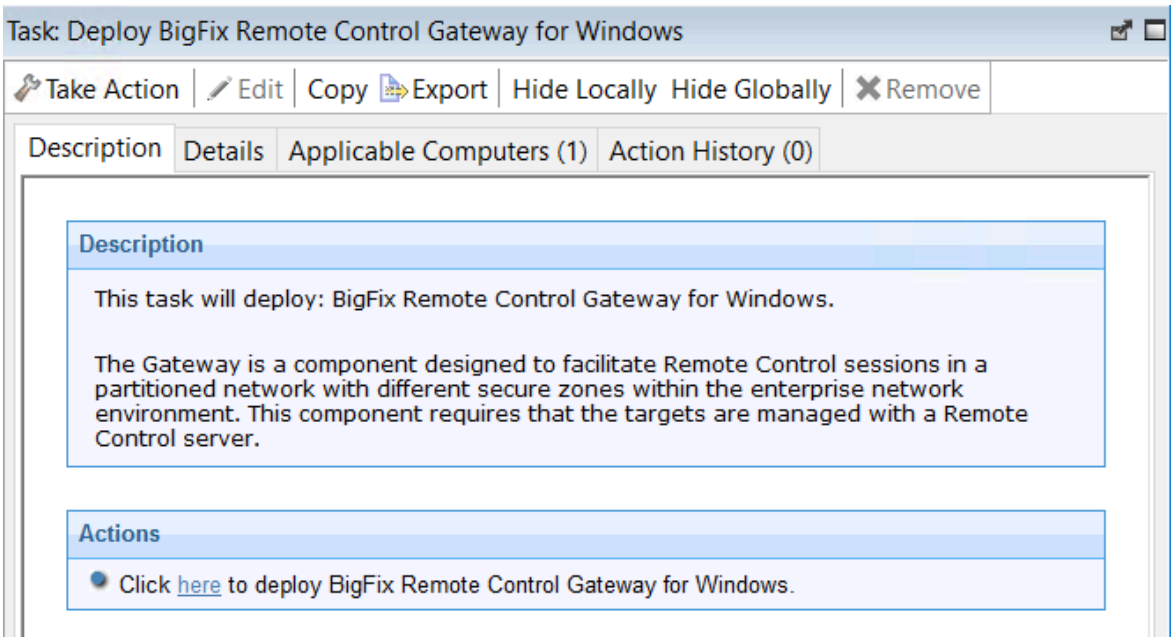
注: CLI ツールが削除された後、一部のファイルは自動的に削除されない場合があります。これらのファイルは、CLI ツールのインストール中に作成されました。それらのファイルは `C:\ProgramData\BigFix\Remote Control\` にあります。

Windows® ゲートウェイ・サポートのインストール

「Remote Control ゲートウェイ (Windows 版) のデプロイ」タスクを使用すると、ゲートウェイ・サポートを Windows® コンピューターにインストールできます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Windows」**をクリックします。
2. **「Remote Control ゲートウェイ (Windows 版) のデプロイ」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「ターゲット」タブで、ゲートウェイ・サポートをデプロイするターゲットを決定するために必要なオプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

ゲートウェイ・サポートが、インストール・タスクを実行したときに選択したターゲットにインストールされます。ファイルは選択したターゲットの `\Program Files\BigFix\Remote Control\Gateway` ディレクトリーにあります。

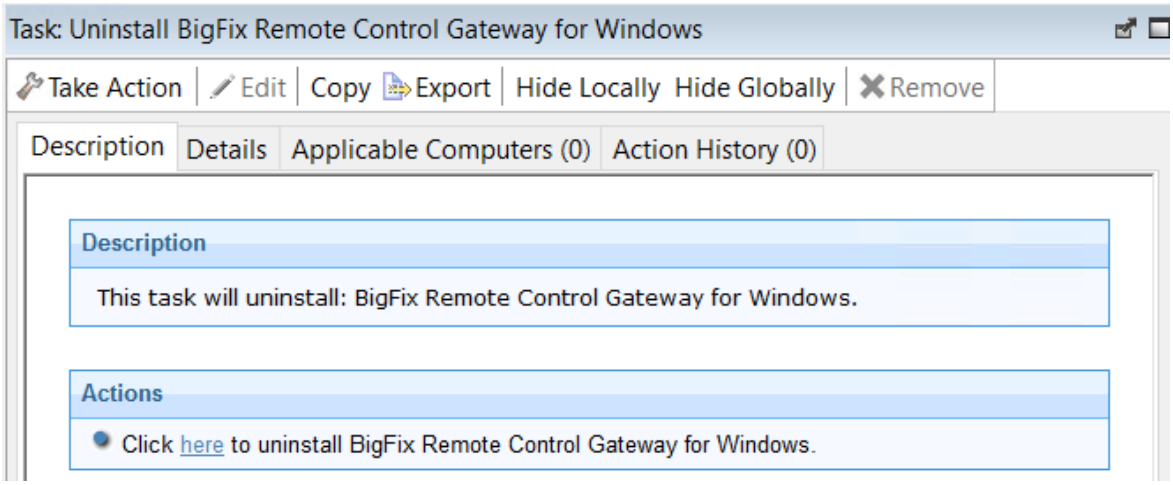
ゲートウェイ・サポートを使用するには、ご使用の環境に合わせてゲートウェイ構成をセットアップする必要があります。これらのゲートウェイの構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

Windows® ゲートウェイ・サポートの削除

「Remote Control ゲートウェイ・サポート (Windows 版) のアンインストール」タスクを使用すると、ゲートウェイ・サポート・ファイルを Windows® コンピューターから削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Windows」**をクリックします。
2. **「Remote Control ゲートウェイ (Windows 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、ゲートウェイ・サポートを削除する対象コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

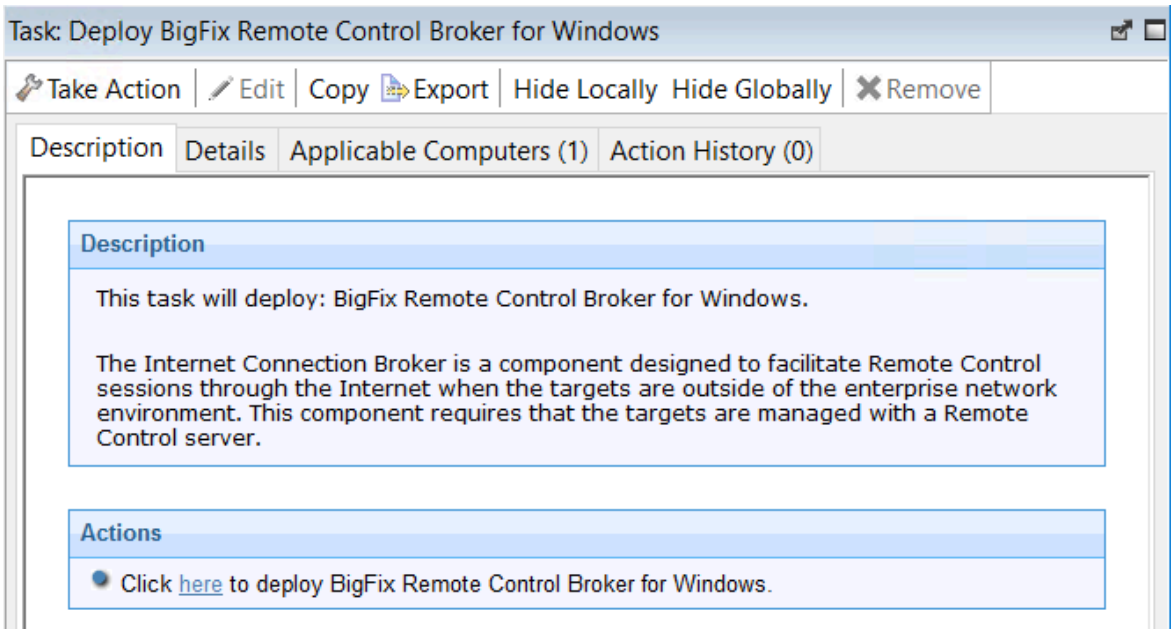
ゲートウェイ・サポート・ファイルは、選択されたターゲットから削除されます。

Windows™ ブローカー・サポートのデプロイ

「Remote Control ブローカー (Windows 版) のインストール (Deploy Broker for Windows)」タスクを使用すると、ブローカー・サポートを Windows™ コンピューターにインストールできます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Windows」**をクリックします。
2. **「Remote Control ブローカー (Windows 版) のデプロイ」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「ターゲット」タブで、ブローカー・サポートをデプロイするターゲットを決定するために必要なオプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。ブローカー・サポートが、インストール・タスクを実行したときに選択したターゲットにインストールされます。ファイルは選択したターゲットの *[working dir]*`\Broker` ディレクトリーにインストールされます。*[working dir]* の値は、ブローカー・サポートのインストール先の Windows™ オペレーティング・システムのバージョンによって決まります。例えば、`C:\ProgramData\BigFix\Remote Control` です。ブローカー・サポートを使用するには、ご使用の環境に合わせてブローカー構成をセットアップする必要があります。これらのブローカーの構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

Windows™ ブローカー・サポートの削除

「Remote Control ブローカー (Windows 版) のアンインストール (Uninstall Broker for Windows)」タスクを使用すると、ブローカー・サポートを Windows™ コンピューターから削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Windows」**をクリックします。
2. **「Remote Control ブローカー (Windows 版) のアンインストール (Uninstall Broker for Windows)」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。

4. 「アクションの実行」ペインの「ターゲット」タブで、ブローカー・サポートを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。ブローカー・サポート・ファイルは、選択されたターゲットから削除されます。

Linux™ システムでのコンポーネントのデプロイ

Linux デプロイメント・ノードには、Linux™ 環境で以下のコンポーネントをインストールまたは削除するために使用できる一連のタスクが用意されています。

- ターゲット・ソフトウェアおよびコントローラー・ソフトウェア
- CLI ツール
- ゲートウェイ・サポート
- ブローカー・サポート

注: ブローカー・コンポーネントのインストール・パッケージは、32 ビット・バージョンの以下のライブラリーに依存しています。**glibc libgcc**、**libblkid**、**libstdc++**。

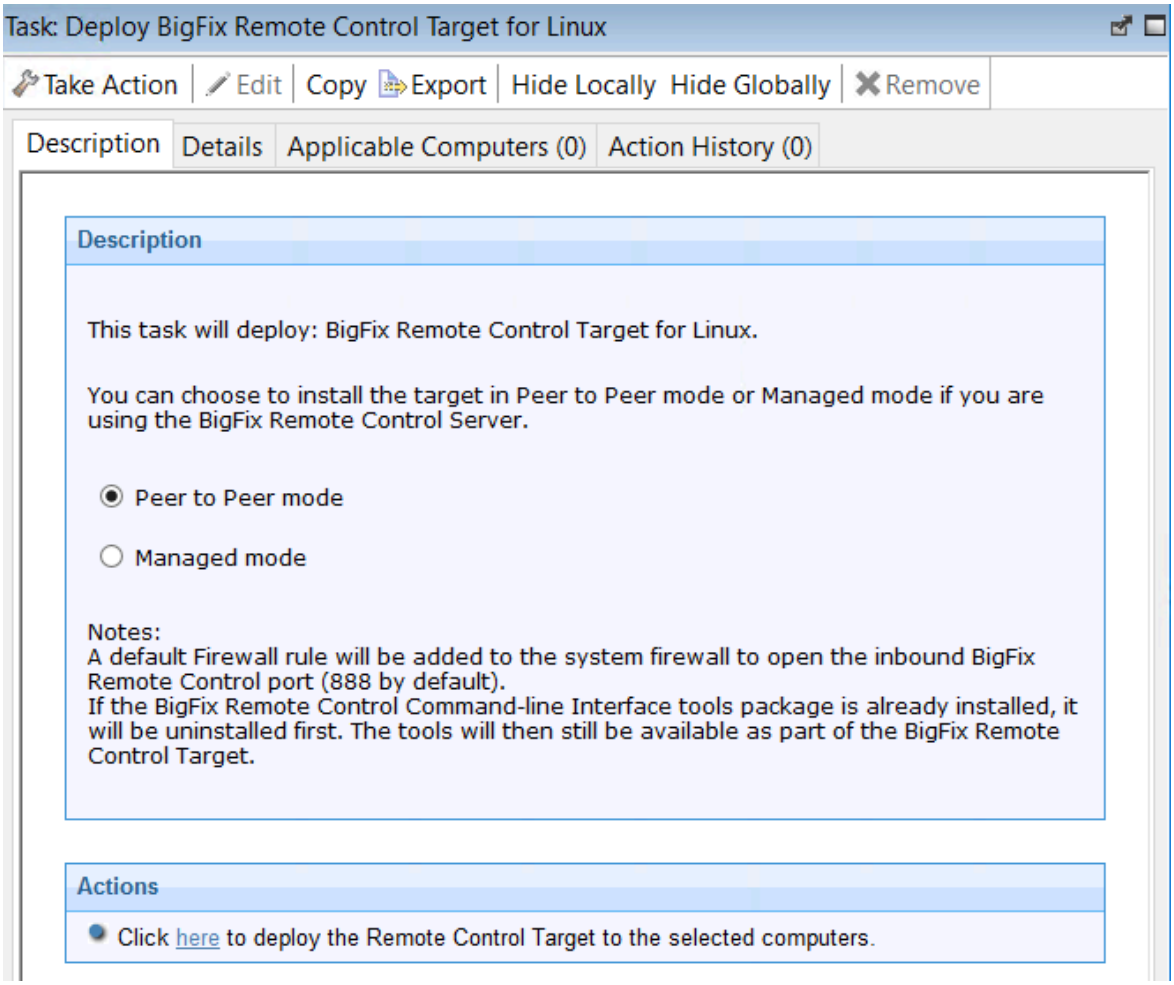
Linux® ターゲットのデプロイ

「Remote Control ターゲットのインストール (Linux 版)」タスクを使用すると、ターゲット・ソフトウェアを Linux® コンピューターにインストールできます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Linux」**をクリックします。
2. **「Remote Control ターゲットのインストール (Linux 版)」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。

インストール方法を決定し、提示された指示に従ってください。



P2P モード

このインストール方法を使用すると、Remote Control サーバーを必要とせずに、コントローラーとターゲットの間に直接リモート・コントロール・セッションを確立できます。このインストール方法では、Remote Control サーバー URL の指定を求めることなくターゲットがインストールされます。リモート・コントロール・セッションを確立するときには、このインストール方法により設定されたローカル・ターゲット・ポリシーが使用されます。ターゲットのインストール・プロパティーについて詳しくは、ターゲット構成およびサーバー構成の管理を参照してください。

「アクションの実行」ペインの「対象」タブで、Remote Control ターゲットをデプロイするコンピューターを決定するための関連オプションを選択します。

「OK」。

概要画面にタスクの進行状況が表示されます。

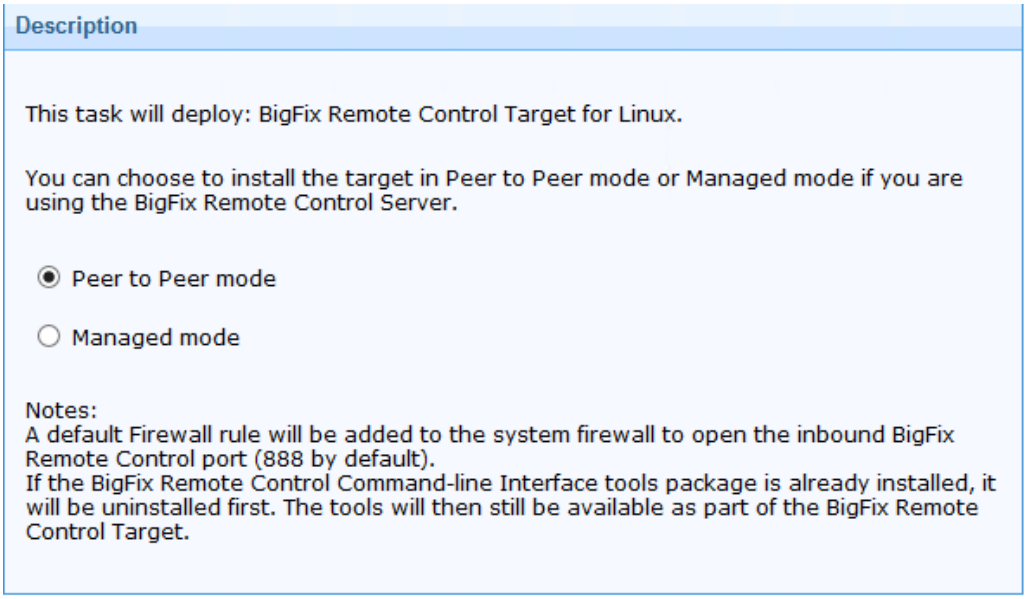
注: ターゲットを将来 Remote Control サーバーに登録する場合は、ターゲット・ウィザードを使用して、構成タスクを作成し、ご使用のサーバーのサーバー URL を指定します。選択したターゲットでこのタスクを実行すると、ターゲットは再構成され、サーバーに接続できるようになります。ターゲット構成タスクについて詳しくは、Remote Control ターゲット構成タスクの作成を参照してください。セキュア登録機能がサーバー上で有効になっている場合、セキュア登録トークンをターゲットに配布できます。詳しくは、『ターゲットへのセキュア登録トークンの配布』を参照してください。

管理対象モード

ターゲットを Remote Control サーバーに登録し、サーバーから起動されたリモート・コントロール・セッションに参加させるには、このインストール・オプションを選択します。このインストール方法では、Remote Control サーバー URL を指定する必要があります。このターゲットに対して、Remote Control サーバーから起動したリモート・コントロール・セッションが要求された場合は、要求を認証するため、指定されたサーバーに接続します。要求が認証されると、セッションに対して設定されたポリシーが Remote Control サーバーからターゲットに渡され、セッションが開始されます。ターゲットのインストール・プロパティーについて詳しくは、ターゲット構成およびサーバー構成の管理を参照してください。

Remote Control サーバーの URL を入力します。

セキュア登録機能がサーバー上で有効になっている場合、有効なセキュア登録トークンを入力します。



「アクションの実行」ペインの「対象」タブで、Remote Control ターゲットをデプロイするコンピューターを決定するための関連オプションを選択します。

「OK」。

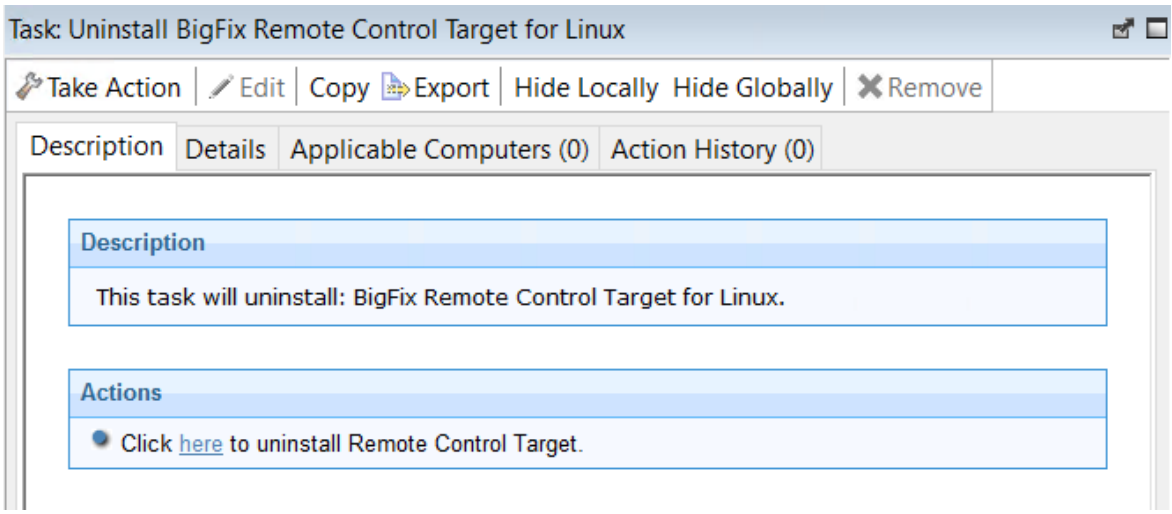
概要画面にタスクの進行状況が表示されます。

Linux® ターゲットの削除

「Remote Control ターゲット (Linux 版) のアンインストール」タスクを使用すると、ターゲット・ソフトウェアを Linux® コンピューターから削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control ターゲット (Linux 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、Remote Control ターゲットを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

注: ターゲットが削除された後、一部のファイルは自動的に削除されない場合があります。これらのファイルは、ターゲットのインストール中に作成されました。これらのファイルは次の `/opt/bigfix` および `/var/opt/bigfix/trc/target` のディレクトリーにあります。

Linux® コントローラーのデプロイ

「Remote Control コントローラー (Linux 版) のインストール」タスクを使用すると、コントローラー・ソフトウェアを Linux® コンピューターにインストールできます。

注: コントローラーを Red Hat 6.0、64 ビット・コンピューターにインストールする場合は、次の追加ライブラリーをそのすべての依存関係とともにインストールする必要があります。`libXft.i686 libXmu.i686 libXp.i686 libXtst.i686`.

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control コントローラー (Linux 版) のインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。

4. 「アクションの実行」ペインの「対象」タブで、コントローラーをデプロイするターゲットを決定するために必要なオプションを選択します。
5. **「OK」**。

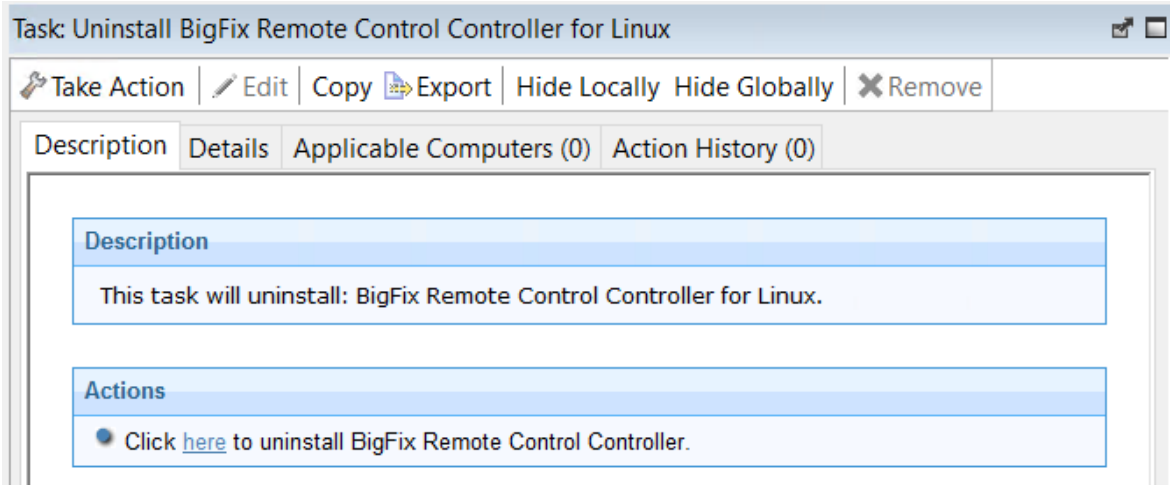
概要画面にタスクの進行状況が表示されます。

Linux® コントローラーの削除

「Remote Control コントローラー (Linux 版) のアンインストール」タスクを使用すると、コントローラー・ソフトウェアを Linux® コンピューターから削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control コントローラー (Linux 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、Remote Control コントローラーを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

Linux® CLI ツールのデプロイ

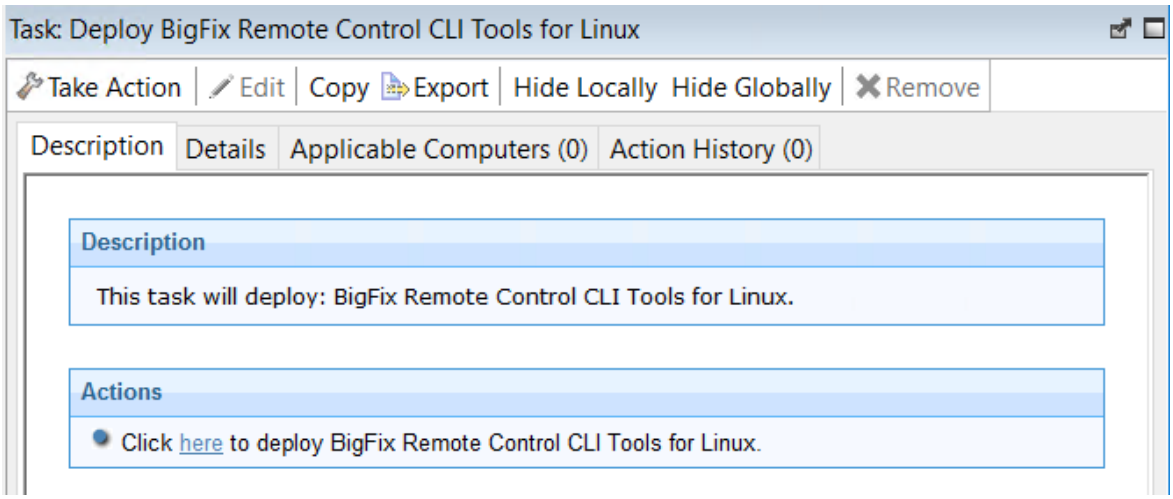
「Remote Control CLI ツール (Linux 版) のデプロイ」タスクを使用すると、CLI ツールを Linux® コンピューターにインストールできます。

注:

1. ターゲット・ソフトウェアをインストールすると、CLI ツールもインストールされます。そのため、**「Remote Control CLI ツール (Linux 版) のデプロイ」** Fixlet を使用して、ターゲット・ソフトウェアがインストールされていないコンピューターにのみ CLI ツールをデプロイします。
2. このタスクを適用するには、アクセス権限がある Remote Control サーバーの URL が必要です。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Linux」**をクリックします。
2. **「Remote Control CLI ツール (Linux 版) のデプロイ」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. Remote Control サーバーの URL を入力し、**「OK」**をクリックします。
5. 「アクションの実行」ペインの「対象」タブで、CLI ツールをデプロイするターゲットを決定するために必要なオプションを選択します。
6. **「OK」**。

概要画面にタスクの進行状況が表示され、タスク完了時には完了ステータスが表示されます。

デプロイメント・タスクを実行したときに選択したターゲット・コンピューターの `/opt/bigfix/trc/target` ディレクトリーに、次の 2 つの CLI ユーティリティーがインストールされます。

`wrc`

このツールを使用して、ターゲットとのリモート・コントロール・セッションを開始します。

`wrcmdpcr`

このツールを使用して、ターゲットでコマンドを実行します。コマンドからの出力は、コマンドを実行したコンピューターで表示されます。

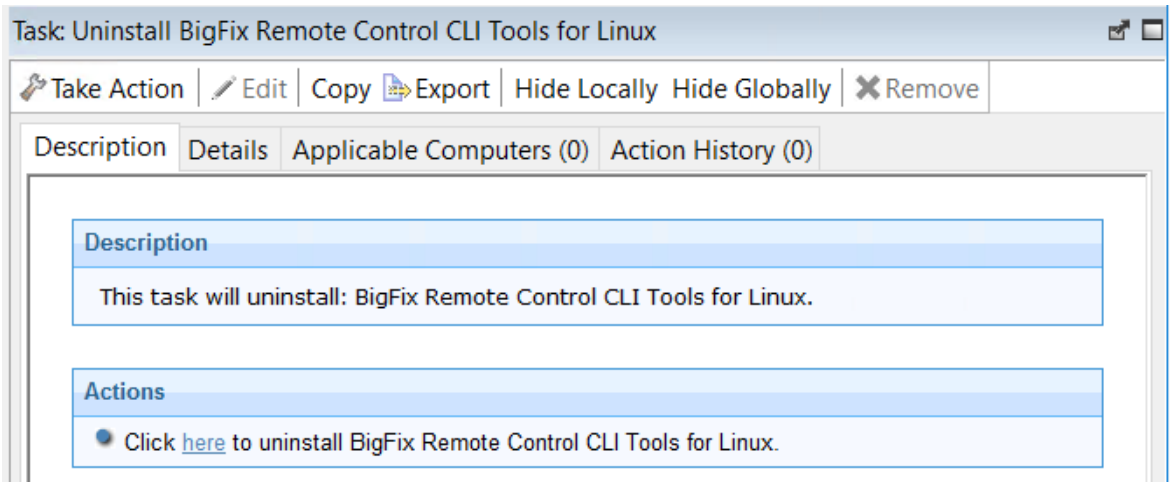
コマンド・ライン・ツールの使用方法について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

Linux® CLI ツールの削除

「Remote Control CLI ツール (Linux 版) のアンインストール」タスクを使用すると、CLI ツールが既にインストールされている Linux® コンピューターから CLI ツールを削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」** > **「Linux」**をクリックします。
2. **「Remote Control CLI ツール (Linux 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、CLI ツールを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

CLI ツールは選択されたターゲットに存在しなくなります。

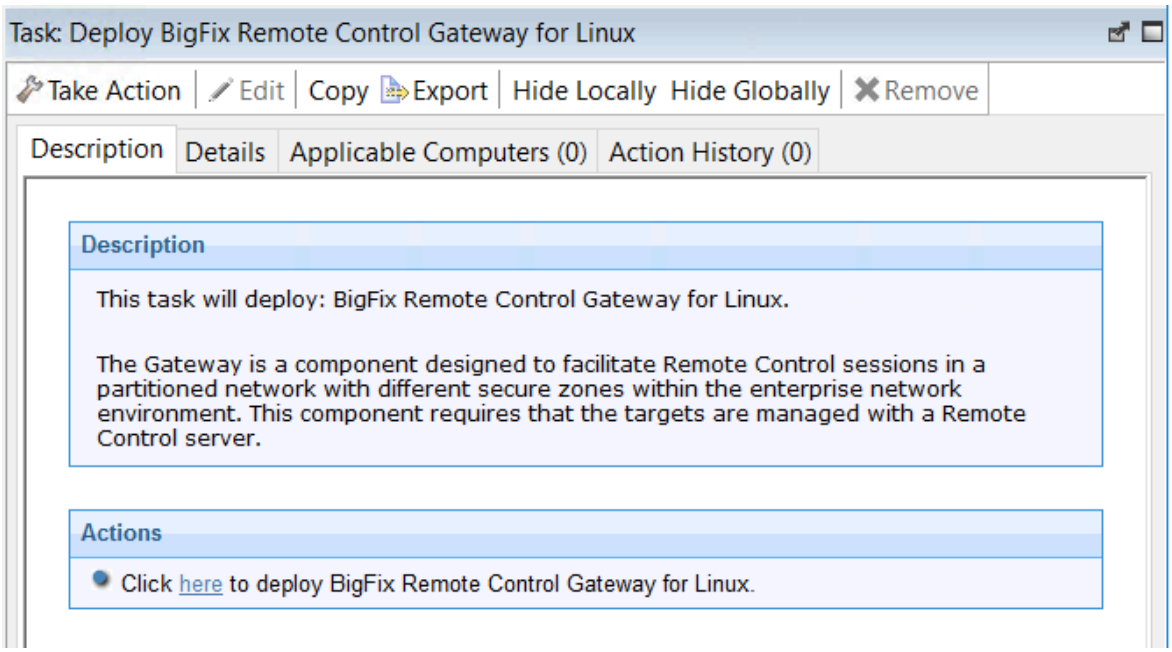
注: CLI ツールが削除された後、一部のファイルは自動的に削除されない場合があります。これらのファイルは、ツールのインストール中に作成されました。これらのファイルは次の `/etc`、`/opt/bigfix`、`/var/opt/bigfix/trc/cli`、`/var/opt/bigfix/trc/target` のディレクトリーにあります。

Linux® ゲートウェイ・サポートのインストール

「Remote Control ゲートウェイ (Linux 版) のデプロイ」タスクを使用すると、ゲートウェイ・サポートを Linux® コンピューターにインストールできます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control ゲートウェイ (Linux 版) のインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、ゲートウェイ・サポートをデプロイするターゲットを決定するために必要なオプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示され、タスク完了時には完了ステータスが表示されます。

ゲートウェイ・サポートが、インストール・タスクを実行したときに選択したターゲットにインストールされます。ファイルは選択したターゲットの `/opt/bigfix/trc/gateway` ディレクトリーにあります。

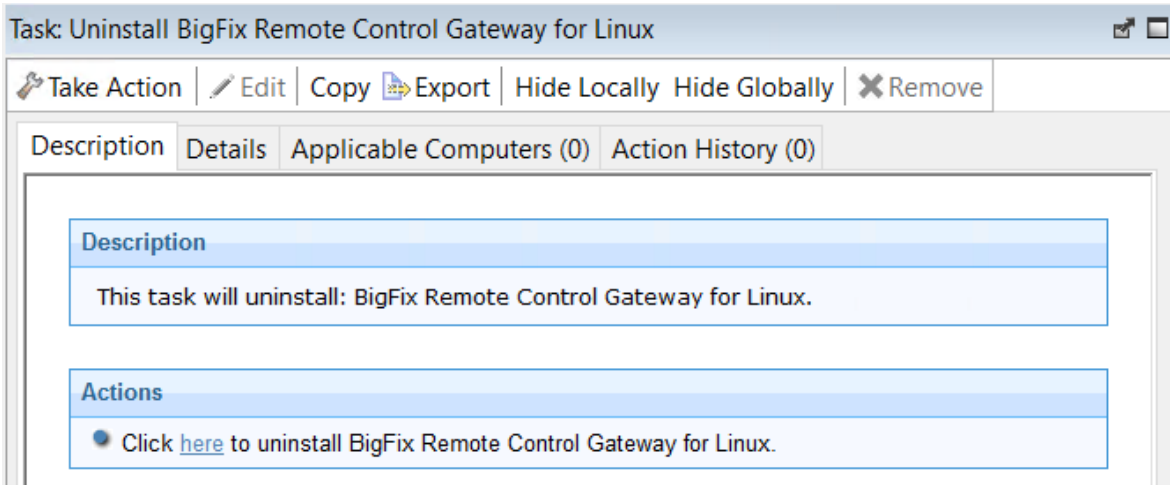
ゲートウェイ・サポートを使用するには、ご使用の環境に合わせてゲートウェイ構成をセットアップする必要があります。これらのゲートウェイの構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

Linux® ゲートウェイ・サポートの削除

「Remote Control ゲートウェイ・サポート (Linux 版) のアンインストール」タスクを使用すると、ゲートウェイ・サポート・ファイルを Linux® コンピューターから削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control ゲートウェイ (Linux 版) のアンインストール」**をクリックします
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、ゲートウェイ・サポートを削除する対象コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示され、タスク完了時には完了ステータスが表示されます。

ゲートウェイ・サポート・ファイルは、選択されたターゲットから削除されます。

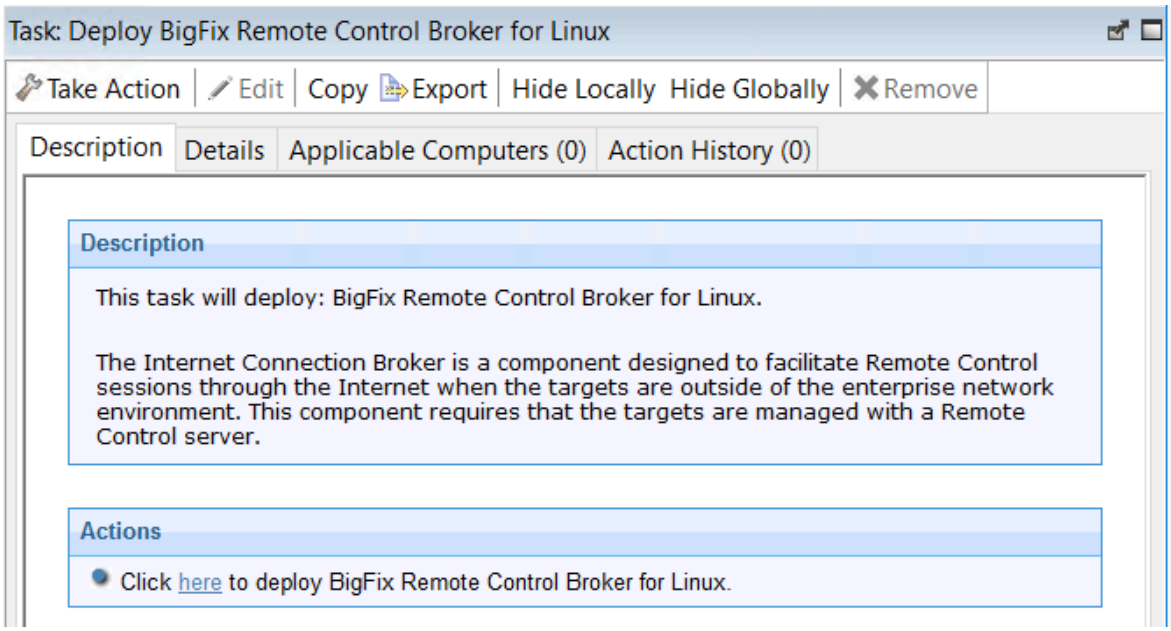
注: ゲートウェイ・サポートが削除された後、一部のファイルは自動的に削除されない場合があります。これらのファイルは、ゲートウェイ・コンポーネントのインストール中に作成されました。これらのファイルは `/opt/bigfix` および `/var/opt/bigfix/trc/gateway` のディレクトリーにあります。

Linux ブローカー・サポートのデプロイ

「Remote Control ブローカー (Linux 版) をインストール」タスクを使用すると、ブローカー・サポートを Linux コンピューターにインストールできます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control ブローカー (Linux 版) のインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、ブローカー・サポートをデプロイするターゲットを決定するために必要なオプションを選択します。
5. **「OK」**。

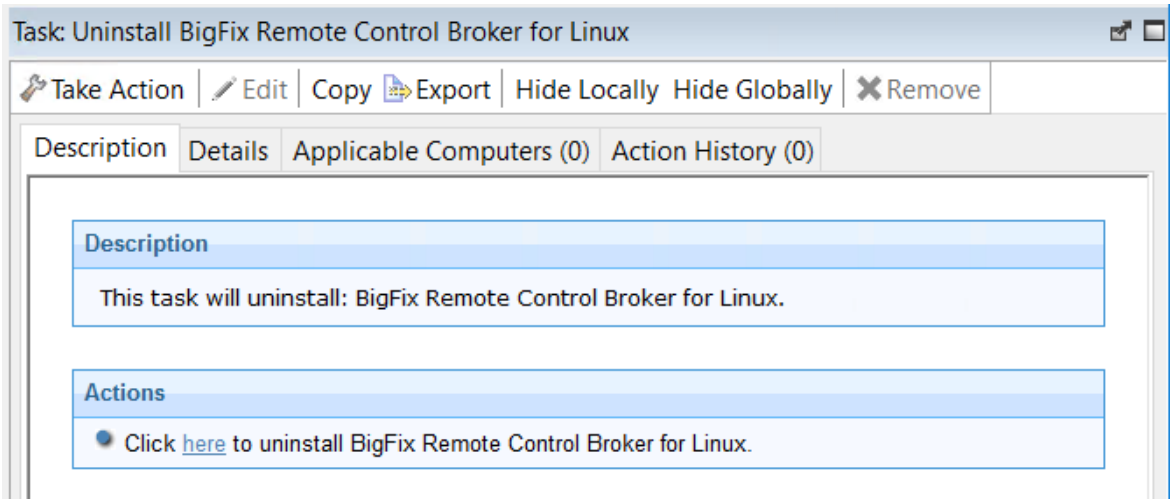
概要画面にタスクの進行状況が表示されます。ブローカー・サポート・ファイルが、インストール・タスクを実行したときに選択したターゲットにインストールされます。ファイルは選択したターゲットの `/opt/bigfix/trc/broker` ディレクトリーにインストールされます。ブローカー・サポートを使用するには、ご使用の環境に合わせてブローカー構成をセットアップする必要があります。これらのブローカーの構成について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

Linux ブローカー・サポートの削除

「Remote Control ブローカー (Linux 版) のアンインストール (Uninstall Broker for Linux)」タスクを使用すると、ブローカー・サポートを Linux コンピューターから削除できます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control ブローカー (Linux 版) のアンインストール」**をクリックします。
3. タスク・ペインで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. 「アクションの実行」ペインの「対象」タブで、ブローカー・サポートを削除するターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。ブローカー・サポート・ファイルは、選択されたターゲットから削除されます。

macOS システムでのコンポーネントのデプロイ

macOS デプロイメント・ノードには、macOS オペレーティング・システム環境で以下のコンポーネントをインストールまたは削除するために使用できる一連のタスクが用意されています。

- ターゲット・コンポーネント
- コントローラー・コンポーネント

BigFix® Remote Control Target for macOSのデプロイ

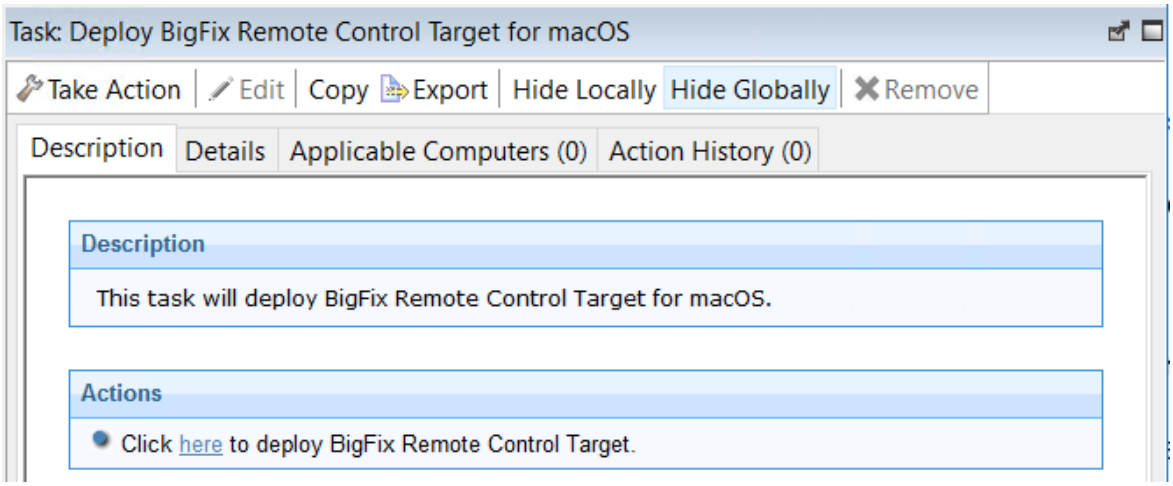
「BigFix® Remote Control Target for macOS のデプロイ」タスクを使用してターゲット・ソフトウェアを macOS システムにインストールします。

注: 管理対象モードを選択するためのオプション (サーバー URL とセキュア登録トークンを求めるプロンプトが出されるオプション) は、管理対象モードが BigFix® Remote Control Target for macOS ではサポートされないために使用できません。

ターゲットをインストールするには、以下のステップを実行します。

1. **「システム・ライフサイクル」**ドメイン内で、**「Remote Control の設定」** > **「Remote Control」**を展開します。
2. **「デプロイメント」**ノードを展開します。
3. **「macOS」**を選択します。

4. **「BigFix® Remote Control Target for macOS のデプロイ 」**を選択します。
5. **「タスク」**ペインで、説明を確認し、**「アクション」**ボックス内の指示に従ってタスクを開始します。



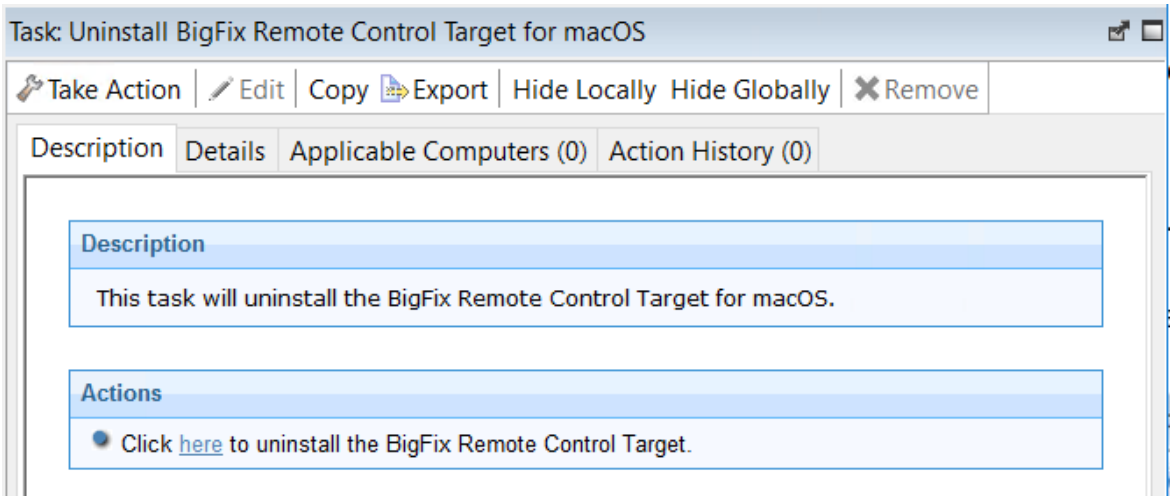
6. **「アクションの実行」**ペインの**「対象」**タブで、BigFix® Remote Control Target for macOS コンポーネントをデプロイするコンピューターを決定するための関連オプションを選択します。
7. 「**OK**」をクリックします。
   概要画面にタスクの進行状況が表示され、タスクが完了すると状況が**「完了」**に設定されます。

以下の削除: BigFix® Remote Control Target for macOS

「アンインストール」BigFix® Remote Control Target for macOSタスクを使用してターゲット・ソフトウェアを macOS システムから削除します。

ターゲットを削除するには、以下の手順を実行します。

1. **「システム・ライフサイクル」**ドメイン内で、**「Remote Control の設定」 > 「Remote Control」**を展開します。
2. **「デプロイメント」**ノードを展開します。
3. **「macOS」**を選択します。
4. **「アンインストール」BigFix® Remote Control Target for macOS**を選択します。
5. **「タスク」**ペインで、説明を確認し、**「アクション」**ボックス内の指示に従ってタスクを開始します。



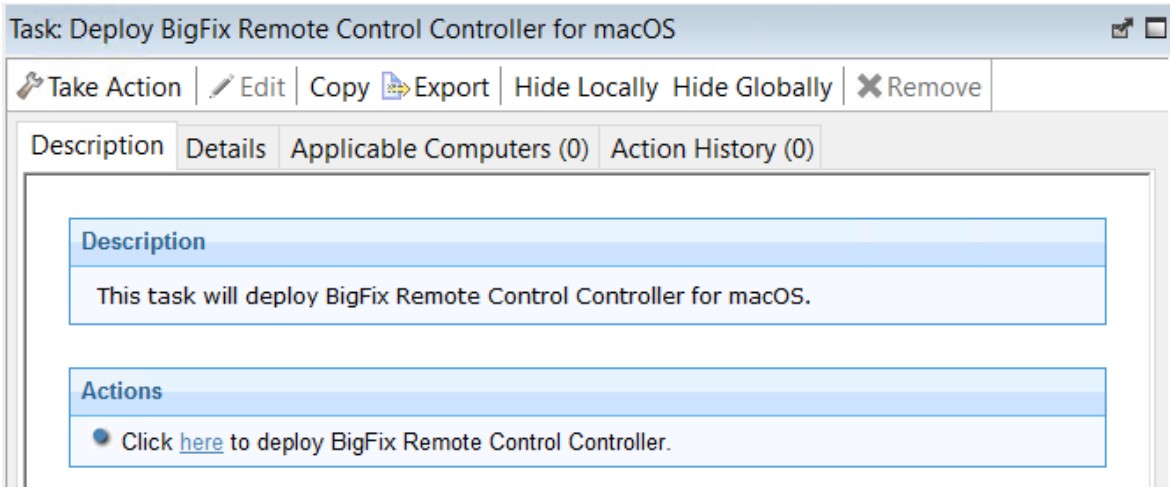
6. **「アクションの実行」**ペインの**「対象」**タブで、BigFix® Remote Control Target for macOS コンポーネントを削除するコンピューターを決定するための関連オプションを選択します。
7. 「**OK**」をクリックします。
   概要画面にタスクの進行状況が表示され、タスクが完了すると状況が**「完了」**に設定されます。

BigFix® Remote Control Controller for macOSのデプロイ

「BigFix® Remote Control Controller for macOS のデプロイ」タスクを使用してコントローラー・ソフトウェアを macOS システムにインストールします。

コントローラーをインストールするには、以下の手順を実行します。

1. **「システム・ライフサイクル」**ドメイン内で、**「Remote Control の設定」** > **「Remote Control」**を展開します。
2. **「デプロイメント」**ノードを展開します。
3. **「macOS」**を選択します。
4. **「BigFix® Remote Control Controller for macOS のデプロイ」**を選択します。
5. **「タスク」**ペインで、説明を確認し、**「アクション」**ボックス内の指示に従ってタスクを開始します。



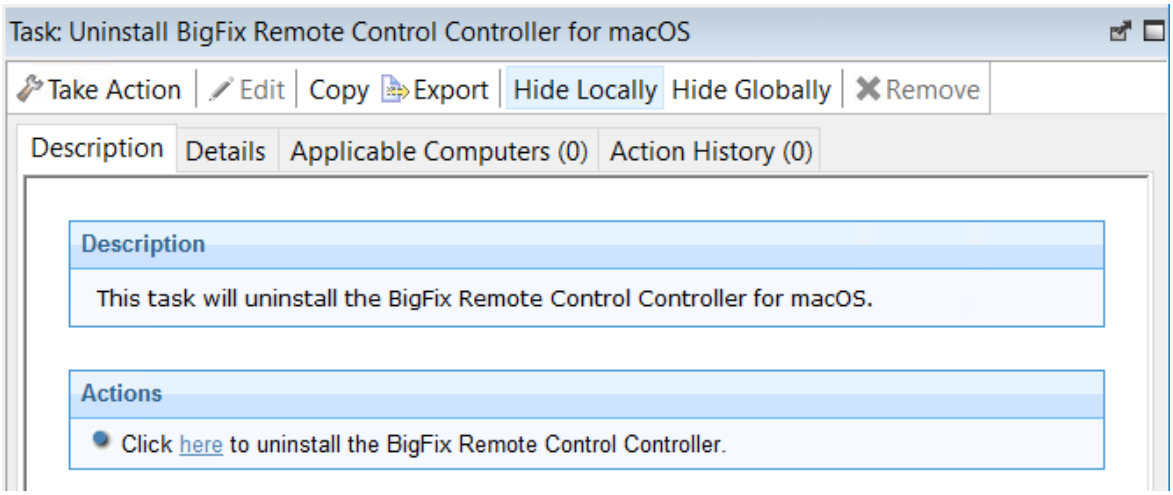
6. **「アクションの実行」**ペインの**「対象」**タブで、BigFix® Remote Control Controller for macOS コンポーネントをデプロイするコンピューターを決定するための関連オプションを選択します。
7. 「**OK**」をクリックします。
   概要画面にタスクの進行状況が表示され、タスクが完了すると状況が**「完了」**に設定されます。

以下の削除: BigFix® Remote Control Controller for macOS

「アンインストール」BigFix® Remote Control Controller for macOSタスクを使用してコントローラー・ソフトウェアを macOS システムから削除します。

コントローラーを削除するには、以下の手順を実行します。

1. **「システム・ライフサイクル」**ドメイン内で、**「Remote Control の設定」** > **「Remote Control」**を展開します。
2. **「デプロイメント」**ノードを展開します。
3. **「macOS」**を選択します。
4. **「アンインストール」BigFix® Remote Control Controller for macOS**を選択します。
5. **「タスク」**ペインで、説明を確認し、**「アクション」**ボックス内の指示に従ってタスクを開始します。



6. **「アクションの実行」**ペインの**「対象」**タブで、BigFix® Remote Control Controller for macOS コンポーネントを削除するコンピューターを決定するための関連オプションを選択します。
7. 「**OK**」をクリックします。
   概要画面にタスクの進行状況が表示され、タスクが完了すると状況が**「完了」**に設定されます。

Remote Control コンポーネントの更新

Remote Control ナビゲーション・ツリーの**「更新」**ノードには、オペレーティング・システム固有のサブノードがあります。コンポーネントを新しいバージョンにアップグレードするには、**「更新」**ノードを使用します。コンポーネントのアップグレードに使用できるタスクのリストを表示するには、関連するオペレーティング・システム・ノードを選択します。

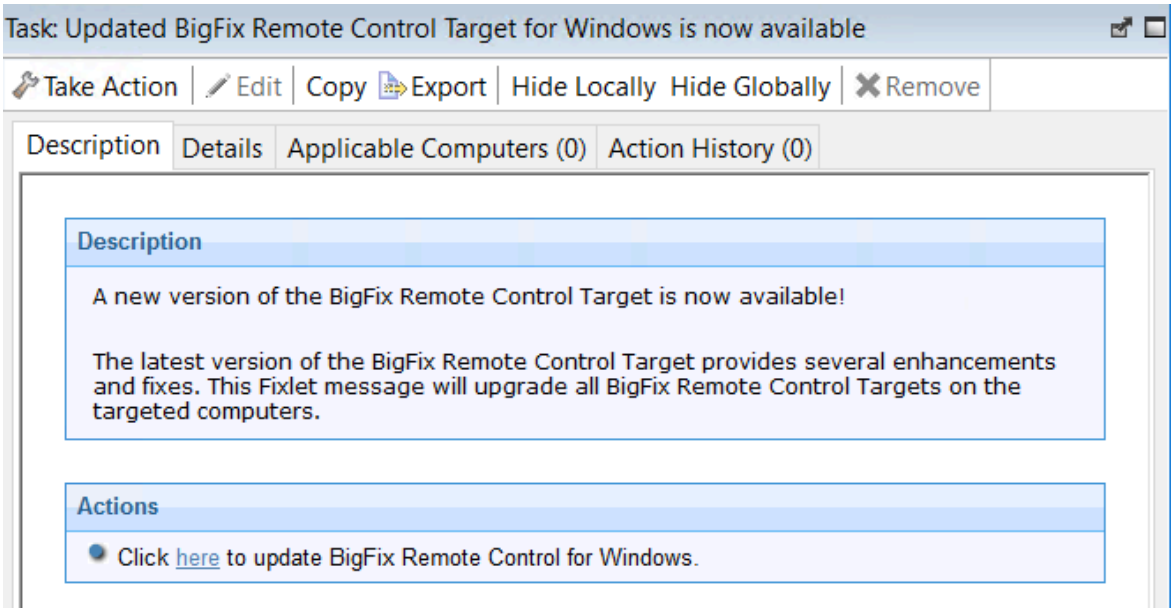
Windows™ システムでのコンポーネントの更新

Windows サブノードには、Windows™ システムで使用する最新レベルの Remote Control コンポーネント・ソフトウェアが用意されています。これらのコンポーネントには、Remote Control に適用された最新の機能拡張およびフィックスが含まれます。

Windows™ ターゲットの更新

Windows™ オペレーティング・システム・タスクを使用して、Windows™ コンピューター上のターゲット・ソフトウェアを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているターゲット構成に適用されます。タスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」** > **「Windows」**をクリックします。
2. アップグレード後のターゲットのバージョンに関連する Fixlet を選択します。
   例えば、**「更新された Remote Control ターゲット (Windows 版) を提供しています(バージョン 10.x.x)**。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。
   例えば、以下のようにします。



4. **「アクションの実行」**ウィンドウの「対象」タブで、ターゲットの更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

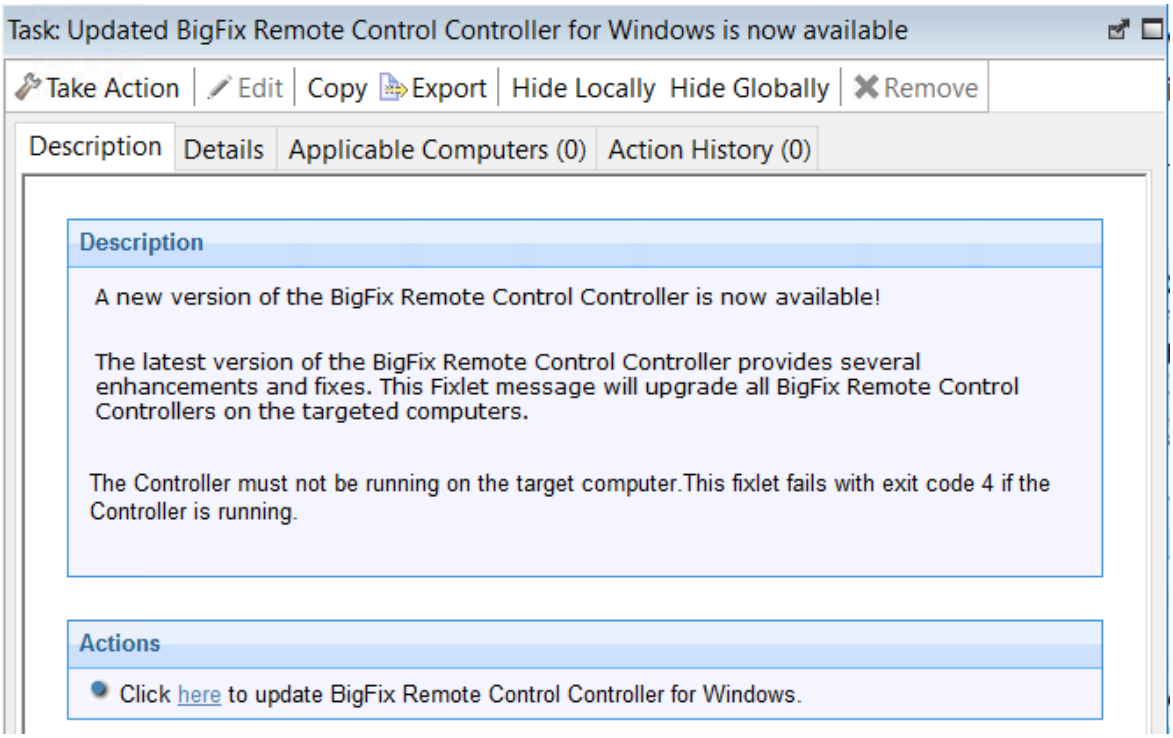
概要画面にタスクの進行状況が表示されます。

これで、選択されたターゲットは、選択された更新に該当するターゲット・ソフトウェアのバージョンにアップグレードされます。

Windows™ コントローラーの更新

Windows™ オペレーティング・タスクを使用して、Windows™ コンピューター上のコントローラー・ソフトウェアを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているコントローラーに適用されます。タスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Windows」**をクリックします。
2. アップグレード後のコントローラーのバージョンに関連する Fixlet を選択します。
   例えば、**「更新された Remote Control コントローラー (Windows 版) を提供しています (バージョン 10,x,x)」**を選択します。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ウィンドウの「対象」タブで、コントローラーの更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

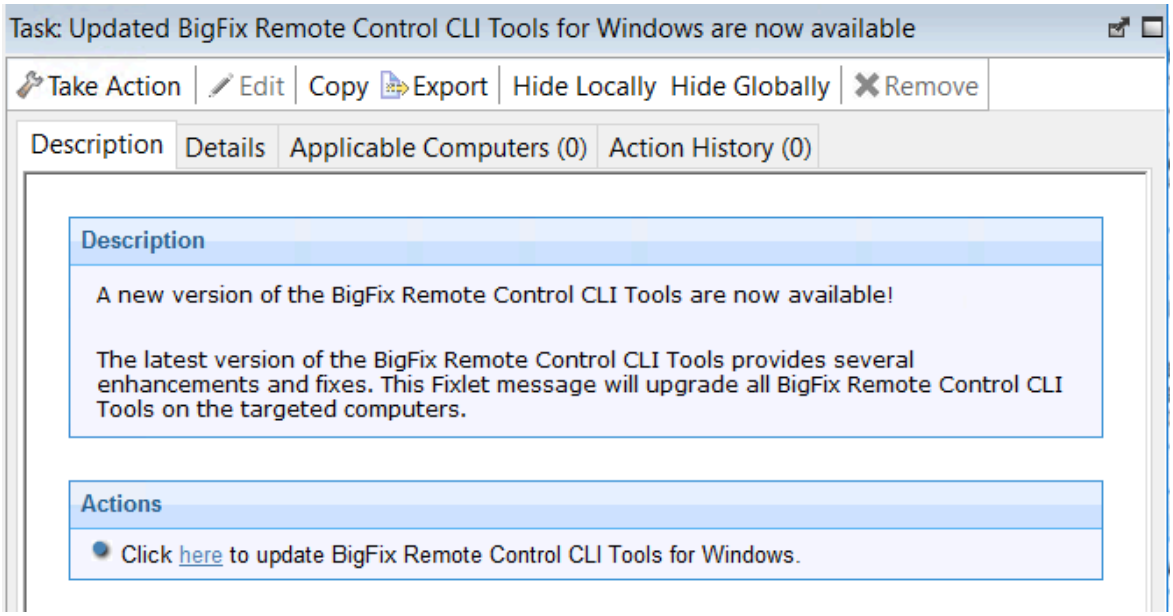
概要画面にタスクの進行状況が表示されます。

選択されたターゲット上のコントローラー・ソフトウェアは、選択された更新のバージョンにアップグレードされます。

Windows™ コマンド・ライン・ツールの更新

Windows™ オペレーティング・システム・タスクを使用して、Windows™ コンピューター上の CLI ツールを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされている CLI ツール構成に適用されます。タスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Windows」**をクリックします。
2. アップグレード後の CLI ツールのバージョンに関連する Fixlet を選択します。例えば、**「更新された Remote Control CLI ツール (Windows 版) を提供しています (Updated CLI tools for Windows is now available!) (バージョン 10.x.x)**。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ウィンドウの「対象」タブで、CLI の更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

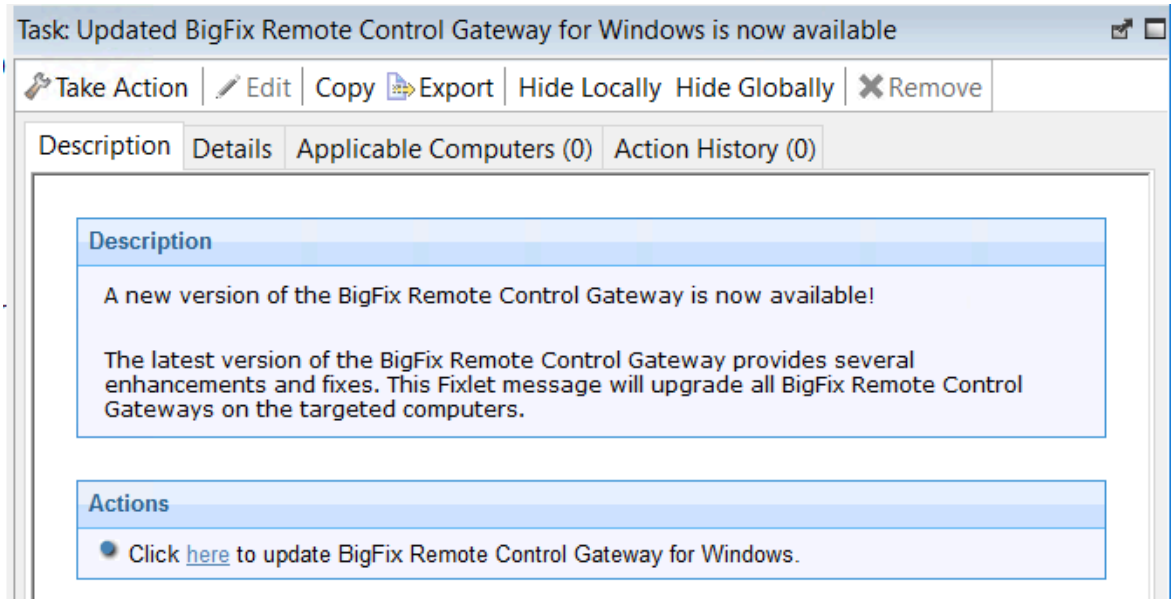
選択されたターゲット上の CLI ツールは、選択された更新のバージョンにアップグレードされます。

Windows™ ゲートウェイ・サポートの更新

Windows™ オペレーティング・システム・タスクを使用して、Windows™ コンピューター上のゲートウェイ・サポート・ファイルを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているゲートウェイ構成に適用されます。

タスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Windows」**をクリックします。
2. アップグレード後のゲートウェイのバージョンに関連する Fixlet を選択します。例えば、**「更新された Remote Control ゲートウェイ (Windows 版) を提供しています (Updated Gateway for Windows is now available!) (バージョン 10.x.x)**。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ウィンドウの「対象」タブで、ゲートウェイの更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

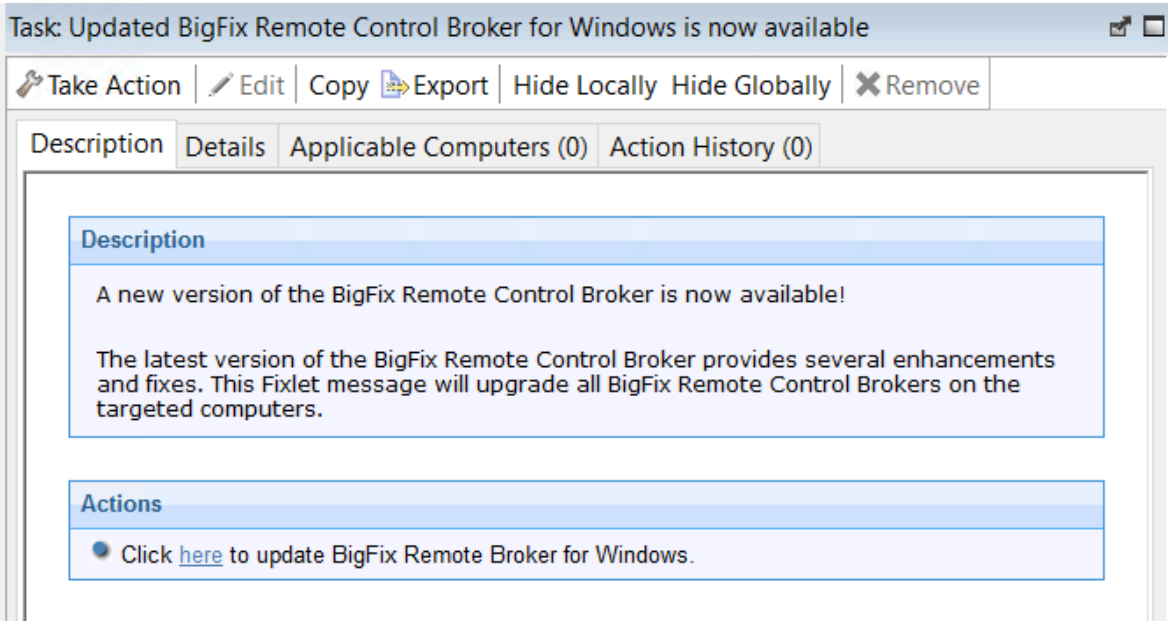
概要画面にタスクの進行状況が表示されます。

選択されたターゲット上のゲートウェイ・サポートは、選択された更新のバージョンにアップグレードされます。

Windows™ ブローカー・サポートの更新

Windows™ オペレーティング・システム・タスクを使用して、Windows™ コンピューター上のブローカー・ソフトウェアを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているブローカーに適用されます。タスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Windows」**をクリックします。
2. アップグレード後のブローカーのバージョンに関連する Fixlet を選択します。
   例えば、**「更新された Remote Control ブローカー (Windows 版) を提供しています (Updated Broker for Windows is now available!) (バージョン 10.x.x)**。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ウィンドウの「対象」タブで、ブローカーの更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

選択されたターゲット上のブローカー・ソフトウェアは、選択された更新のバージョンにアップグレードされます。

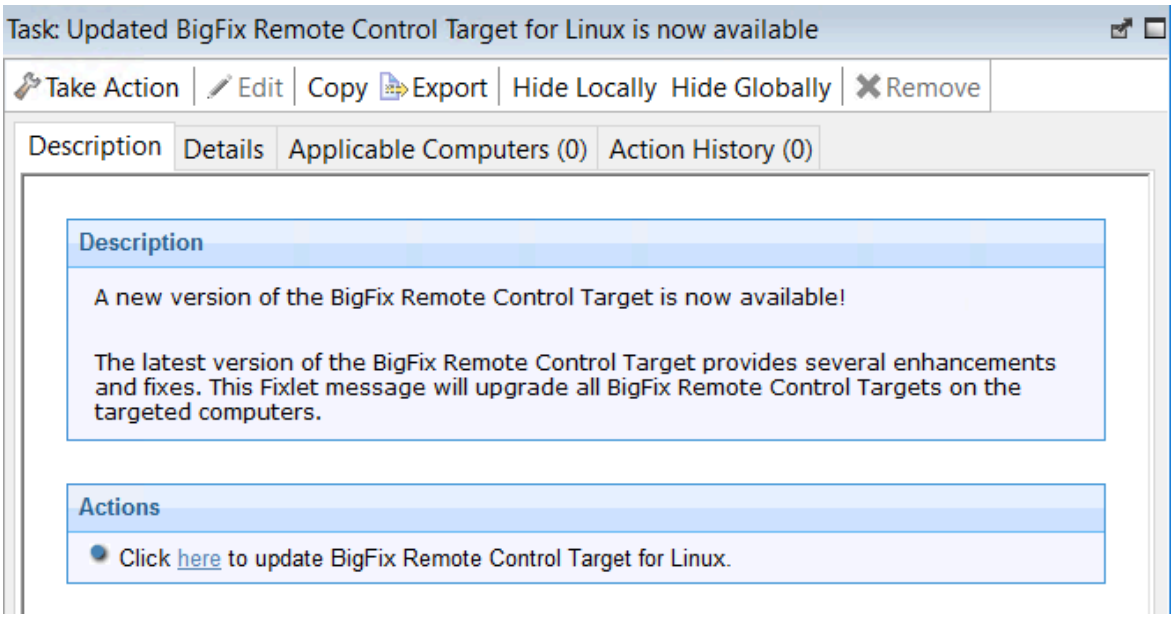
Linux® コンポーネントの更新

Linux® サブノードには、Linux® 環境用の最新レベルの Remote Control コンポーネント・ソフトウェアが用意されています。これらのコンポーネントには、Remote Control に適用された最新の機能拡張およびフィックスが含まれます。

Linux™ ターゲットの更新

Linux™ タスクを使用して、Linux™ コンピューター上のターゲット・ソフトウェアを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているターゲット構成に適用されます。このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Linux」**をクリックします。
2. アップグレード後のターゲットのバージョンに関連する Fixlet を選択します。例えば、**「更新された Remote Control ターゲット (Linux 版) を提供しています (Updated Target for Linux is now available!) (バージョン 10.x.x)**。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



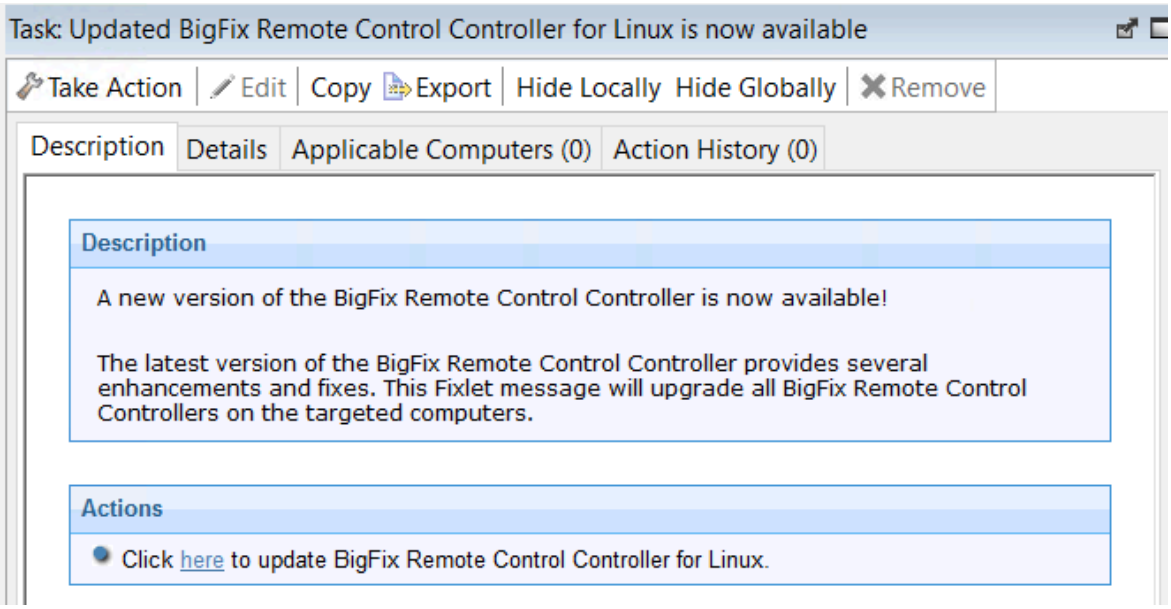
4. **「アクションの実行」**ウィンドウの「対象」タブで、ターゲットの更新をインストールするターゲット・コンピューター (複数可) を決定するためにオプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

Linux™ コントローラーの更新

Linux™ タスクを使用して、Linux™ コンピューター上のコントローラー・ソフトウェアを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているコントローラー構成に適用されます。タスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Linux」**をクリックします。
2. アップグレード後のコントローラーのバージョンに関連する Fixlet を選択します。
   例えば、**「更新された Remote Control Controller (Linux 版) を提供しています (バージョン 10,x,x)」**を選択します。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



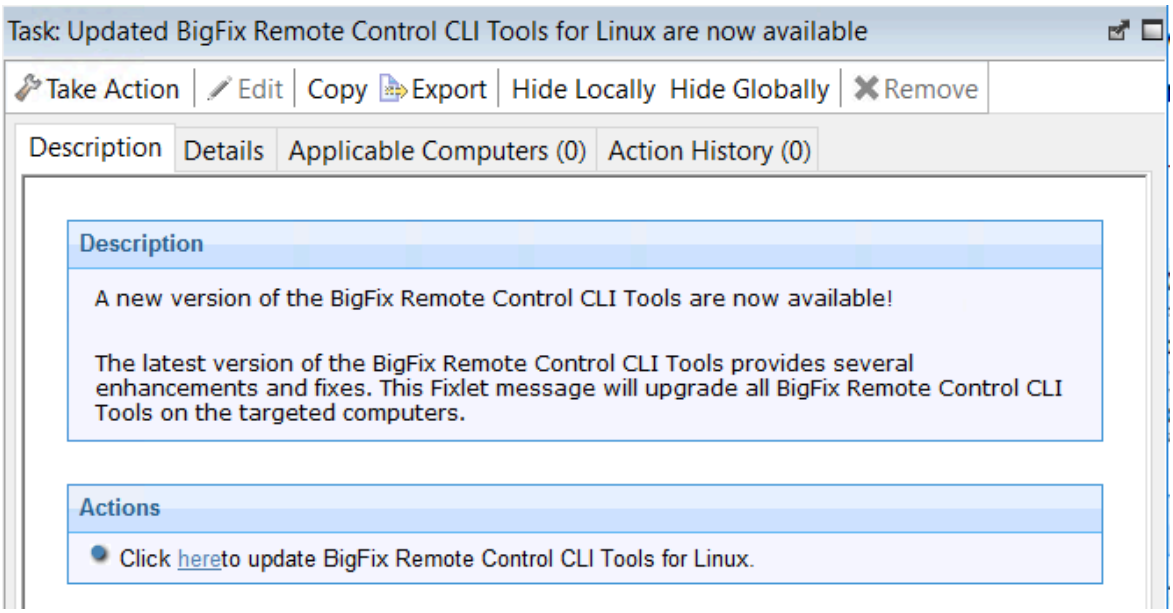
4. **「アクションの実行」**ウィンドウの「対象」タブで、コントローラーの更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。選択されたターゲット上のコントローラー・ソフトウェアは、選択された更新のバージョンにアップグレードされます。

Linux™ コマンド・ライン・ツールの更新

Linux™ タスクを使用して、Linux™ コンピューター上の CLI ツールを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされている CLI ツール構成に適用されます。このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Linux」**をクリックします。
2. アップグレード後の CLI ツールのバージョンに関連する Fixlet を選択します。例えば、**「更新された Remote Control CLI ツール (Linux 版) を提供しています (Updated CLI tools for Linux is now available!) (バージョン 10.x.x)**。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ウィンドウの「対象」タブで、CLI の更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

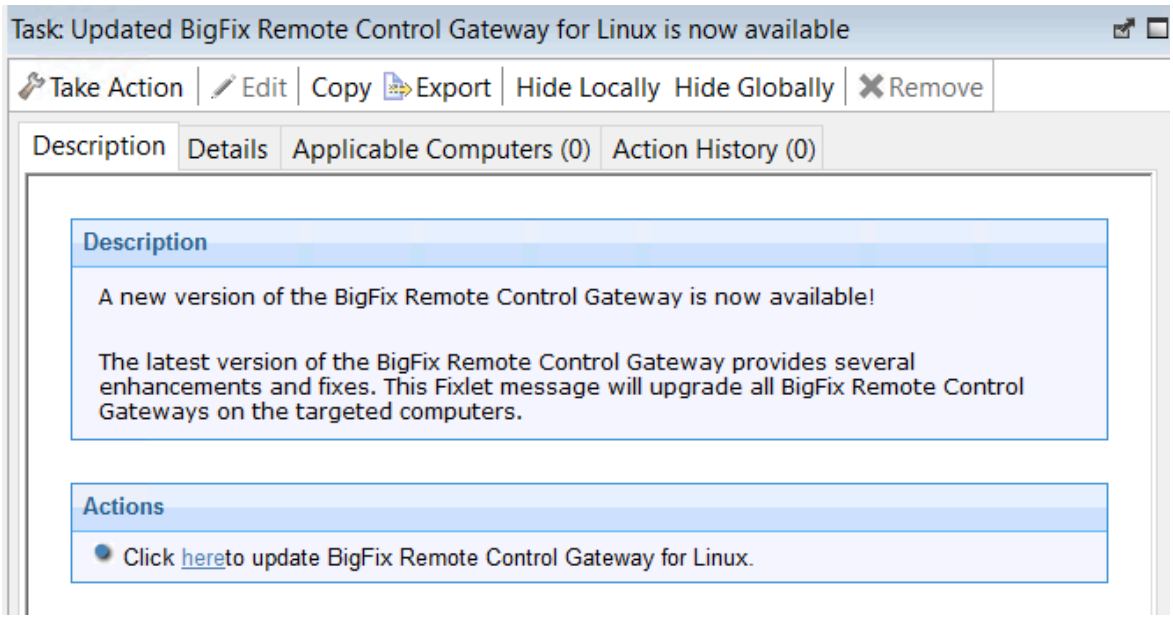
選択されたターゲット上の CLI ツールは、選択された更新のバージョンにアップグレードされます。

Linux™ ゲートウェイ・サポートの更新

Linux™ タスクを使用して、Linux™ コンピューター上のゲートウェイ・サポート・ファイルを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているゲートウェイ構成に適用されます。

このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Linux」**をクリックします。
2. アップグレード後のゲートウェイのバージョンに関連する Fixlet を選択します。例えば、**「更新された Remote Control ゲートウェイ (Linux 版) を提供しています (バージョン 10.x.x)」**を選択します。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ウィンドウの「対象」タブで、ゲートウェイの更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

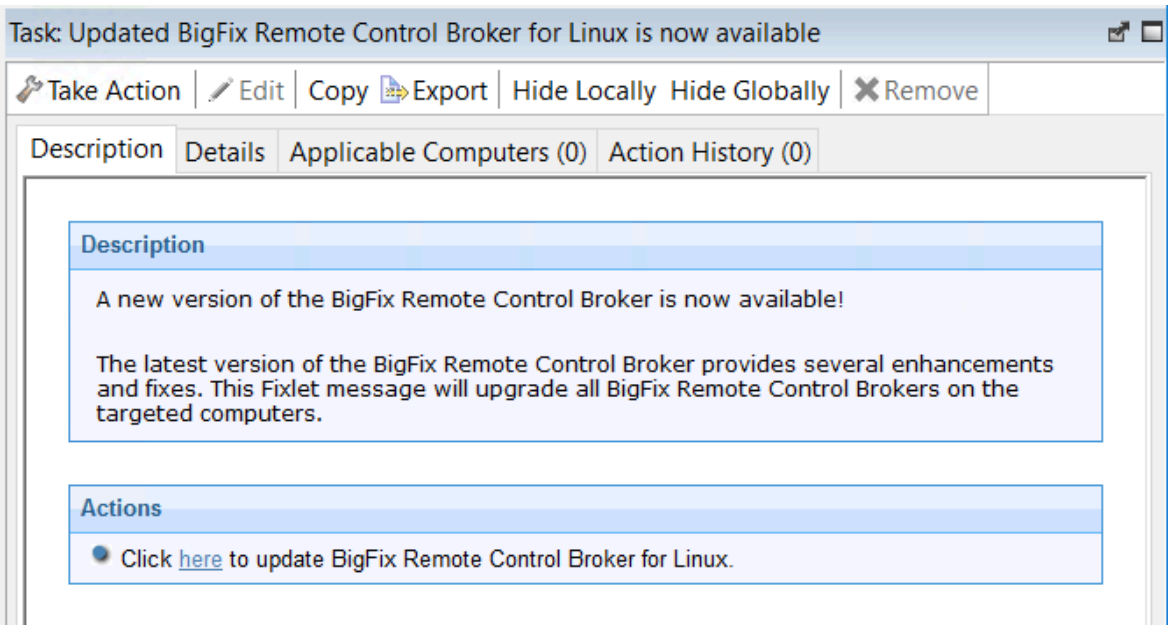
概要画面にタスクの進行状況が表示されます。

選択されたターゲット上のゲートウェイ・サポートは、選択された更新のバージョンにアップグレードされます。

Linux® ブローカー・サポートの更新

Linux タスクを使用して、Linux® コンピューター上のブローカー・ソフトウェアを更新します。これらのタスクでは、選択したバージョンに含まれているすべての新規拡張機能およびフィックスが、既にインストールされているブローカー構成に適用されます。このタスクを開始するには、以下のステップを実行します。

1. ナビゲーション・ツリーの**「更新」 > 「Linux」**をクリックします。
2. アップグレード後のブローカーのバージョンに関連する Fixlet を選択します。
   例えば、**「更新された Remote Control ブローカー (Linux 版) を提供しています (バージョン 10.x.x)」**を選択します。
3. **「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



4. **「アクションの実行」**ウィンドウの「対象」タブで、ブローカーの更新をインストールするターゲット・コンピューター (複数可) を決定するために関連オプションを選択します。
5. **「OK」**。

概要画面にタスクの進行状況が表示されます。

選択されたターゲット上のブローカー・ソフトウェアは、選択された更新のバージョンにアップグレードされます。

Remote Control サーバー・コンポーネントのダウンロード

Fixlet を実行して、選択したコンピューター上の特定の場所に Remote Control サーバーのインストーラー・ファイルをダウンロードすることができます。

Windows 用の Remote Control サーバーのインストーラー・ファイルのダウンロード

BigFix® コンソールで Fixlet を実行して、Windows 用の Remote Control サーバーのインストーラー・ファイルをダウンロードします。

`trc_server_setup.exe` ファイルをダウンロードするには、以下の手順を実行します。

1. ナビゲーション・ツリーで、**「デプロイメント」** > **「Windows」**をクリックします。
2. **「Remote Control サーバー (Windows 版) をダウンロード」**タスクを選択します。
3. **「説明」**タブの情報を確認します。
4. **「アクション」**フィールドの指示に従ってインストーラー・ファイルをダウンロードします。
5. インストーラー・ファイルを保存する場所を入力して、**「OK」**をクリックします。

`trc_server_setup.exe` ファイルが、選択されたコンピューターにダウンロードされます。サーバーのインストールについて詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

Linux 用の Remote Control サーバーのインストーラー・ファイルのダウンロード

BigFix® コンソールで Fixlet を実行して、Linux 用の Remote Control サーバーのインストーラー・ファイルをダウンロードします。

`trc_server_setup.bin` ファイルをダウンロードするには、以下の手順を実行します。

1. ナビゲーション・ツリーで、**「デプロイメント」 > 「Linux」**をクリックします。
2. **「Remote Control サーバー (Linux 版) をダウンロード」**タスクを選択します。
3. **「説明」**タブの情報を確認します。
4. **「アクション」**フィールドの指示に従ってインストーラー・ファイルをダウンロードします。
5. インストーラー・ファイルを保存する場所を入力して、**「OK」**をクリックします。

`trc_server_setup.bin` ファイルが、選択されたコンピューターにダウンロードされます。サーバーのインストールについて詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

リモート・コントロール・セッションの開始

Remote Control コントローラー・コンポーネントおよびターゲット・コンポーネントを使用すると、両者の間にリモート接続を確立して、ターゲット・システムをモニターまたは制御することができます。

リモート・コントロール・セッションのタイプには、ターゲットとコントローラーの間で直接行われる P2P セッションと、Remote Control サーバーから開始される管理対象セッションの 2 つがあります。セッションのタイプについて詳しくは、Remote Control で使用される用語の定義を参照してください。

リモート・コントロール・セッションの終了方法について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

P2P セッションの開始

コントローラーとターゲットの間の P2P リモート・コントロール・セッションを開始するには 2 つの方法があります。

- BigFix® コンソールから行う方法
- コントローラー・コンポーネントを使用する方法

BigFix® コンソールからの P2P セッションの開始

BigFix® コンソールを使用して、コンソールから直接、P2P セッションを開始します。セッションを開始するターゲット・コンピューターを右クリックすると表示されるメニュー・オプションを使用します。

注:

1. リモート・コントロール・セッションを BigFix® コンソールから開始するには、コンソールがインストールされているのと同じコンピューターにコントローラー・コンポーネントをインストールします。ただし、コントローラーがインストールされたとき、セッションを開始するメニュー項目の表示権限があるのは、コントローラー・コンピューターにログオンしている現行ユーザーのみです。メニュー項目は他のユーザーに表示されません。詳しくは、『よくある質問』を参照してください。
2. メニュー項目を使用可能にするには、**「Remote Control のインストールおよびセキュリティー・オプション」**分析が、選択されたコンピューターについてアクティブである必要があります。この分析では、Remote Control ターゲットがアクティブであると報告されている必要があります。

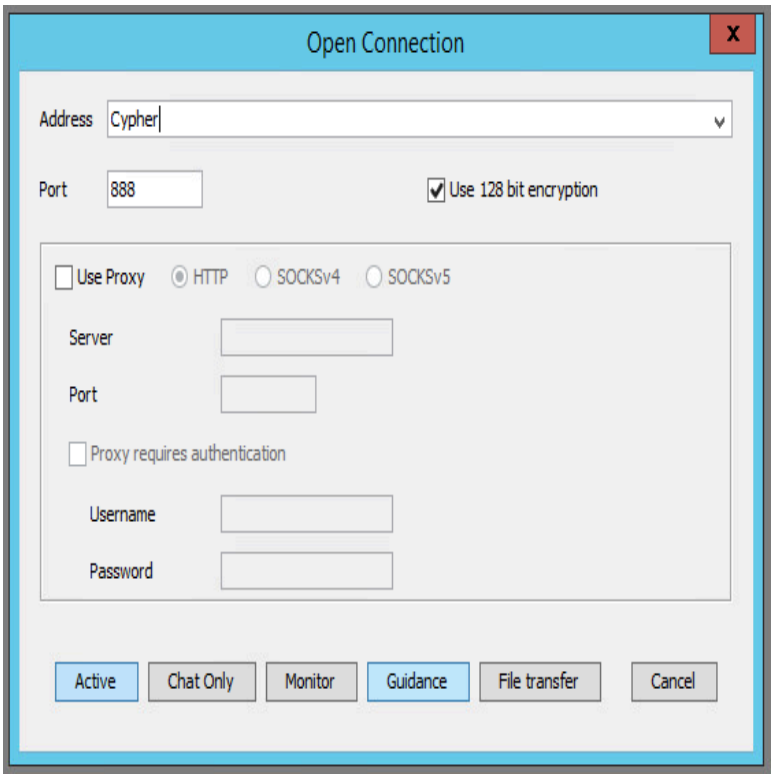
P2P セッションを開始するには、以下の手順を実行します。

1. ターゲット・コンピューターのリストから、リモート・コントロール・セッションを開始する対象となるターゲットを右クリックします。
2. **Remote Control** を選択します。

   注:

   a. このアクションは、コンソールにおいて、コンピューター・リストが表示されるどのセクションでも実行できます。
   b. 以前のバージョンのコントローラーがインストールされている場合は、代わりに「IBM® Endpoint Manager for Remote Control 」がメニュー項目として表示される可能性があります。

3. 「接続を開く」ウィンドウが表示され、接続先となるターゲットの IP アドレスまたは URLが指定されています。



4. プロキシーを使用している場合、**「プロキシーの使用」**を選択します。関連するプロトコルおよび情報を選択します。

   サーバー

   プロキシー・サーバーのホスト名または IP アドレス。

   ポート\n

   プロキシー・サーバーに必要なポート。

   プロキシーは認証が必要です

   プロキシー・サーバーを認証する場合は、このオプションを選択します。認証に有効なユーザー名とパスワードを指定します。

5. セッション・タイプを選択します。
   確立できるセッション・タイプについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

注:

a. ログイン・ウィンドウが表示された場合は、有効な Windows オペレーティング・システム ID およびパスワードを入力して、先に進みます。
b. ターゲットに設定されたポリシーに応じて、ユーザー確認ウィンドウがターゲットで表示される場合があります。ターゲット・ユーザーは、セッションを受け入れるか、または拒否することができます。

セッションが受け入れられて開始されると、ターゲットにローカルに設定されたポリシー値によって、セッション中に実行できるアクションが決まります。P2P セッションの詳細、およびコントローラー UI で使用できる機能については、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

コントローラーを使用した P2P セッションの開始

コントローラー・コンポーネントのインストール対象である任意のコンピューターから、P2P セッションを開始できます。

コントローラー・コンポーネントを使用して P2P セッションを開始するには、以下のステップを実行します。

1. コントローラーを始動します。

   Windows® システム

   a. **「スタート」 > 「すべてのプログラム」**をクリックします。
   b. **「Remote Control」 > 「コントローラー」**をクリックします。

   Linux® システム

   コントローラーを始動するには、オペレーティング・システム・アプリケーション・インターフェースから Remote Control コントローラー・アプリケーションを見つけるか、以下のコマンドを実行します。

   ```
   java jar /opt/bigfix/trc/controller/TRCConsole.jar
   ```

2. BigFix コンソールからの P2P セッションの開始 のステップ 3 以降の説明に従って、セッションを開始します。

セッションが受け入れられて開始されると、ターゲットにローカルに設定されたポリシー値によって、セッション中に実行できるアクションが決まります。P2P セッションの詳細、およびコントローラー UI で使用できる機能については、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

サーバーから起動されるリモート・コントロール・セッションの開始

Remote Control サーバー UI から起動されるリモート・コントロール・セッションを開始するには、サーバー・コンポーネントがインストールされ、稼働している必要があります。サーバー・インストール構成タスクの作成および実行について詳しくは、Remote Control サーバー・インストール・タスクの作成を参照してください。

注: サーバーは、インストール・ファイルを使用してインストールすることもできます。詳しくは、*BigFix® Remote Control* インストール・ガイド を参照してください。

サーバー・コンポーネントをインストールしたら、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を使用して、サーバー UI へのアクセスおよびログオン方法の詳細を確認してください。Remote Control サーバーから起動されるリモート・コントロール・セッションでは、アクセス許可リンクが設定されている必要があります。このリンクは、コントローラー・ユーザーとターゲットが所属するグループ間で作成されます。このアクセス許可リンクによって、セッションに有効なポリシーが決定されます。ユーザー・グループおよびターゲット・グループ

の作成、アクセス許可リンクの作成、およびリモート・コントロール・セッションのポリシーの解決方法について詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

サーバーをインストールして、関連グループおよびアクセス許可リンクを作成したら、Remote Control サーバー UI を使用してリモート・コントロール・セッションを開始できます。詳しくは、*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド を参照してください。

警告への対処

検出プロセス中に、Remote Control コンポーネントの通常操作を妨げる問題が検出された場合は、Remote Control ナビゲーション・ツリーに**「警告」**ノードが表示されます。

注: 検出プロセス中に問題が検出されない場合、ナビゲーション・パネルにこのノードは表示されません。

このノードには、該当するコンピューターでの問題の解決に使用できる、関連 Fixlet が表示されます。Remote Control ターゲット・ソフトウェアをインストールすると、Remote Control の受信ポートを開くためのデフォルト・ファイアウォール・ルールが作成されます。ターゲット・オペレーティング・システムがこのポートをブロックしている場合は、Fixlet を使用して、Remote Control の受信 TCP 接続を有効にするためのルールを追加します。

注: SUSE ファイアウォール Fixlet は、ファイアウォールが手動で始動される場合は関連せず、ファイアウォールが自動モードの場合にのみ関連します。

ターゲット構成およびサーバー構成の管理

Remote Control には、Remote Control サーバー構成またはターゲット構成をインストールするタスクの作成に使用できる 2 つのウィザードがあります。これらのタスクは、すべてのサーバーまたはターゲットに対して、あるいは特定のサーバーまたはターゲットに対して実行できます。

Remote Control サーバー・インストール・タスクの作成

Remote Control **サーバー・インストーラー・ウィザード**を使用して、リモート・コントロール・サーバーをインストールするインストール・タスクを作成できます。

このタスクを Windows™® システムまたは Linux™ (Red Hat および SUSE) システムで実行して、完全に機能する自己完結型の Remote Control サーバーを、以下のいずれかのコンポーネント設定でインストールします。

- WebSphere® Application Server Liberty Profile バージョン および Derby データベースを備えた Remote Control サーバー。
- WebSphere® Application Server Liberty Profile バージョン および以下のいずれかのデータベースを備えた Remote Control サーバー。
    - IBM DB2 11.5 仮想プロセッサー・コア (VPC)。
    - Oracle 11g および 12c。

Oracle データベースを使用する場合、Oracle 11g ドライバーを使用している場合は、trc.properties ファイルで oracle.increment.keys.off=1 を設定してください。サーバー・サービスを再起動します。

- Microsoft SQL Server 2008、2012、2014、2016、2017、2019。

  バージョンが 6.3 以上の JDBC ドライバーを使用する必要があります。古いバージョンでは、TLS1.2 または JRE8 はサポートされません。

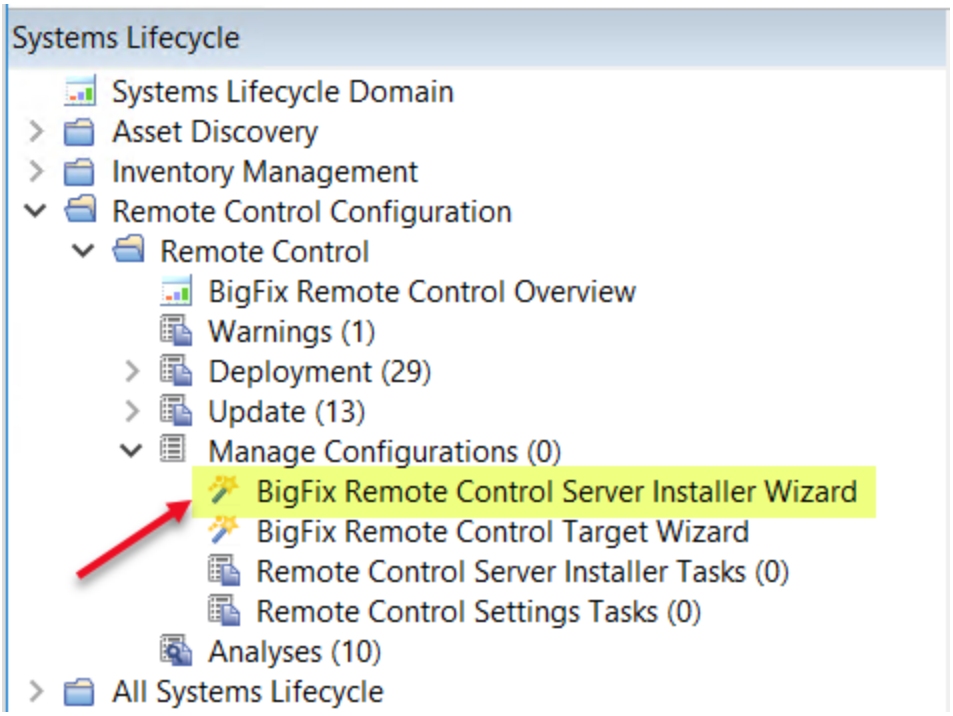
  MS SQL データベースを使用する場合、Windows™ 認証はサポートされません。ドメイン・ユーザーを使用してログインすることはできません。混合モード認証を使用し、データベースに接続するための SQL ユーザーを作成する必要があります。

注:

1. DB2®、MS SQL、または Oracle データベース・オプションを選択する場合は、サーバー・インストール・タスクを実行する前に、データベースをインストールして、データベース・インスタンスを作成しておく必要があります。
2. DB2® 9.7 GA バージョンを使用する場合、DB2® には生成されたキー値で NULL 値が返されるという問題があるため、DB2® 9.7 フィックス・パック 1 にアップグレードする必要があります。

Remote Control サーバー・インストーラー・ウィザードにアクセスするには、以下のステップを実行します。

1. Remote Control ナビゲーション・ツリーで、**「設定の管理」 > 「Remote Control サーバー・インストーラー・ウィザード」**を選択します。



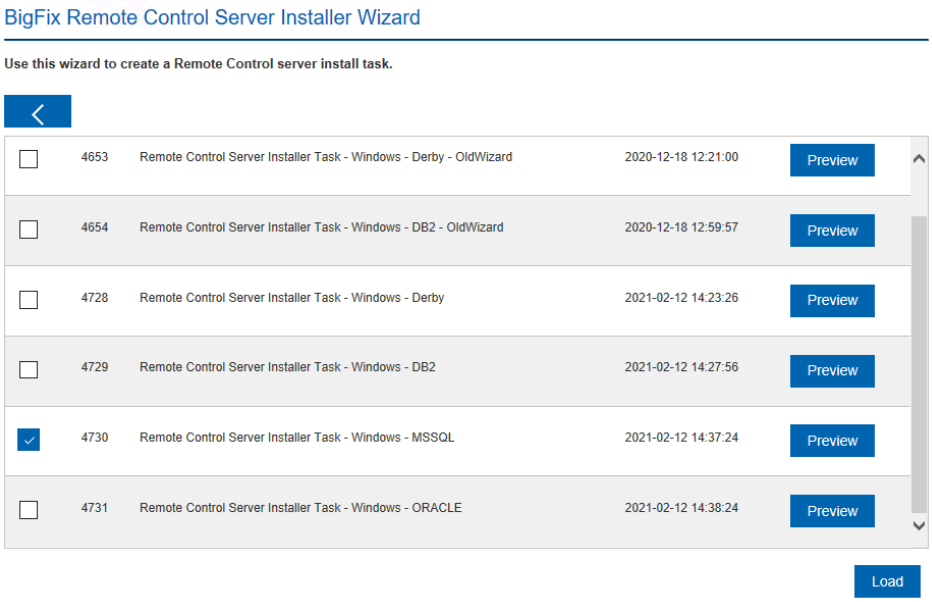
2. 以下のいずれかのオプションを使用して、構成値を設定します。

「既存のタスクから設定を読み込む」

ウィザードは最初はサーバー構成のデフォルト値を表示しますが、これらの値は要件に合うように変更できます。以前に保存した設定をロードするには、以下の手順を実行します。

a. **「既存のタスクから設定を読み込む」**をクリックします。

b. **「ウィザードの Fixlet」**画面で、タスクを選択します。



c. **「Fixlet を使用してウィザードを読み込み」**をクリックします。構成値がウィザードにロードされます。

d. 新しい構成タスクの作成の手順に従い、新しい構成タスクを作成します。

「デフォルト値にリセット」

この機能を使用すると、すべての選択をクリアし、ウィザード内の値をデフォルト構成値に戻すことができます。

新しい構成タスクの作成

ご使用のデータベースに該当する手順に従ってください。

- Derby のインストール。詳しくは、『デフォルト・サーバー構成の作成』を参照してください。
- DB2®. 詳しくは、『DB2 サーバー構成の作成』を参照してください。
- MSSQL. 詳しくは、『MS SQL サーバー構成の作成』を参照してください。
- Oracle。詳しくは、『Oracle サーバー構成の作成』を参照してください。

デフォルト・サーバー構成の作成

デフォルト・サーバー構成を使用して、Remote Control のインストールの一部として含まれている組み込み Derby データベースをインストールし、使用します。データベースは、ローカルにインストールされます。デフォルト・インストール・タスクを作成するには、以下のステップを実行します。

1. 関連するオペレーティング・システムを選択します。
2. Remote Control サーバーがインストールされるインストール・ディレクトリーを入力するか、提示されているデフォルトを受け入れます。

   注: WebSphere® Application Server は、名前に非英語文字が含まれているディレクトリーにはインストールできません。このインストールでは、組み込みバージョンの WebSphere® Application Server がインストールされます。そのため、英語以外の文字が含まれていないインストール・ファイルの宛先を選択する必要があります。

3. **「Derby」**を選択し、関連するデータベース・パラメーター値を入力します。

   「使用するデータベース名」

   Remote Control サーバーで使用されるデータベースの名前を指定するか、提示されているデフォルトを受け入れます。

4. サーバー・インストール・パラメーター値を入力します。

   「デフォルトでターゲットの URL に HTTPS を使用」

   ターゲットが HTTPS サーバー URL を使用してサーバーと通信する場合、このオプションを選択します。`trc.properties` ファイル内の **enforce.secure.endpoint.callhome** プロパティーと **enforce.secure.endpoint.upload** プロパティーも *true* に設定されています。これを選択しない場合は、HTTP URL が使用されます。 HTTPS によるログオンおよび Web ポータルへのアクセスを有効にする **enforce.secure.web.access**、 **enforce.secure.weblogon**、および **enforce.secure.alllogon** プロパティーは、どれを選択するかにかかわらず、すべてデフォルトで *True* に設定されています。これらのプロパティーについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。新規インストールではこのチェック・ボックスはデフォルトで選択されています。

   注: HTTPS の場合は、**「Websphere サーバーのアドレス」**フィールドで完全修飾ドメイン名を使用する必要があります。

   「セキュア登録トークンを使用してターゲットを登録する」

   セキュア・ターゲット登録機能を有効にするにはこのオプションを選択します。この機能により、無許可のターゲットは Remote Control サーバーに登録できなくなります。**「デフォルトでターゲットの URL に HTTPS を使用」**オプションも選択していることを確認してください。セキュア登録について詳しくは、セキュア・ターゲット登録の有効化を参照してください。

WebSphere® サーバーのアドレス。

Remote Control サーバーの完全修飾名。例えば、`trcserver.example.com` です。

注: 完全修飾名を入力してください。この名前を使用して、ターゲットが初めてサーバーに接続するときにそのターゲットに渡される URL を `trc.properties` ファイル内に作成します。完全修飾名が誤っていると、 ターゲットが次にサーバーに接続するときに正常に接続できない可能性があります。

「URL の Web パス」

サーバー URL の Web パスを指定します (`http://trcserver.example.com/webpath`)。例えば、`trc` です。 `http://trcserver.example.com/trc`

「HTTP ポート」

サーバーのポートを指定します。デフォルトは 80 です。

「HTTPS ポート」

SSL を使用する場合は、ポートを指定します。デフォルトは 443 です。

「管理者の電子メール」

管理者の電子メール・アドレスを指定します。例えば、 `admin@company.com`

注: Remote Control サーバー内で電子メール機能を使用するには、メール・サーバーがインストールされている必要があります。電子メールの有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「FIPS を有効にする」

サーバーで FIPS 準拠性を使用可能にするには、これを選択します。FIPS 準拠の有効化について詳しくは、*BigFix® Remote Control* インストール・ガイドを参照してください。

NIST SP800-131A 準拠性を使用可能にする (FIPS を使用可能にする) (Enable NIST SP800-131A compliance (Enables FIPS))

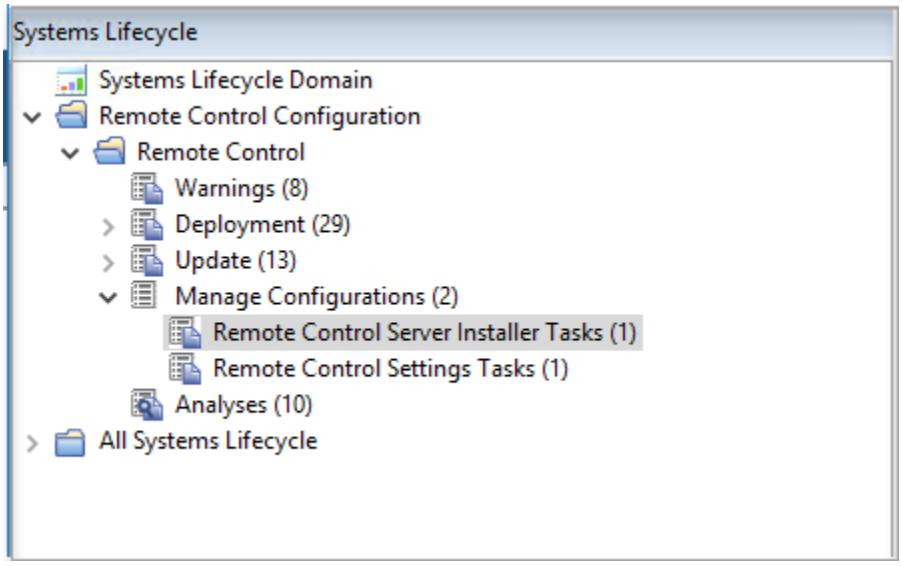
すべての暗号機能について NIST SP800-131A 準拠のアルゴリズムと鍵強度を使用する場合は、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「一部の Web パラメーターを調整する」

追加のポート値を設定するには、このオプションを選択します。

5. 以下のステップを実行して、構成を保存します。
   a. **「サーバー・インストール・タスクの作成 (Create Server Installation Task)」**をクリックします。
   b. タスクに関連する情報を入力して、**「OK」**をクリックします。

これで、作成したタスクは**「Remote Control サーバー・インストーラー・タスク」**サブノードのリスト・パネルに表示されます。



DB2® サーバー構成の作成

DB2® データベースを使用するサーバー・インストール構成を作成できます。Remote Control サーバーをインストールする前に、ローカル側またはリモート側でデータベースをインストールして、データベース・インスタンスを作成する必要があります。

タスクを作成する前に、必ずデータベースをセットアップしてください。データベースのセットアップについて詳しくは、「*BigFix® Remote Control* インストール・ガイド」、およびデータベースのセットアップについて説明している章を参照してください。

DB2® サーバー構成タスクを作成するには、以下のステップを実行します。

1. 関連するオペレーティング・システムを選択します。
2. Remote Control サーバーがインストールされるインストール・ディレクトリーを入力するか、提示されているデフォルトを受け入れます。
3. 関連する DB2® バージョンを選択し、関連するデータベース・パラメーターを入力します。

「データベース・サーバーのアドレス」

データベース・サーバーの IP アドレスまたはホスト名。

注: DB2® がローカルにインストールされている場合、127.0.0.1を使用できます。DB2® がリモート・システムにインストールされている場合は、リモート・システムの IP アドレスを入力します。

「データベース接続に使用するポート番号」

DB2® がインストールされているポート。

注:

a. Windows™® システムの場合、デフォルト・ポートは 50000 です。Linux™ システムの場合、デフォルト・ポートは 50001 です。
b. リモート DB2® インストールは、タイプ 4 接続に制限されます。ローカル・インストールではタイプ 2 または 4 を使用できます。タイプ 2 接続ではポート値を 0 に設定します。

「使用するデータベース名」

Remote Control サーバーで使用されるデータベースの名前を指定するか、提示されているデフォルトを受け入れます。

「データベース管理者のユーザー ID」

データベースにログオンするときに使用する管理者ユーザー ID を指定します。このユーザー ID は、データベースへの管理アクセス権限を持っている必要があります。

「データベース管理者のパスワード」

データベースに接続するための管理者パスワードを指定します。

「JDBC ドライバーへのパス」

DB2® JAR ファイル、`db2jcc.jar`、 および `db2jcc_license.jar` へのパスを指定します。

「db2profile スクリプトへのパス」

DB2® インスタンスの db2profile へのパスを指定します。例えば、 `/home/db2inst1/sqllib/db2profile`

注: このフィールドは、Linux™ オペレーティング・システムにインストールし、データベースの作成を選択した場合のみ使用可能です。

「DB2® ライブラリーへのパス」

DB2® ライブラリーへのパスを指定します。例えば、 `/home/db2inst1/sqllib/lib32`

注: このフィールドは、Linux™ オペレーティング・システムにインストールし、データベースの作成を選択した場合のみ使用可能です。

「ローカルの場合、データベースを作成」

DB2® がローカル (127.0.0.1) にインストールされている場合は、インストール中にブランク・データベースを作成することを選択できます。既存のローカル・データベースを除去して新規データベースを作成することも選択できます。

注: リモート・データベースを使用する場合は、データベースの作成とデータベースの除去のいずれも選択しないでください。

「ローカルの場合、既存のデータベースをドロップ」

DB2® がローカル (127.0.0.1) にインストールされている場合は、データベースをドロップして新規データベースを作成することを選択できます。

注: リモート・データベースを使用する場合、データベースをドロップしないでください。

「新規データベースの場所 (ドライブ名)/(パス名)」

データベースをインストールできる場所のパスを指定します。インストール済み環境がローカルであり、データベースの作成を選択した場合は、指定された管理ユーザーが適切な権限を持っていなければなりません。Windows™ システムでは db2admin ユーザーを使用します。Linux™ システムでは、ユーザーがグループ db2grp1 のメンバーであることが必要です。

注:

Linux™ システム

管理ユーザー ID が読み取り権限および書き込み権限を持つディレクトリーを指定します。

Windows™ システム

ドライブ名を指定します。

4. サーバー・インストール・パラメーター値を入力します。

「デフォルトでターゲットの URL に HTTPS を使用」

ターゲットが HTTPS サーバー URL を使用してサーバーと通信する場合、このオプションを選択します。`trc.properties` ファイル内の **enforce.secure.endpoint.callhome** プロパティーと **enforce.secure.endpoint.upload** プロパティーも *true* に設定されています。これを選択しない場合は、HTTP URL が使用されます。 HTTPS によるログオンおよび Web ポータルへのアクセスを有効にする **enforce.secure.web.access**、 **enforce.secure.weblogon**、および **enforce.secure.alllogon** プロパティーは、どれを選択するかにかかわらず、すべてデフォルトで *True* に設定されています。これらのプロパティーについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。新規インストールではこのチェック・ボックスはデフォルトで選択されています。

注: HTTPS の場合は、**「Websphere サーバーのアドレス」**フィールドで完全修飾ドメイン名を使用する必要があります。

「セキュア登録トークンを使用してターゲットを登録する」

セキュア・ターゲット登録機能を有効にするにはこのオプションを選択します。この機能により、無許可のターゲットは Remote Control サーバーに登録できなくなります。**「デフォルトで**

ターゲットの URL に HTTPS を使用」オプションも選択していることを確認してください。セキュア登録について詳しくは、セキュア・ターゲット登録の有効化を参照してください。

WebSphere® サーバーのアドレス。

Remote Control サーバーの完全修飾名。例えば、`trcserver.example.com` です。

注: 完全修飾名を入力してください。この名前を使用して、ターゲットが初めてサーバーに接続するときにそのターゲットに渡される URL を `trc.properties` ファイル内に作成します。完全修飾名が誤っていると、 ターゲットが次にサーバーに接続するときに正常に接続できない可能性があります。

「URL の Web パス」

サーバー URL の Web パスを指定します (`http://trcserver.example.com/webpath`)。例えば、`trc` です。 `http://trcserver.example.com/trc`

「HTTP ポート」

サーバーのポートを指定します。デフォルトは 80 です。

「HTTPS ポート」

SSL を使用する場合は、ポートを指定します。デフォルトは 443 です。

「管理者の電子メール」

管理者の電子メール・アドレスを指定します。例えば、 `admin@company.com`

注: Remote Control サーバー内で電子メール機能を使用するには、メール・サーバーがインストールされている必要があります。電子メールの有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「FIPS を有効にする」

サーバーで FIPS 準拠性を使用可能にするには、これを選択します。FIPS 準拠の有効化について詳しくは、*BigFix® Remote Control* インストール・ガイドを参照してください。

NIST SP800-131A 準拠性を使用可能にする (FIPS を使用可能にする) (Enable NIST SP800-131A compliance (Enables FIPS))

すべての暗号機能について NIST SP800-131A 準拠のアルゴリズムと鍵強度を使用する場合は、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「一部の Web パラメーターを調整する」

追加のポート値を設定するには、このオプションを選択します。

5. 以下のステップを実行して、構成を保存します。
   a. **「サーバー・インストール・タスクの作成 (Create Server Installation Task)」**をクリックします。
   b. タスクに関連する情報を入力して、**「OK」**をクリックします。

MS SQL サーバー構成の作成

MS SQL データベースを使用するサーバー・インストール構成を作成できます。Remote Control サーバーをインストールする前に、ローカル側またはリモート側でデータベースをインストールして、データベース・インスタンスを作成する必要があります。

MS SQL サーバー構成タスクを作成するには、以下のステップを実行します。

1. 関連するオペレーティング・システムを選択します。
2. Remote Control サーバーがインストールされるインストール・ディレクトリーを入力するか、提示されているデフォルトを受け入れます。
3. 関連する MS SQL バージョンを選択し、関連するデータベース・パラメーターを入力します。

「データベース・サーバーのアドレス」

データベース・サーバーの IP アドレスまたはホスト名。

注: MS SQL が Windows™ システム上にローカルにインストールされている場合のみ、127.0.0.1 を使用できます。

「データベース接続に使用するポート番号」

MS SQL がインストールされているポート。

「使用するデータベース名」

Remote Control サーバーで使用されるデータベースの名前を指定するか、提示されているデフォルトを受け入れます。

「データベース管理者のユーザー ID」

データベースにログオンするときに使用する管理者ユーザー ID を指定します。このユーザー ID は、データベースへの管理アクセス権限を持っている必要があります。

「データベース管理者のパスワード」

データベースに接続するための管理者パスワードを指定します。

「JDBC ドライバーへのパス」

MS JDBC Java ファイルへのパスを指定します。使用している MS SQL データベースのバージョンに応じて、`mssql-jdbc-X.X.X.jre8.jar` ファイルを使用する必要があります。

「ローカルの場合、データベースを作成」

MS SQL がローカル環境にインストールされている場合は、インストール中にブランク・データベースを作成することを選択できます。

「ローカルの場合、既存のデータベースをドロップ」

MS SQL がローカルにインストールされている場合は、データベースをドロップして新規データベースを作成することを選択できます。リモート・データベースを使用する場合、データベースのドロップを選択しないでください。

「新規データベースの場所 (ディレクトリーが存在している必要があります)」

データベースのインストール・パスを指定します。インストール済み環境がローカルであり、データベースの作成を選択した場合は、管理ユーザーがこの処理を行うための適切な権限を持っていなければなりません。

Linux™ システム。

管理ユーザー ID が読み取り権限および書き込み権限を持つディレクトリーを指定します。

Windows™ システム。

既存のディレクトリーを指定します。

4. サーバー・インストール・パラメーター値を入力します。

「デフォルトでターゲットの URL に HTTPS を使用」

ターゲットが HTTPS サーバー URL を使用してサーバーと通信する場合、このオプションを選択します。`trc.properties` ファイル内の **enforce.secure.endpoint.callhome** プロパティーと **enforce.secure.endpoint.upload** プロパティーも *true* に設定されています。これを選択しない場合は、HTTP URL が使用されます。 HTTPS によるログオンおよび Web ポータルへのアクセスを有効にする **enforce.secure.web.access**、 **enforce.secure.weblogon**、および **enforce.secure.alllogon** プロパティーは、どれを選択するかにかかわらず、すべてデフォルトで *True* に設定されています。これらのプロパティーについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。新規インストールではこのチェック・ボックスはデフォルトで選択されています。

注: HTTPS の場合は、**「Websphere サーバーのアドレス」**フィールドで完全修飾ドメイン名を使用する必要があります。

「セキュア登録トークンを使用してターゲットを登録する」

セキュア・ターゲット登録機能を有効にするにはこのオプションを選択します。この機能により、無許可のターゲットは Remote Control サーバーに登録できなくなります。**「デフォルトでターゲットの URL に HTTPS を使用」**オプションも選択していることを確認してください。セキュア登録について詳しくは、セキュア・ターゲット登録の有効化を参照してください。

WebSphere® サーバーのアドレス。

Remote Control サーバーの完全修飾名。例えば、`trcserver.example.com` です。

注: 完全修飾名を入力してください。この名前を使用して、ターゲットが初めてサーバーに接続するときにそのターゲットに渡される URL を `trc.properties` ファイル内に作成します。完全修飾名が誤っていると、 ターゲットが次にサーバーに接続するときに正常に接続できない可能性があります。

「URL の Web パス」

サーバー URL の Web パスを指定します (`http://trcserver.example.com/webpath`)。例えば、`trc` です。 `http://trcserver.example.com/trc`

「HTTP ポート」

サーバーのポートを指定します。デフォルトは 80 です。

「HTTPS ポート」

SSL を使用する場合は、ポートを指定します。デフォルトは 443 です。

「管理者の電子メール」

管理者の電子メール・アドレスを指定します。例えば、 `admin@company.com`

注: Remote Control サーバー内で電子メール機能を使用するには、メール・サーバーがインストールされている必要があります。電子メールの有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「FIPS を有効にする」

サーバーで FIPS 準拠性を使用可能にするには、これを選択します。FIPS 準拠の有効化について詳しくは、*BigFix® Remote Control* インストール・ガイドを参照してください。

NIST SP800-131A 準拠性を使用可能にする (FIPS を使用可能にする) (Enable NIST SP800-131A compliance (Enables FIPS))

すべての暗号機能について NIST SP800-131A 準拠のアルゴリズムと鍵強度を使用する場合は、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「一部の Web パラメーターを調整する」

追加のポート値を設定するには、このオプションを選択します。

5. 以下のステップを実行して、構成を保存します。
   a. **「サーバー・インストール・タスクの作成 (Create Server Installation Task)」**をクリックします。
   b. タスクに関連する情報を入力して、**「OK」**をクリックします。

Oracle サーバー構成の作成

Oracle データベースを使用するサーバー・インストール構成を作成できます。Remote Control サーバーをインストールする前に、ローカル側またはリモート側でデータベースをインストールして、データベース・インスタンスを作成する必要があります。

Oracle サーバー構成タスクを作成するには、以下のステップを実行します。

1. 関連するオペレーティング・システムを選択します。
2. Remote Control サーバーがインストールされるインストール・ディレクトリーを入力するか、提示されているデフォルトを受け入れます。
3. 関連する Oracle バージョンを選択し、関連するデータベース・パラメーターを入力します。

「データベース・サーバーのアドレス」

ご使用のデータベース・サーバーの IP アドレスまたはホスト名。ローカルに Oracle がインストールされている場合は、127.0.0.1 を使用できます。Oracle がリモート・システムにインストールされている場合は、リモート・システムの IP アドレスを入力します。

「データベース接続に使用するポート番号」

Oracle がインストールされているポート。

「使用するデータベース名」

データベースの名前を指定します。この名前は、`tnsnames.ora` 内の名前ではなく、サーバーでの SID 名です。例えば、`TRCDB` です。

「データベース管理者のユーザー ID」

データベースにログオンするときに使用する管理者ユーザー ID を指定します。このユーザー ID は、データベースへの管理アクセス権限を持っている必要があります。

注: Oracle のインストール済み環境では、 **asset** というユーザーが存在していなければなりません。このユーザー ID をここで使用することも、既存または新規のユーザーを使用することもできます。

「データベース管理者のパスワード」

データベースに接続するための管理者パスワードを指定します。

「JDBC ドライバーへのパス」

oracle Java™ JDBC ライブラリーへのパスを指定します。ロケーションは、Oracle サーバーのインストール済み環境から取得するか、Oracle Web サイトからダウンロードできます。例えば、 `c:\oracle\ora92\jdbc\lib\ojdbc14.jar`

4. サーバー・インストール・パラメーター値を入力します。

「デフォルトでターゲットの URL に HTTPS を使用」

ターゲットが HTTPS サーバー URL を使用してサーバーと通信する場合、このオプションを選択します。`trc.properties` ファイル内の **enforce.secure.endpoint.callhome** プロパティーと **enforce.secure.endpoint.upload** プロパティーも *true* に設定されています。これを選択しない場合は、HTTP URL が使用されます。 HTTPS によるログオンおよび Web ポータルへのアクセスを有効にする **enforce.secure.web.access**、 **enforce.secure.weblogon**、および **enforce.secure.alllogon** プロパティーは、どれを選択するかにかかわらず、すべてデフォルトで *True* に設定されています。これらのプロパティーについて詳しくは、 「*BigFix® Remote Control* 管理者ガイド」を参照してください。新規インストールではこのチェック・ボックスはデフォルトで選択されています。

注: HTTPS の場合は、 **「Websphere サーバーのアドレス」** フィールドで完全修飾ドメイン名を使用する必要があります。

「セキュア登録トークンを使用してターゲットを登録する」

セキュア・ターゲット登録機能を有効にするにはこのオプションを選択します。この機能により、無許可のターゲットは Remote Control サーバーに登録できなくなります。**「デフォルトでターゲットの URL に HTTPS を使用」**オプションも選択していることを確認してください。セキュア登録について詳しくは、セキュア・ターゲット登録の有効化を参照してください。

WebSphere® サーバーのアドレス。

Remote Control サーバーの完全修飾名。例えば、`trcserver.example.com` です。

注: 完全修飾名を入力してください。この名前を使用して、ターゲットが初めてサーバーに接続するときにそのターゲットに渡される URL を `trc.properties` ファイル内に作成します。完全修飾名が誤っていると、 ターゲットが次にサーバーに接続するときに正常に接続できない可能性があります。

「URL の Web パス」

サーバー URL の Web パスを指定します (`http://trcserver.example.com/webpath`)。例えば、`trc` です。 `http://trcserver.example.com/trc`

「HTTP ポート」

サーバーのポートを指定します。デフォルトは 80 です。

「HTTPS ポート」

SSL を使用する場合は、ポートを指定します。デフォルトは 443 です。

「管理者の電子メール」

管理者の電子メール・アドレスを指定します。例えば、 `admin@company.com`

注: Remote Control サーバー内で電子メール機能を使用するには、メール・サーバーがインストールされている必要があります。電子メールの有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「FIPS を有効にする」

サーバーで FIPS 準拠性を使用可能にするには、これを選択します。FIPS 準拠の有効化について詳しくは、*BigFix® Remote Control* インストール・ガイドを参照してください。

NIST SP800-131A 準拠性を使用可能にする (FIPS を使用可能にする) (Enable NIST SP800-131A compliance (Enables FIPS))

すべての暗号機能について NIST SP800-131A 準拠のアルゴリズムと鍵強度を使用する場合は、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

「一部の Web パラメーターを調整する」

追加のポート値を設定するには、このオプションを選択します。

5. 以下のステップを実行して、構成を保存します。
   a. **「サーバー・インストール・タスクの作成 (Create Server Installation Task)」**をクリックします。
   b. タスクに関連する情報を入力して、**「OK」**をクリックします。

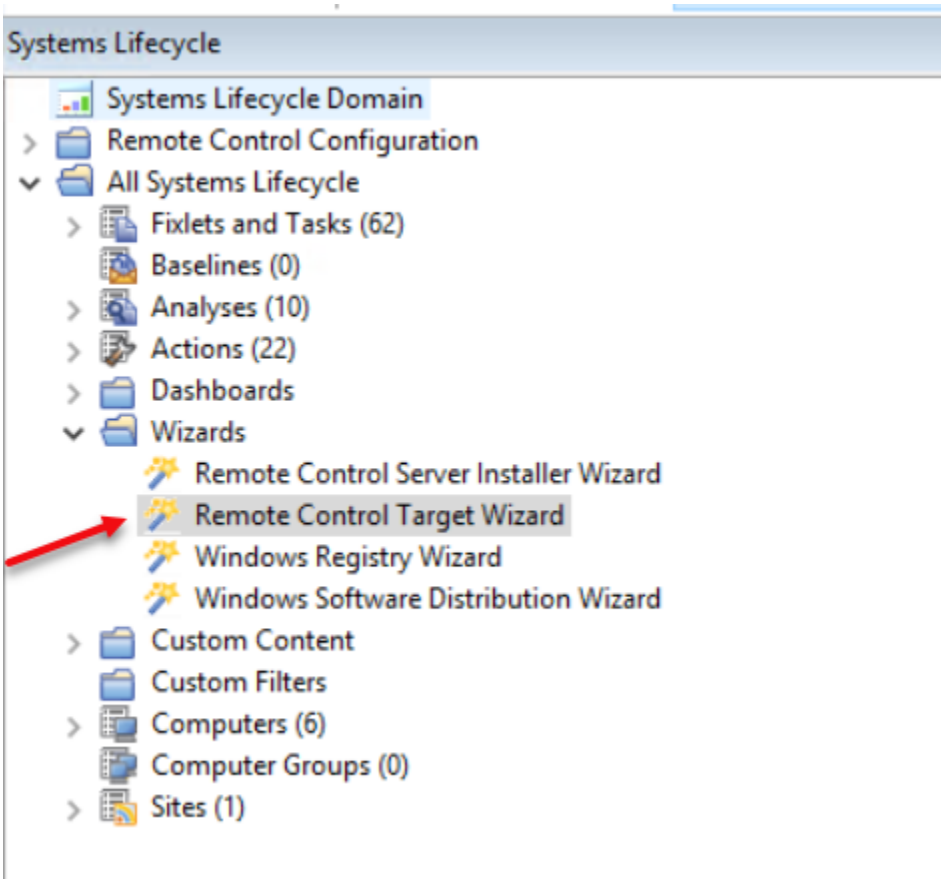
Remote Control ターゲット構成タスクの作成

Remote Control ターゲット・ウィザードを使用して、一連のターゲット構成パラメーターを作成します。

Remote Control ターゲット・ソフトウェアが既にインストールされているすべてのターゲット、または選択したターゲットに対して、パラメーターを適用するタスクを実行します。この構成により、ターゲットが参加できるセッションのタイプが決定され、リモート・コントロール・セッション中にコントローラー・ユーザーがアクションを実行できます。オプションについて詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。構成タスクを作成するには、以下のステップを実行します。

注: ここで設定された構成値は、ターゲットに対して P2P セッションが要求された場合に限り有効になります。リモート・コントロール・セッションが Remote Control サーバーから開始された場合、セッション・ポリシーはサーバーからターゲットに渡されます。

Remote Control ナビゲーション・ツリーで、**「設定の管理」 > 「Remote Control ターゲット・ウィザード」**を選択します。

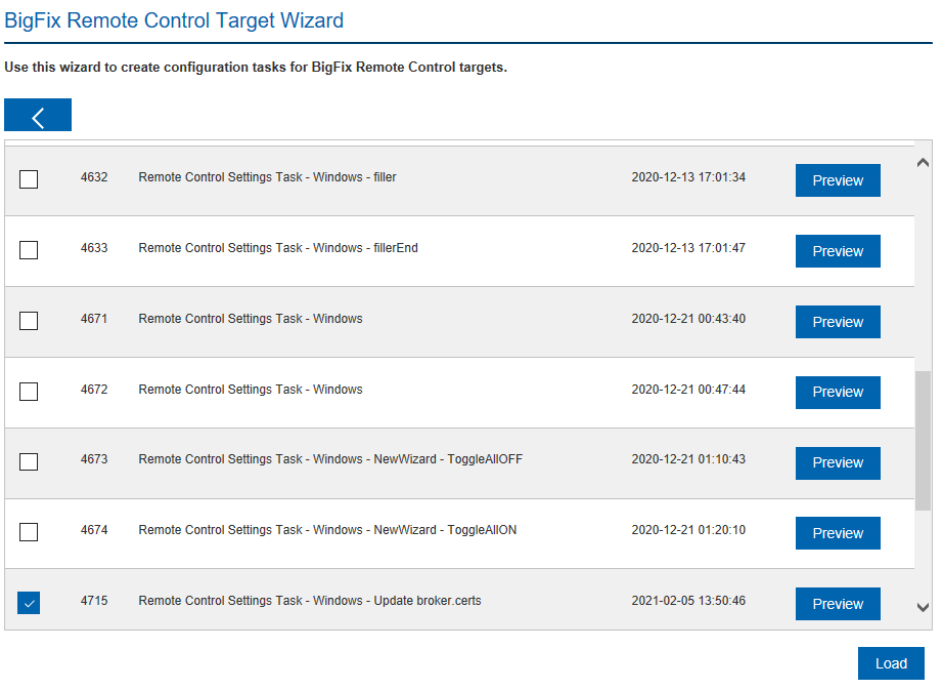


1. 関連するオペレーティング・システムを選択します。
2. 構成値を設定します。

「既存のタスクからの設定の読み込み」

この機能を使用して、以前に作成された構成設定をロードします。

a. **「既存のタスクからの設定の読み込み」**をクリックします。
b. **「ウィザードの Fixlet」**パネルで、タスクを選択します。



「Fixlet を使用してウィザードを読み込み」をクリックします。構成値がウィザードにロードされます。

「デフォルト値にリセット」

この機能を使用して、すべての選択をクリアし、ウィザード内の値をデフォルト構成値に戻します。

「構成値の選択 (Selecting configuration values)」

デフォルト構成値を使用してウィザードがロードされます。関連オプションを選択またはクリアすることにより、これらの構成値をユーザー独自の要件に合うように変更できます。

注: 選択したオペレーティング・システムに応じて、次のプロパティーの全部または一部が表示されます。

表 1. インストール・オプションの説明

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
サーバー URL	ServerURL	ブランク	ターゲットをサーバーに登録し、サーバーから開始されるリモート・コントロール・セッションに参加させるには、次の形式で Remote Control サーバーの URL を指定します。`http://servername/trc` (*servername* は、Remote Control サーバーの完全修飾名) となります。

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			例えば、`http://trcserver.example.com/trc` です。 **注:** ◦ サーバー URL を指定する場合に、ターゲットをサーバーから開始されたリモート・コントロール・セッションのみに参加させるには、**「p2p モードの許可」**で**「いいえ」**を選択します。 ◦ *Remote Control* サーバーが */trc* で終わっていないカスタム *URL* (例: *https://my.rcserver/trccustom*) を使用してインストールされている場合は、フィールドが正しく検証されるように、ServerURL の末尾に */trc* を付けて指定する必要があります (例: *https://my.rcserver/trc*)。その後、Fixlet が生成されたら、その *URL* を *ActionScript* で手動で編集する必要があります。例えば、"*ServerURL"="https://my.rcserver/trc"* という行は、"ServerURL"="*https://my.rcserver/trccustom"* という行に置き換えます。
プロキシー URL	ProxyURL	ブランク	プロキシー・サーバーのホスト名または IP アドレス (使用している場合)。
ブローカー・リスト	BrokerList	ブランク	ターゲットの接続先とする、ブローカーおよびそのポートのホスト名または IP アドレスのリスト。**hostname1:port,hostname2:port,hostname3:port** の形式で入力します。
ブローカー接続のトラステッド証明書 (Trusted certificates for Broker connections)		n/a	ブローカー証明書の検証に使用されるトラストストアを構成するには、このオプションを選択します。証明書を追加するには、以下のステップを実行します。 a. 証明書ファイルをテキスト・エディターで開きます。 b. 証明書を選択してクリップボードにコピーします。

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			注: BEGIN CERTIFICATE および END CERTIFICATE の行を含むすべてを選択する必要があります。 c. **「保存」**をクリックします。
ターゲットをグループに登録	GroupLabel	ブランク	構成の適用時にターゲットがメンバーになるターゲット・グループ名を入力します。このターゲット・グループは、Remote Control データベースに存在していなければなりません。 **注: GroupLabel** プロパティーを使用できるのは、ターゲットがまだサーバーに登録されていない場合のみです。ターゲットが既に登録されている場合は、ターゲット・グループに割り当てられません。**GroupLabel** プロパティー値を適用するには、サーバー上の `trc.properties` ファイルの **allow.target.group.override** プロパティーを true に設定する必要があります。
Remote Control ポート	PortToListen	888	ターゲットが listen する TCP ポートを指定します。
ピアツーピア・モードを許可します	AllowP2P	なし	P2P モードを有効にするために使用されます。 **なし** コントローラーとこのターゲットの間に P2P セッションを確立できません。**ServerURL** が指定されている場合、ターゲットは、サーバーから開始されたリモート・コントロール・セッションにのみ参加できます。 **サーバーと通信不能な場合のみ** Remote Control サーバーがダウンしているか、通信不能である場合のみ、コントローラー・ユーザーとこのターゲットの間に P2P セッションを確立できます。 **常時**

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			コントローラー・ユーザーとこのターゲットの間に P2P セッションを確立できます。 **注:** このオプションが選択され、サーバー URL が指定された場合、ターゲットは、P2P セッションと、サーバーから開始されたセッションの両方に参加できます。
FIPS 準拠	FIPSCompliance	未選択	このオプションを選択すると、すべての暗号化機能について、FIPS 準拠の暗号化サービス・プロバイダーの使用が有効になります。FIPS 準拠の有効化について詳しくは、*BigFix® Remote Control* インストール・ガイドを参照してください。 **注:** ターゲットで FIPS 準拠を有効にする場合は、インストールしたコントローラー・コンポーネントでも FIPS 準拠を有効にしてください。FIPS 準拠モードでは、IBM® Java™ Run-time Environment (JRE) のみがサポートされます。JRE はコントローラー・ソフトウェアのインストール時にインストールされます。コントローラーで FIPS 準拠を有効にするには、以下のステップを実行します。 a. コントローラーがインストールされているシステムで、`trc_controller.cfg` ファイルを編集します。 **Windows® システム** *`[controller installation dir]`*`\trc_controller.cfg` ここで、*[controller installation dir]* はコントローラーがインストールされているディレクトリーです。 **Linux® システム**

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			`opt/bigfix/trc/controller/trc_controller.cfg` b. **fips.compliance** プロパティーを trueに設定し、ファイルを保存します。
NIST SP800-131A 準拠性を使用可能にする (FIPS を使用可能にする) (Enable NIST SP800-131A compliance (Enables FIPS))	SP800131ACompliance	未選択	すべての暗号機能について NIST SP800-131A 準拠のアルゴリズムと鍵強度を使用する場合は、このオプションを選択します。NIST SP800-131A 準拠の有効化について詳しくは、「*BigFix® Remote Control* インストール・ガイド」を参照してください。 **注:** ターゲットで NIST SP800-131A 準拠を有効にする場合は、インストールされているコントローラー・コンポーネントでも NIST SP800-131A 準拠を有効にしてください。NIST SP800-131A 準拠モードでは、IBM®Java™ Run-time Environment (JRE) のみがサポートされます。JRE はコントローラー・ソフトウェアのインストール時にインストールされます。コントローラーで NIST SP800-131A 準拠を有効にするには、以下のステップを実行します。 a. コントローラーがインストールされているシステムで、`trc_controller.cfg` ファイルを編集します。 **Windows® システム** `[controller installation dir]\trc_controller.cfg` ここで、*[controller installation dir]* はコントローラーがインストールされているディレクトリーです。 **Linux® システム**

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			opt/bigfix/ trc/controller/ trc_controller.cfg b. **sp800131A.compliance** プロパティーを true に設定し、ファイルを保存します。
アクセシビリティー	アクセシビリティー	未選択	ユーザー補助 UI を有効にするには、このオプションを選択します。オペレーティング・システムとして **Windows** が選択されている場合に使用できます。
ログ・レベル	LogLevel	2	ログ・レベルによって、エントリーのタイプと、ログ・ファイルに追加される情報量が決定されます。デフォルト値は 2 です。 0 - ロギングが最小レベルに設定されます。 1 - ロギングが **ERROR** レベルに設定されます。 2 - ロギングが **INFO** レベルに設定されます。 4 - ロギングが **DEBUG** レベルに設定されます。 **注:** ログ・レベル 4 は、HCL サポートからの要請があった場合にのみ使用してください。
ログのロールオーバー	LogRollover	毎日	新しいログ・ファイルが開始されるまでの期間を制御します。この期間は LogRotation 期間より短くなければならないため、すべての組み合わせが有効とは限りません。LogRollover を無効にすることはできません。デフォルト値は Daily です。 **毎時** 毎正時に新しいログ・ファイルを開始します。ログが頻繁に書き込まれる場合、またはログ・レベル 2 より高いレベルを使用する場合にお勧めします。 **毎日** 新しいログ・ファイルを毎日開始します。

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
ログのローテーション	LogRotation	週次	古いログ・ファイルが上書きされるようになるまでの期間を制御します。ログ・ローテーションは無効にすることができます。デフォルト値は Weekly です。 **毎日** 1 日経過したログ・ファイルを上書きします。LogRollover を Hourly に設定した場合は、ログ・ファイル名に 00H から 23H までのサフィックスが追加されます。 **週次** 1 週間経過したログ・ファイルを上書きします。LogRollover を Hourly に設定した場合は、ログ・ファイル名に追加されるサフィックスは曜日と時間を示します。値は Mon-00H から Sun-23H になります。LogRollover を Daily に設定した場合は、ログ・ファイル名に追加されるサフィックスは曜日を示します。値は Mon から Sun になります。 **月次** 1 か月 (01-00H から 31-23H) 経過したログ・ファイルを上書きします。LogRollover を Hourly に設定した場合は、ログ・ファイル名に追加されるサフィックスは月の日付 (数値) と時間を示します。値は 01-00H から 31-23H になります。LogRollover を Daily に設定した場合は、ログ・ファイル名に追加されるサフィックスは月の日付 (数値) を示します。値は 01 から 31 になります。 **無効** LogRotation は無効です。LogRollover を Hourly に設定した場合は、ログ・ファイル名に追加されるサフィックスは現在の日時を示します。値は YYYY-MM-DD-hh になります。LogRollover を Daily に設定した場合は、ログ・ファイル名に追加されるサフィックス

インストール・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			は現在の日付を示します。値は YYYY-MM-DD になります。

表 2. セッション・オプションの説明

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
モニター・モードの許可	AllowMonitor	選択	ターゲットがモニター P2P セッションに参加できるかどうかを決定します。確立できるリモート・コントロール・セッションのさまざまなタイプについて詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。 **選択** ターゲットはモニター P2P セッションに参加できます。コントローラー・ウィンドウのセッション・タイプ・リストで、「モニター」オプションを選択できます。「接続のオープン」ウィンドウにも「モニター」オプションがリストされます。 **未選択** ターゲットはモニター P2P セッションに参加できません。コントローラー・ウィンドウのセッション・タイプ・リストで、「モニター」オプションは選択できません。
ガイダンス・モードの許可	AllowGuidance	選択	ターゲットがガイダンス P2P セッションに参加できるかどうかを決定します。 **選択** ターゲットはガイダンス P2P セッションに参加できます。コントローラー・ウィンドウのセッション・タイプ・リストで、「ガイダンス」オプションを選択できます。「接続のオープン」ウィンドウにも「ガイダンス」オプションがリストされます。 **未選択**

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			ターゲットはガイダンス P2P セッションに参加できません。コントローラー・ウィンドウのセッション・タイプ・リストで、「ガイダンス」オプションは選択できません。
アクティブ・モードの許可	AllowActive	選択	ターゲットがアクティブ P2P セッションに参加できるかどうかを決定します。 **選択** ターゲットはアクティブ P2P セッションに参加できます。コントローラー・ウィンドウのセッション・タイプ・リストで、「アクティブ」オプションを選択できます。「接続のオープン」ウィンドウにも「アクティブ」オプションがリストされます。 **未選択** ターゲットはアクティブ P2P セッションに参加できません。コントローラー・ウィンドウのセッション・タイプ・リストで、「アクティブ」オプションは選択できません。
チャットの無効化	DisableChat	未選択	ターゲットでチャット・セッションを開始し、P2P セッション中にコントローラー・ユーザーとチャットすることができるかどうかを決定します。 **選択** **「チャットのみ」** が「接続のオープン」ウィンドウで接続タイプとして選択された場合、セッションは拒否されます。セッション中、コントローラー・ウィンドウでチャット・アイコンは使用できません。 **未選択** 「接続を開く (Open connection)」ウィンドウから「チャットのみ (Chat Only)」セッションを開始できます。セッション中、コントローラー・ウィンドウでチャット・アイコンが使用できます。
コントローラーへのファイル転	DisableFilePull	未選択	セッション中にターゲットからコントローラーにファイルを転送できるかどうかを決定します。 **選択**

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
送機能の無効化			ファイルをターゲットからコントローラーに転送できます。 **未選択** ファイルをターゲットからコントローラーに転送することはできません。
ターゲットへのファイル転送機能の無効化	DisableFilePush	未選択	セッション中にコントローラーからターゲットにファイルを転送できるかどうかを決定します。 **選択** ファイルをコントローラーからターゲットに転送できます。 **未選択** ファイルをコントローラーからターゲットに転送することはできません。
クリップボード転送の無効化	DisableClipboard	未選択	クリップボード転送メニューを使用できるかどうかを決定します。メニューは、リモート・コントロール・セッション中にコントローラーとターゲットとの間でクリップボードの内容を転送する場合に使用します。 **選択** クリップボード転送メニューはセッション中は使用可能であり、ターゲットとの間でクリップボードの内容を転送できます。 **未選択** セッション中、クリップボード転送メニューは使用できません。
「ローカル記録機能の許可」	AllowRecording	選択	コントローラー・ユーザーは、セッションのローカル記録を作成し、それを制御側のシステムに保存することができます。 **選択** コントローラー・ウィンドウで、記録オプションが使用できます。 **未選択** コントローラー・ウィンドウで、記録オプションは使用できません。

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
コラボレーションの許可	AllowCollaboration	選択	複数のコントローラーがセッションに参加できるようにするには、このプロパティーを使用します。コントローラー・ウィンドウでコラボレーション・アイコンを使用可能にするかどうかを決定します。 **選択** コントローラー・ウィンドウで、コラボレーション・アイコンが使用できます。 **未選択** コントローラー・ウィンドウでコラボレーション・アイコンが使用可能になりません。
ハンドオーバーの許可	AllowHandover	選択	コラボレーション・セッションでは、マスター・コントローラーがセッションの制御を新規コントローラーに引き渡すことができます。コラボレーション・コントロール・パネルで **「ハンドオーバー」** ボタンを使用可能にするかどうかを決定します。 **選択** コラボレーション制御パネルに **「ハンドオーバー」** ボタンが表示されます。 **未選択** コラボレーション制御パネルに **「ハンドオーバー」** ボタンは表示されません。
「セッションの切断要求を許可する (Allows requests to disconnect session)」	AllowForceDisconnect	未選択	ターゲットに接続しようとするときに表示されるメッセージ・ウィンドウで、 **「セッションの切断」** ボタンを使用できるかどうかを決定します。**「セッションの切断」** オプションを使用すると、現行セッションを切断することができます。 **選択** メッセージ・ウィンドウに切断ボタンが表示されます。 **未選択** メッセージ・ウィンドウに切断ボタンが表示されません。
切断猶予時間 (Disconnect grace time)	ForceDisconnectTimeout	45	現行セッションを切断するよう求めるプロンプトに現行コントローラーが応答するのを待つ時間 (秒数)。指定された時間内に応答しない場合は、セッションから自動的に切断されます。このタイマーは、**AllowForceDisconnect** と **CheckUserLogin** が「はい」に設定されている場合のみ有効になります。デフォルト値は45です。

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
「ログオン時に接続」	AutoWinLogon	選択	ユーザーがターゲットにログオンしていない場合に、セッションを開始できるようにするかどうかを決定します。 **選択** ターゲットでセッションが開始されます。 **未選択** セッションは開始されず、以下のメッセージが表示されます。セッションを確認するためにログインしているユーザーが存在しないため、セッションは拒否されました
セッション前に実行するスクリプト	RunPreScript	未選択	リモート・コントロール・セッションの開始前にユーザー定義スクリプトを実行するかどうかを決定します。このスクリプトは、セッションが許可された直後で、かつコントローラー・ユーザーがターゲットにアクセスできるようになる前に実行されます。スクリプト実行の結果およびセッションの続行は,**「開始前/終了後スクリプトの失敗時も続行」** で設定される値によって決まります。 **選択** リモート・コントロール・セッションが要求されると、定義済みスクリプトは、コントローラー・ユーザーがターゲットへのアクセス権限を持つ前に実行されます。 **未選択** セッション前にスクリプトは実行されません。 セッション前スクリプトおよびセッション後スクリプトのセットアップについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。
セッション後に実行するスクリプト	RunPostScript	未選択	リモート・コントロール・セッションの完了後にユーザー定義スクリプトを実行するかどうかを決定します。 **選択** リモート・コントロール・セッションが終了すると、ユーザー定義スクリプトが実行されます。 **未選択** セッション後にスクリプトは実行されません。 セッション前スクリプトおよびセッション後スクリプトのセットアップについて詳しくは、「*BigFix® Remote Control* 管理者ガイド」を参照してください。

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
開始前/終了後スクリプトの失敗時も続行	ProceedOnScriptFail	未選択	前スクリプトまたは後スクリプトの実行が失敗する場合に取るアクション。正の値または 0 の場合は、前スクリプトまたは後スクリプトの実行が成功したとみなされます。負の値の場合や、スクリプトが見つからない場合、あるいは実行が 3 分以内に完了しなかった場合は、失敗とみなされます。 **選択** 前スクリプトまたは後スクリプトの実行が失敗した場合でも、セッションは続行します。 **未選択** 前スクリプトまたは後スクリプトの実行が失敗した場合、セッションは続行されずに終了します。
RDP コンソール・セッション後にコンソールをリセット	WorkaroundW2K3RDP	未選択	リモート・デスクトップ・コンソール・セッションの後、コンソールを自動的にリセットします。リモート・デスクトップ・ユーザーが **/admin** または **/console** のオプションを使用して Windows® Server 2003 システムでのリモート・デスクトップ・セッションを開始する場合、ユーザーがこのリモート・デスクトップ・セッションの前後または最中にこのターゲットとのリモート・コントロール・セッションを開始すると、リモート・コントロールは表示を取り込むことができません。その結果、コントローラーにはグレイ画面が表示されます。この問題は、 Windows®Server 2003オペレーティングシステムの制限です。そのため、このプロパティーには、選択された値に応じて、各リモート・デスクトップ・セッションの終了後か、あるいはリモート・コントロール・セッションの開始前に、Windows® セッションをリセットするという回避策が導入されています。 **0** 回避策が使用不可になります。この値はデフォルト値です。 **1** リモート・コントロール・セッションが開始したときに、セッションを自動的にリセットします。 **注:** Windows® セッションは初期化するのに数分かかるため、コントローラーでは初期化が完了するまでデスクトップ画面がブランクになります。セッションはリセット中であり、数分かかる可能

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			性があることをコントローラー・ユーザーに知らせるメッセージが表示されます。 **2** リモート・デスクトップ・ユーザーがログアウトしたときに、セッションを自動的にリセットします。
アクティブ・セッションのフォロー	FollowActiveSession	未選択	選択すると、コントローラーはターゲット上のアクティブなセッションに接続します。そのセッションがリモート・デスクトップ・セッションであっても、この動作は変わりません。この機能は、Remote Control v9.1.2 IF0002 以降のバージョンで使用でき、次のバージョンの Microsoft™ Windows™ オペレーティング・システムでサポートされています。 ◦ Microsoft™ Windows™ Vista ◦ Microsoft™ Windows™ 7 ◦ Microsoft™ Windows™ 8 ◦ Microsoft™ Windows™ 8.1 ◦ Microsoft™ Windows™ 10 この機能は、Microsoft™ Windows™ のいずれの Server Edition でもサポートされていません。

表 3. ユーザー確認オプションの説明

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
着信接続の確認	ConfirmTakeOver	選択	リモート・コントロール・セッションが要求されたときに、ターゲットに確認ウィンドウを表示するかどうかを決定します。 **選択** ユーザー確認ウィンドウが表示され、ターゲット・ユーザーはセッションを受け入れるか、拒否することができます。 **未選択** ユーザー確認ウィンドウは表示されずに、セッションが確立されます。
モードの変更の確認	ConfirmModeChange	選択	コントローラー・ユーザーがコントローラー・ウィンドウのセッション・モード・リストから別のセッション・モードを選択した場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			選択 セッション・モードの変更が要求されるたびにユーザー確認ウィンドウが表示され、ターゲット・ユーザーは要求を受け入れるか、拒否する必要があります。 **未選択** ユーザー確認ウィンドウは表示されず、セッション・モードは自動的に変更されます。
ファイル転送の確認	ConfirmFileTransfer	選択	コントローラー・ユーザーがターゲットとコントローラーの間でファイルを転送することを選択した場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。 **選択** 確認ウィンドウは以下の 2 とおりの場合に表示されます。ターゲット・ユーザーは、ファイル転送を受け入れるか、拒否する必要があります。 ◦ コントローラー・ユーザーが、コントローラー・ウィンドウの「ファイルの転送」メニューから **「ファイルをプル」** を選択した場合。ターゲット・ユーザーは、要求を受け入れた後、転送するファイルを選択する必要があります。 ◦ コントローラー・ユーザーがターゲット・ウィンドウの**「アクション」**メニューから**「コントローラーへファイルを送信」**を選択した場合。 **未選択** 要求された場合、確認ウィンドウは表示されず、ファイルは自動的にターゲットからコントローラー・システムに転送されます。
システム情報の確認	ConfirmSysInfo	選択	コントローラー・ユーザーがターゲット・システム情報の表示を要求した場合にユーザー確認ウィンドウを表示するかどうかを決定します。 **選択** コントローラー・ユーザーがコントローラー・ウィンドウの**「システム情報」**をクリックすると、ユーザー確認ウィンドウが表示されます。ターゲット・ユーザーは、要求を受け入れるか、拒否する必要があります。ターゲット・ユーザーが「受け入れ」をクリックすると、コントローラー・システムでターゲット・システム情報が別のウィンドウに表示されます。「拒否」をクリックすると、コントローラーにメッセージが表示され、システム情報は表示されません。 **未選択** コントローラー・ユーザーがシステム情報アイコンをクリックすると、ターゲット・システム情報が自動的に表示されます。

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
記録機能の確認	ConfirmRecording	選択	コントローラー・ユーザーがコントローラー・ウィンドウで記録アイコンをクリックした場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。 **選択** コントローラー・ユーザーがコントローラー・ウィンドウの記録アイコンをクリックすると、メッセージ・ウィンドウが表示されます。ターゲット・ユーザーが**「受け入れ」**をクリックした場合は、コントローラー・ユーザーが記録の保存ディレクトリーを選択できます。ターゲット・ユーザーが**「拒否」**をクリックした場合は、記録が拒否されたことを示すメッセージがコントローラーに表示されます。 **注:** ターゲット・ユーザーが記録要求を受け入れた後に、コントローラー・ユーザーがローカル記録を停止して再開した場合、確認ウィンドウは表示されません。 **未選択** コントローラー・ユーザーがコントローラー・ウィンドウの記録アイコンをクリックすると、メッセージ・ウィンドウは表示されません。コントローラー・ユーザーは、記録の保存先ディレクトリーを選択できます。
コラボレーションの確認	ConfirmCollaboration	選択	別のコントローラー・ユーザーがターゲットとのコラボレーション・セッションへの参加を要求した場合に、ユーザー確認ウィンドウを表示するかどうかを決定します。 **選択** コラボレーション・セッションにコントローラー・ユーザーが参加しようとすると、ユーザー確認ウィンドウが表示されます。ターゲット・ユーザーは、この追加コントローラーのセッション参加許可の要求を受け入れるか、拒否する必要があります。ターゲット・ユーザーが「同意する」をクリックした場合、追加コントローラーはコラボレーション・セッションに参加します。「拒否する (refuse)」をクリックした場合は、コントローラー・システムにメッセージが表示され、追加コントローラーはコラボレーション・セッションに参加できません。 **未選択** 追加コントローラーは、セッションのマスター・コントローラーに接続しようとしたときに、自動的にコラボレーション・セッションに参加します。
確認待ち時間	AcceptanceGraceTime	45	セッションの開始またはタイムアウトまでのターゲット・ユーザー応答の待ち時間 (秒数) を設定します。これは、**「着信接続の確認」**と使用します。 ◦ 許容値は 0 から 60 です。0 に設定した場合、ターゲット・ユーザーはセッション要求への応答を求められません。

ユーザー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			注: **「着信接続の確認」**を選択した場合は、**「確認待ち時間」**には必ず 0 より大きい値を設定して、ターゲット・ユーザーが応答するのに十分な時間を与えてください。
確認要求のタイムアウト時も続行	AcceptanceProceed	未選択	ユーザー確認ウィンドウがタイムアウトになる場合に実行されるアクションです。ターゲット・ユーザーは、**「受け入れ猶予時間」**に定義された秒数内に「受け入れ」または「拒否」をクリックしませんでした。 **選択** セッションが確立されます。 **未選択** セッションは確立されません。
ウィンドウの非表示	HideWindows	未選択	**「着信接続の確認」**も選択された場合に、ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスを表示するかどうかを決定します。 **選択** ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスが表示されます。 **未選択** ユーザー確認ウィンドウに**「ウィンドウの非表示」**チェック・ボックスは表示されません。

表 4. セキュリティー・オプションの説明

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
システム・ログオンを使用した認証	CheckUserLogin	選択	**「接続のオープン」**ウィンドウでセッション・タイプが選択されたときにログイン・ウィンドウを表示するかどうかを決定します。 **はい** ログオン・ウィンドウが表示され、コントローラー・ユーザーは有効な Windows™ オペレーティング・システム ID およびパスワードを使用してログオンする必要があります。ログオン資格情報が無効な場合、ターゲットはセッションを拒否します。

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			いいえ ログオン・ウィンドウは表示されずに、P2P セッションが確立されます。

指定ユーザー・グループ	CheckUserGroup	説明を参照	デフォルト値は、次のとおりです。
			Windows® システム
			`BUILTIN\Administrators`
			Linux® システム
			`wheel`
			「指定ユーザー・グループ」に値が設定されている場合、認証に使用するユーザー名は、リストされているグループのうちのいずれかのグループのメンバーでなければなりませんユーザーがメンバーではない場合、セッションは拒否されます。複数のグループを指定する場合は、セミコロンで区切る必要があります。例えば、 `wheel;trcusers`
			注: デフォルトでは、Windows® システムの場合、管理者ユーザーのみにアクセス権限が付与されます。Linux® システムの場合、デフォルトではどのユーザーにもアクセス権限は付与されません。この問題を解決するには、以下のいずれかのステップを実行します。
			a. ユーザーに管理者権限も付与するために、それらのユーザーを Administrators グループ (Windows® システムの場合) または wheel グループ (Linux® システムの場合) にメンバーとして追加します。
			b. 管理者権限を持たないユーザーについて、以下のステップを実行します。
			i. グループを作成するか、既存のグループを使用します。例えば、root として次のコマンドを実行できます。
			`groupadd trcusers`
			.

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			 ii. ユーザーをこのグループに追加します。例えば、root として次のコマンドを実行して、**bsmith** を **trcusers** に追加します。 `usermod -a -G trcusers <bsmith>` iii. このグループを**「指定ユーザー・グループ」**フィールドのリストに追加します。
監査結果のシステム・ログへの記録	AuditToSystem	選択	リモート・コントロール・セッション中に実行されるアクションが、ターゲット上のアプリケーション・イベント・ログに記録されるかどうかを決定します。このファイルは、監査の目的で使用できます。 **選択** セッション中に実行された各アクションに対応するエントリーが、ターゲットのアプリケーション・イベント・ログに記録されます。 **未選択** アプリケーション・イベント・ログにエントリーは記録されません。
チャット・メッセージの保存	AutoSaveChat	未選択	チャット・セッション中に入力されたチャット・テキストを保存できるかどうかを決定します。 **選択** チャット・テキストは html ファイルとして保存されます。このファイルは `chat-`*`username-date`*`.html` です。*username* は、P2P セッション中にコントローラー・マシンにログオンしたユーザーの表示名です。管理対象モードの場合、*username* はサーバー上のコントローラー・ユーザーの表示名です。日付は *YYYYMMDD* 形式で示します。このファイルは、ターゲットの作業ディレクトリーに保

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			存されます。作業ディレクトリーの場所は、ターゲット・プロパティー **WorkingDir** で定義されます。例えば、Windows™ システムではこのファイルは次の場所に保存されます。 `c:\ProgramData\BigFix\Remote Control`. Linux システムではこのファイルは `/var/opt/bigfix/trc/target/` に保存されます。 **未選択** チャット・テキストはファイルに保存されません。
ファイル転送のためのシステム・アクセスを有効にする	EnableFileTransferSystemAccess	未選択	ファイル転送セッションが、システム特権 (Windows) または root 特権 (Linux) を使用して、ターゲット・ファイル・システムのアクセスを許可するかどうかを決定します。このオプションはピアツーピア・セッションにのみ有効です。 **選択** ファイル転送セッションは、ターゲット・ファイル・システムでシステム特権 (Windows) または root 特権 (Linux) を使用します。 **未選択** ファイル転送セッションでは、ターゲット・ファイル・システム上のログオン・ユーザーの権限が使用されます。
接続切断時にターゲットをロック	SessionDisconnect	未選択	リモート・コントロール・セッションが終了したときに、ターゲット・コンピューターを自動的にロックするかどうかを決定します。指定できる値:*lock*。 値を *lock* に設定すると、セッションの終了時に、ターゲット・コンピューターは自動的にロックされます。このプロパティーを空白にするか、別の値に設定すると、セッションの終了時に、ターゲット・コンピューターは自動的にロックされません。

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
プライバシーの保護	AllowPrivacy	選択	リモート・コントロール・セッション中に、コントローラー・ユーザーがターゲットのローカル入力および画面をロックできるかどうかを決定します。コントローラー・ウィンドウに**「プライバシーの有効化」**オプションを表示できるかどうかを決定します。 **選択** **「プライバシーの有効化」**オプションは、コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで選択できます。 **未選択** **「プライバシーの有効化」**オプションは、コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで選択できません。
「入力ロックの許可」	AllowInputLock	選択	このプロパティーは、**「プライバシーの保護」**と組み合わせても、単独で使用しても機能します。**「入力ロックの許可」**を使用すると、リモート・コントロール・セッション中にターゲット・ユーザーのマウスとキーボードをロックできます。 **選択** コントローラー・ウィンドウで**「ターゲット内のアクションを実行」**メニューの**「ターゲットの入力をロック」**メニュー項目が有効になります。**「ターゲットの入力をロック」**を選択すると、リモート・コントロール・セッション中、ターゲット・ユーザーのマウスとキーボードをロックします。ターゲット・ユーザーに対してはターゲット画面が引き続き表示されます。 **未選択** コントローラー・ウィンドウの**「ターゲット内のアクションを実行」**メニューで「ターゲットの入力をロック」メニュー項目は有効になりません。

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			注: セッション中に**「プライバシーの有効化」**オプションを選択すると、リモート・ユーザー入力が自動的にロックされます。入力をロックせずにプライバシーを使用可能にすることはできません。
プライバシーの有効化	EnablePrivacy	未選択	すべてのセッションでローカル入力および画面をロックするかどうかを決定します。これにより、ターゲット・ユーザーは、リモート・コントロール・セッション中にターゲットで入力を含むあらゆる操作ができなくなります。 **選択** セッションが開始されると、プライバシー・ビットマップによってターゲット画面がブランクになるので、ターゲット・ユーザーはセッション中は画面を操作できなくなります。その場合でも、コントローラー・ウィンドウでは、ターゲット・デスクトップがコントローラー・ユーザーに表示されます。 **未選択** セッションが開始されたときにターゲット画面はブランクにならず、ターゲット・ユーザーは画面を操作することができます。
入力ロックの有効化	EnableInputLock	未選択	このプロパティーは、**「プライバシーの有効化」**との組み合わせで機能します。プライバシー・モードが有効な場合は、**「入力ロックの有効化」**を使用して、リモート・コントロール・セッション中、ターゲット・ユーザーがターゲット画面を表示できるようにするかどうかを決定します。 **選択** プライバシー・モードの場合、セッション中、ターゲット画面はターゲット・ユーザーに表示されますが、ユーザーのマウスおよびキーボードの制御はロックされます。 **未選択**

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			ターゲット画面はターゲット・ユーザーに表示されません。セッション中、プライバシー・ビットマップがターゲットに表示されます。また、ターゲット・ユーザーのマウスおよびキーボード入力も無効になります。 **注:「入力ロックの有効化」**を有効にするには、**「プライバシーの有効化」**を選択する必要があります。
DisablePanicKey	DisablePanicKey	未選択	ターゲット・ユーザーが PAUSE/BREAK キーを使用してリモート・コントロール・セッションを自動的に終了できるようにするかどうかを決定します。 **選択** ターゲット・ユーザーは Pause Break キーを使用してリモート・コントロール・セッションを自動終了できません。 **未選択** ターゲット・ユーザーは、PAUSE/BREAK キーを使用してリモート・コントロール・セッションを自動的に終了できます。
画面上のセッション通知の有効化	EnableOSSN	未選択	リモート・コントロール・セッションが進行中であることを示す半透明のオーバーレイをターゲット・コンピューターに表示するかどうかを決定します。このプロパティーは、プライバシーが懸念される場合に使用します。これによりユーザーは、自分のコンピューターを誰かがリモートで表示または制御できる場合には、そのことがはっきりと通知されます。 **選択** ターゲット画面に、**Remote Control** というテキストと、進行中のリモート・コントロール・セッションのタイプを示す、半透明のオーバーレイが表示されます。`For example, Remote Control - Active Mode.` このオーバーレイはキーボードまたはマウスのアク

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			ションを妨害するものではないため、ユーザーは引き続き自分の画面を操作できます。 **未選択** ターゲット・コンピューターにオーバーレイは表示されません。 **注:** このポリシーは、Windows® オペレーティング・システムがインストールされているターゲットでのみサポートされます。
GUI の無効化	DisableGUI	未選択	リモート・コントロール・セッションの開始時およびセッション中にターゲット GUI を表示するかどうかを決定します。 **注:** このオプションは、ターゲットが P2P モードでインストールされ、**管理**ターゲット・プロパティが「いいえ」に設定されている場合にのみ機能します。このオプションは、サーバー URL が指定された時に、Remote Control サーバー・モードを使用してインストールされたターゲットに適用された場合は無視されます。 **選択** ターゲットにターゲット GUI は表示されず、セッションが開始したことはターゲット・ユーザーには分かりません。Remote Control ターゲット・アイコンは、Windows® システム・トレイに表示されません。 **未選択** ターゲット GUI は、セッションが開始するときにターゲットに表示され、リモート・コントロール・セッション中もターゲット・ユーザーに対して使用可能です。

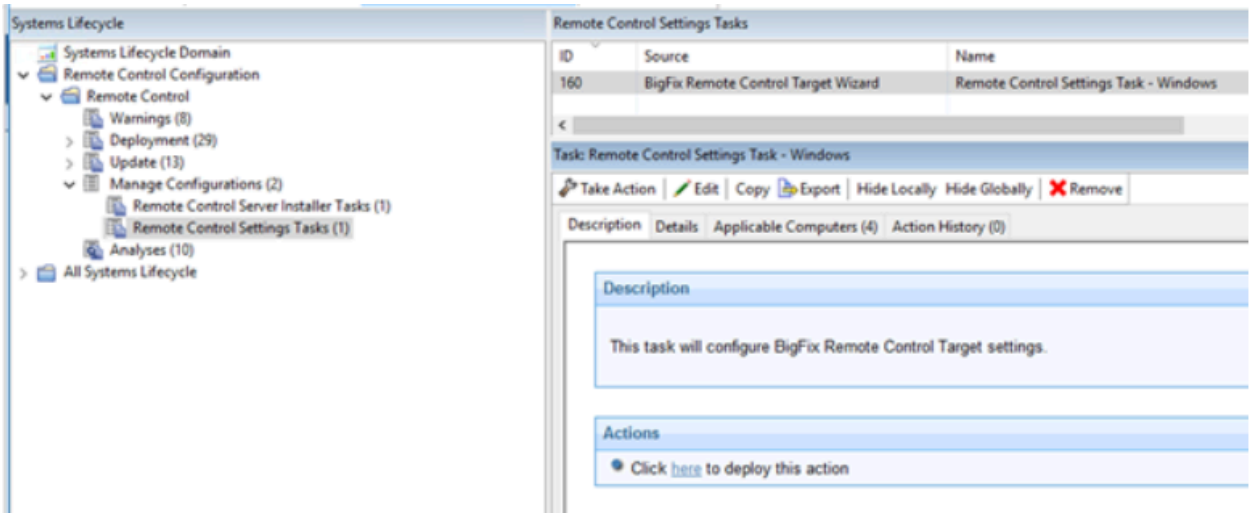
表 5. パフォーマンス・オプションの説明

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
一定時間操作がなかったことによるタイムアウト	IdleTimeout	360	セッション・アクティビティーがない場合に、接続の終了まで待機する秒数。タイマーを無効にして、セッションが自動的に終了しないようにするには、この値を 0 に設定します。最小タイムアウト値は 60 秒です。1 から 59 までの値を設定した場合、セッションは 60 秒間アクティビティーがないとタイムアウトになります。 **注:** 非アクティブ・タイムアウトの値は、「アクティブ」セッション・モードにのみ適用されます。他のセッション・モードの使用時には、セッションは自動的に終了しません。 デフォルト値は 360 です。
高品質カラーを使用可能にする	EnableTrueColor	未選択	セッションの開始時に、コントローラー・ウィンドウでターゲット・デスクトップを高品質カラーで表示するかどうかを決定します。**「カラー品質のロック」**とともに使用します。 **選択** セッション開始時にトゥルー・カラーの 24 ビット・モードでターゲット・デスクトップが表示されます。部分的な画面更新も有効になります。 **未選択** セッション開始時に 8 ビット・カラー・モードでターゲット・デスクトップが表示されます。部分的な画面更新も有効になります。この値はデフォルト値です。
カラー品質のロック	LockColorDepth	未選択	リモート・コントロール・セッション開始時のカラー品質を、セッション中に変更できるかどうかを判別します。**「高品質カラーを使用可能にする」**とともに使用します。 **選択** リモート・コントロール・セッションに対して選択された初期カラー品質はロックされ、セッション中に変更することはできません。コントローラー・ウィンドウで、**「パフォーマンス設定」**アイコンが使用不可になります。コントローラー・ユーザーは、

セキュリティー・オプション	ターゲット・プロパティー	デフォルト値	説明\n
			ネットワークが低速の場合にセッションのパフォーマンスを向上させるために設定を変更することができません。 **未選択** セッション中にカラー品質を変更することができます。コントローラー・ウィンドウで、**「パフォーマンス設定」**アイコンが使用可能になります。
デスクトップの削除	RemoveBackground	未選択	リモート・コントロール・セッション中にデスクトップ背景画像をビューから削除できるかどうかを決定します。 **選択** リモート・コントロール・セッション中、ターゲットのデスクトップ背景画像は表示されません。 **未選択** リモート・コントロール・セッション中、ターゲットのデスクトップ背景画像は表示されます。
スクリーン・セーバーの更新を停止	NoScreenSaver	未選択	スクリーン・セーバーがアクティブであることが検出されたときに、ターゲットによる画面更新の送信を停止します。 **選択** ターゲット・システムでスクリーン・セーバーがアクティブであるときに、ターゲットによる画面更新の送信が停止されます。コントローラー・コンピューターには、シミュレートされたスクリーン・セーバーが表示されるので、コントローラー・ユーザーはスクリーン・セーバーがリモート画面でアクティブになっていることを認識します。コントローラー・ユーザーは、キーを押すかマウスを動かすことによりスクリーン・セーバーを閉じることができます。 **未選択** シミュレートされたスクリーン・セーバーはセッション・ウィンドウに表示されません。ターゲット画面が通常どおり表示され、ターゲットは引き続き画面更新を送信します。

3. **「設定タスクの作成」**をクリックします。タスクに関連する情報を入力して、**「OK」**をクリックします。

これで、作成したタスクは「Remote Control 設定タスク」サブノードのリスト・パネルに表示されます。

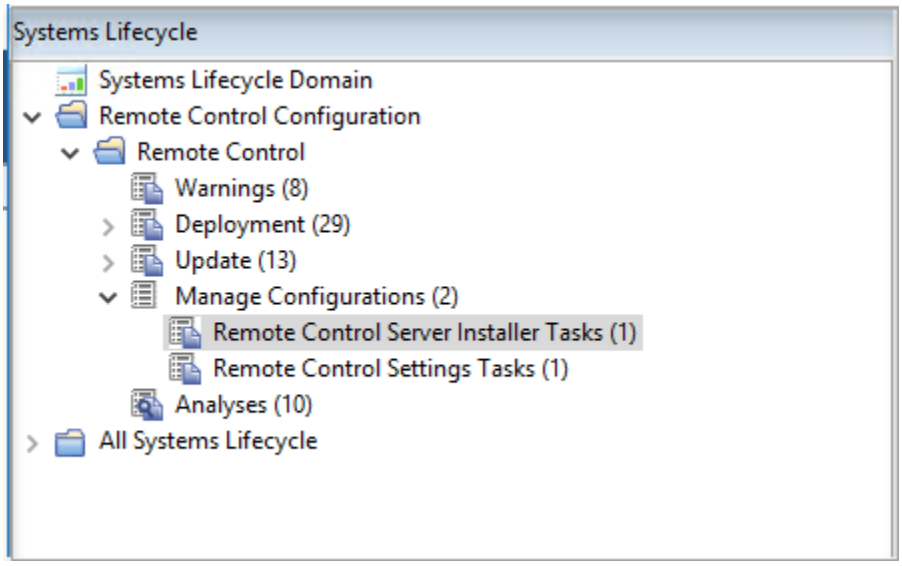


Remote Control タスクの実行

サーバーおよびターゲットの構成タスクを作成したら、これらのタスクを実行して、Remote Control サーバー・ソフトウェアをインストールしたり、既にインストールされているターゲットの構成を変更したりします。

サーバー・インストーラー・タスクの実行

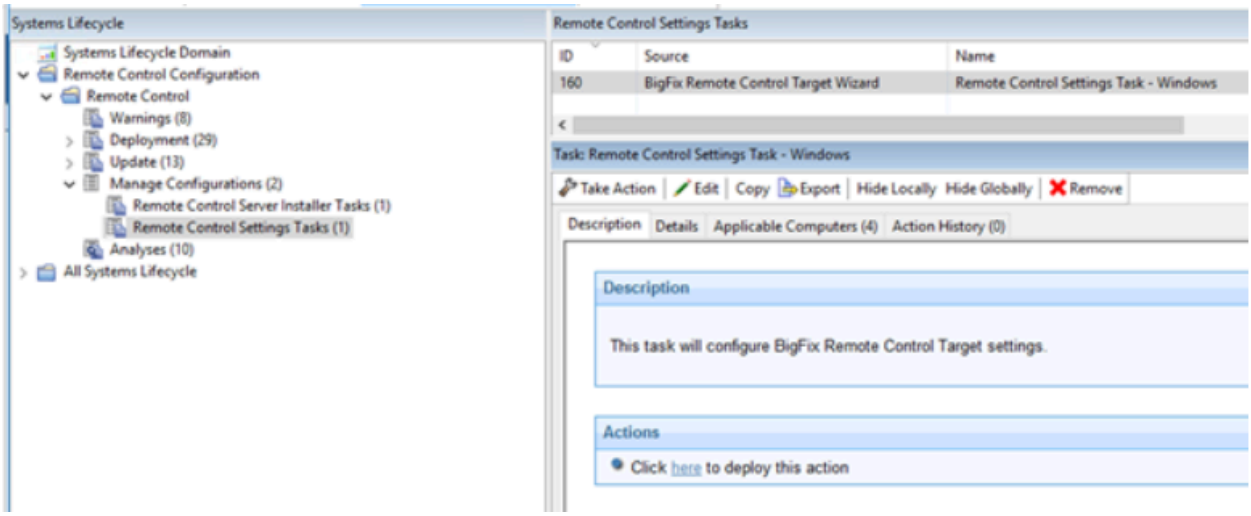
「リモート・コントロール・サーバー・インストーラー・タスク」サブノードを使用して、 **Remote Control サーバー・インストーラー・ウィザード**で作成したタスクを実行します。必要なタスクを選択します。**「説明」**タブを選択して、説明を確認します。DB2、MS SQL、または Oracle のデータベースを使用している場合は、データベース・パスワードを入力する必要があります。「アクション」ボックス内の指示に従ってタスクを開始します。これらのタスクにより、選択したコンピューターに Remote Control サーバー・ソフトウェアがインストールされます。



注: サーバー・インストーラーが失敗した場合、このタスクは失敗し、終了コードが表示されます。

ターゲット構成タスクの実行

「リモート・コントロール設定タスク」サブノードを使用して、**Remote Control ターゲット・ウィザード**で作成した構成タスクを実行します。タスクを選択します。**「タスク」**ウィンドウで、説明を確認し、「アクション」ボックス内の指示に従ってタスクを開始します。



分析

「分析」サブノードには、インストール、ユーザー、および監査の情報を収集する一連の分析が用意されています。このデータは、コントローラー・コンポーネントまたはターゲット・コンポーネントがインストールされている環境内のコンピューター上で発生したリモート・コントロール接続イベントの履歴を提供します。これらの分析は全体でアクティブ化されるため、環境内で分析が関連しているどのコンピューターについても、値が報告されます。

ターゲットのインストールおよびセキュリティー・データの取得

「リモート・コントロールのインストールおよびセキュリティー・オプション」分析は、環境内のターゲットから、インストールおよびセキュリティーのプロパティー値に関する情報を収集するために使用されます。返される値は、ターゲットに関する情報を提供します。例えば、P2P セッションへの参加を許可されているかどうか、Remote Control サーバーから起動されたリモート・コントロール・セッションに参加できるかどうかなどです。プロパティー値の定義については、ステップ 2 を参照してください。

分析がアクティブな場合、**「結果」**タブには、この分析が関連したコンピューターと、インストールおよびセキュリティーのオプションの値が表示されます。**「適用可能なコンピューター」**エントリーを展開し、**取得プロパティー**によってデータをさらにフィルタリングすることができます。この機能は、いろいろな面で役立ちます。例えば、P2P リモート・コントロール・セッションに参加できるターゲットを確認する場合や、さまざまな Remote Control ターゲットにインストールされているターゲット・ソフトウェアのバージョンを表示する場合などに使用できます。

例えば、特定のバージョンの Remote Control ターゲット・ソフトウェアを実行しているターゲットのリストを表示するには、**「適用可能なコンピューター」** > **「取得プロパティー別」** > **「Remote Control ターゲットのバージョン別」**を展開して、リストから特定のバージョンを選択します。関連するターゲットのリストが表示されます。

監査イベント・データの取得

「リモート・コントロール・ターゲット・ログ」分析は、Remote Control コントローラー・コンポーネントがインストールされている環境内のコンピューターから監査イベントを収集するために使用されます。この情報は、6 時間ごとに取得され、更新されます。この情報は、監査の目的で使用できるほか、コントローラー・ユーザーが実行したセッション・アクティビティーをモニターするためにも使用できます。

分析がアクティブな場合、**「結果」**タブには、この分析が関連したコンピューターのリストが表示されます。コンピューターの 1 つをダブルクリックすると、選択したコンピューターの概要データが表示されます。このデータには、**「リモート・コントロール・コントローラー・ログ」**分析によって取得されたコントローラー・ログ・エントリーのセクションが含まれています。**「適用可能なコンピューター」**エントリーを展開し、特定の取得プロパティーによってデータをさらにフィルタリングすることもできます。

注: コントローラー・コンポーネントがリモート・コントロール・セッションでアクティブである場合に、分析でそのコントローラーからデータを収集しようとすると、エラーが報告されます。このエラーは、分析結果で報告され、ファイルが使用中であることを示します。

ユーザー、セッション、およびパフォーマンス・データの取得

「リモート・コントロール・ユーザー、セッション、パフォーマンス・オプション」分析は、環境内のターゲットから、ユーザーの操作、セッションの動作、およびパフォーマンスのプロパティー値を収集するために使用されます。これらのプロパティーを使用すると、このターゲットとのリモート・コントロール・セッション中にコントローラー・ユーザーが実行できるアクションを確認できます。プロパティー値の定義については、ステップ 2 を参照してください。

分析がアクティブな場合、「結果」タブには、この分析が関連したコンピューターと、ユーザー操作プロパティーの値が表示されます。**「適用可能なコンピューター」**エントリーを展開し、特定の取得プロパティーによってデータをさらにフィルタリングすることができます。

セッション接続データの取得

「リモート・コントロール・ターゲット・ログ (開始/停止)」分析は、Remote Control ターゲット・コンポーネントがインストールされている環境内のコンピューターから監査イベントを収集するために使用されます。

この情報は、6 時間ごとに取得され、更新されます。この分析で返される情報は、特定ターゲットでのリモート・コントロール・セッション使用アクティビティーを表示するのに役立ちます。セッション接続、開始イベント、および終了イベントのみが各セッションについて返されます。リモート・コントロール・セッション・アクティビティーに関する情報が必要な場合は、**「リモート・コントロール・ ターゲット・ログ」**分析を使用してください。

注: この分析は、Windows™ ターゲットにのみ有効です。

分析がアクティブな場合、「結果」タブには、この分析が関連していたコンピューターがリストされます。コンピューターをダブルクリックすると、選択したコンピューターの概要データが表示され、その中にターゲット・ログ

開始/停止エントリーのセクションが含まれています。「適用可能なコンピューター」エントリーを展開し、特定の取得プロパティーによってデータをさらにフィルタリングすることもできます。

セッション・アクティビティー・データの取得

「リモート・コントロール・ターゲット・ログ」分析は、Remote Control ターゲット・コンポーネントがインストールされている環境内のコンピューターから監査イベントを収集するために使用されます。この情報は、6 時間ごとに取得され、更新されます。この情報は、監査のために役立ちます。リモート・コントロール・セッション中に実行されたアクションの詳細が表示されます。例えば、セッション・タイプの変更やファイルの転送などです。セッションのコントローラー・ユーザーも表示されます。

分析がアクティブな場合、**「結果」**タブには、この分析が関連したコンピューターが表示されます。コンピューターの 1 つをダブルクリックすると、選択したコンピューターの概要データが表示されます。このデータには、**「リモート・コントロール・ターゲット・ログ」**分析によって取得されたターゲット・ログ・エントリーのセクションが含まれています。**「適用可能なコンピューター」**エントリーを展開し、特定の取得プロパティーによってデータをさらにフィルタリングすることもできます。

注: 理由コードの詳細情報を表示するには、Web レポート機能を使用して出力を表示します。Web ツールの詳細については、Web レポートの表示を参照してください。

ターゲットでのスマート・カード認証の有効化

BigFix® Remote Control ターゲット でスマート・カード認証をサポートするには、仮想スマート・カード・リーダー・ドライバーと関連証明書をターゲットにインストールする必要があります。ターゲットをインストールした後に、BigFix® コンソールで Fixlet® を実行してドライバーおよび証明書をインストールすることができます。Active Directory グループ・ポリシーを使用しても証明書をインストールすることができます。

リモート認証でスマート・カードを使用できるようにする場合、あるいはターゲット・コンピューターに対してアクションを実行する場合は、IBM® 仮想スマート・カード・リーダー用のデバイス・ドライバーが必要です。リモート・コントロール・セッション中に、ターゲットは仮想カード・リーダーを作成します。コントローラー・ユーザーは、使用しているシステム上にある物理カード・リーダーを選択し、これを仮想カード・リーダーに接続して、ターゲット・システムがスマート・カードにアクセスできるようにします。セッション中に、Windows™ から仮想カード・リーダーに要求が出されると、ターゲットはその要求をコントローラー・システム上の物理カード・リーダーにリダイレクトします。セッション中のスマート・カード機能の使用について詳しくは、「*BigFix® Remote Control* コントローラー・ユーザーズ・ガイド」を参照してください。

注: IBM® 仮想スマート・カード・リーダーのデバイス・ドライバーは、Windows™ 7 以降、および Windows™ Server 2008 R2 以降でのみサポートされます。

スマート・カード・サポートが有効になっているかどうかの判別

ターゲットでスマート・カード・サポートを有効にするには、複数の前提条件を満たす必要があります。分析を使用して、どのコンピューターでアクションが必要であるかを確認してください。

コンピューターの状況を確認するには、以下の手順を実行します。

1. **「Remote Control」**サイトの**「Remote Control - 仮想スマート・カード・リーダーのドライバー状況」**分析に進みます。
2. **「説明」**タブの情報を確認します。
3. **「結果」**タブの情報を確認します。
   スマート・カードのサポートが有効になっている場合、**「ドライバーはインストール済み」**の値はインストールされたドライバーのバージョンを報告し、以下のプロパティーには「はい」の値が表示されます。
   - **Trusted Publisher SHA1 はインストール済み**
   - **Trusted Publisher SHA256 はインストール済み**
   - **Root CA SHA1 はインストール済み**
   - **Root CA SHA256 はインストール済み**

   プロパティー**「KB2921916 はインストール済み」**および**「KB3033929 はインストール済み」**には、ターゲットにインストールされている Windows オペレーティング・システムのバージョンによって「はい」または「該当なし」の値が表示されます。

注: 「KB2921916 はインストール済み」列および**「KB3033929 はインストール済み」**列に *<error>* が表示される場合は、Windows™ サイト向けパッチをサブスクライブしていることを確認する必要があります。BigFix® コンソールの**「ライセンスの概要」**セクションで、Windows™ サイト向けパッチを有効にしてください。

Fixlet の実行による仮想スマート・カード・リーダー・ドライバーおよび証明書のインストール

BigFix® コンソールで Fixlet を実行して、仮想スマート・カード・リーダー用のデバイス・ドライバーを証明書と一緒にインストールします。

ターゲットをインストールした後に、Fixlet を実行してドライバーおよび証明書をインストールすることができます。ドライバーおよび証明書をインストールするには、以下の手順を実行します。

1. **Remote Control**サイトで、**「デプロイメント」**ノードをクリックします。
2. **「Remote Control 仮想スマート・カード・リーダー・ドライバーバージョン10.0.0.23 および証明書をインストール」**タスクを選択します。
3. **「説明」**タブの情報を確認します。
4. **「アクション」**フィールドの説明に従い、ドライバーをインストールします。

スマート・カード認証に必要なデバイス・ドライバーおよび証明書がインストールされます。これで、リモート・コントロール・セッション中にコントローラー・ユーザーがシステム上の物理カード・リーダーを選択すると、ターゲットは仮想カード・リーダーを作成できるようになります。

注: Fixlet の実行中にエラーが報告される場合、ターゲットのインストール・ディレクトリーにある `VSCDriverInstall.log` ファイルをデバッグのために使用してください。

の実行による仮想スマート・カード・リーダー・ドライバーおよび証明書の削除 Fixlet®

BigFix® コンソールで Fixlet® を実行して、IBM® 仮想スマート・カード・リーダー用のデバイス・ドライバーを証明書と一緒に削除します。

ドライバーおよび証明書を削除するには、以下の手順を実行します。

1. **Remote Control**サイトで、**「デプロイメント」**ノードをクリックします。
2. **「Remote Control の仮想スマート・カード・リーダー・ドライバーをアンインストール」**タスクを選択します。
3. **「説明」**タブの情報を確認します。
4. **「アクション」**フィールドの指示に従ってドライバーおよび証明書を削除します。

スマート・カード認証に必要なデバイス・ドライバーおよび Trusted Publisher 証明書が、選択されたコンピューターから削除されます。選択されたコンピューターでは、スマート・カード機能を使用できなくなります。

注: Fixlet® の実行中にエラーが報告される場合、ターゲットのインストール・ディレクトリーにある `VSCDriverUninstall.log` ファイルをデバッグのために使用してください。

の実行による証明書のインストール Fixlet®

Fixlet® を使用して、仮想スマート・カード・リーダー用のデバイス・ドライバーに必要な証明書をインストールします。

Fixlet® を実行することによって、証明書をドライバーと一緒にインストールすることができます。ただし、**「Remote Control - 仮想スマート・カード・リーダーのドライバー状況」**分析の結果に、デバイス・ドライバーはコンピューターにインストールされていて証明書は存在していないことが示される場合、Fixlet® を実行して証明書をインストールすることができます。証明書をインストールするには、以下の手順を実行します。

1. **Remote Control**サイトで、**「デプロイメント」**ノードをクリックします。
2. **「仮想スマート・カード・リーダー・ドライバー・バージョン 10.0.0.23 の Remote Control 証明書をインストールする」**タスクを選択します。
3. **「説明」**タブの情報を確認します。
4. **「アクション」**フィールドの説明に従い、ドライバーをインストールします。

スマート・カード認証に必要な証明書がインストールされます。**「Remote Control - 仮想スマート・カード・リーダーのドライバー状況」**分析について詳しくは、『スマート・カード・サポートが有効になっているかどうかの判別』を参照してください。

注: Fixlet® の実行中にエラーが報告される場合、ターゲットのインストール・ディレクトリーにある `VSCCertsInstall.log` ファイルをデバッグのために使用してください。

仮想スマート・カード・リーダー用の証明書のダウンロード

仮想スマート・カード・リーダー用のデバイス・ドライバーに必要な証明書をダウンロードして、手動でインストールすることができます。例えば、Active Directory グループ・ポリシーを使用します。

証明書のダウンロードは複数の方法で実行できます。証明書をダウンロードする方法を選択してください。

- BigFix® コンソールの Remote Control サイトからのファイルのダウンロード:
  1. **「デプロイメント」**ノードをクリックして、**「Remote Control 仮想スマート・カード・リーダー・ドライバー・バージョン 10.0.0.23 および証明書をインストールする」**タスクを選択します。
  2. **「説明」**タブを選択します。
  3. **「説明」**フィールドの説明に従い、証明書をダウンロードします。
  4. `vsc_certs_1020.zip` ファイルを保存します。
  5. `.zip` ファイルから証明書ファイルを解凍します。
- インストール・メディアからの証明書ファイルの解凍:
  1. イメージ・ファイルにアクセスします。イメージ・ファイルについて詳しくは、インストール・ファイルの入手を参照してください。
  2. `BigFix_Rem_Cntrl_V10xx_Image_1.zip` ファイルをダウンロードします。ここで、*10xx* はインストールされているバージョンに対応します。
  3. `.zip` ファイルの `\Windows` ディレクトリーから、証明書ファイルを解凍します。

証明書をインストールするときに、`HCL_America_Inc-sha256.crt` ファイルを Trusted Publishers ストアにインストールする必要があります。`TrustedRoot.crt` ファイルおよび `DigiCertCA-sha256.crt` ファイルを Trusted Root Certificate Authorities ストアにインストールします。

サーバーでのシングル・サインオン (SSO) の構成

Remote Control V9.1.3 では、Remote Control サーバー上で SAML 2.0 認証がサポートされるようになりました。

シングル・サインオン (SSO) は複数の方法で構成できます。

- Remote Control サーバーのインストール中。
- サーバーのインストール後。

SSO を構成して、Remote Control サーバーにアクセスすると、ログオンのために SAML ID プロバイダーのログオン・ページにリダイレクトされます。Remote Control サーバー UI のログオン・ページは、表示されなくなりました。ただし、管理者ユーザー ID では、SSO を使用せずに Remote Control サーバーにログオンできるはずです。SSO が有効な場合に、ご使用のブラウザーで次の URL を入力して、管理者ユーザー ID でログオンしてください。`https://[serverurl]/trc/altLogon.do`、ここで *[serverurl]* は Remote Control サーバーの URL です。

インストール中のシングル・サインオン用のサーバーの構成

Remote Control サーバーのインストール中に、SAML V2.0 認証に対するサポートを構成することができます。

Fixlet® を実行して、サーバーのインストール・ファイルをダウンロードします。詳しくは、『Remote Control サーバー・コンポーネントのダウンロード』を参照してください。

1. 「」の「**サーバー・インストーラーを使用したインストール**」*BigFix® Remote Control* インストール・ガイド 章のインストール手順に従います。
2. インストール中に、SSO の構成ウィンドウで構成オプションを選択します。

   SSO の有効化 (Enable SSO)

   シングル・サインオン (SSO) を有効にするには、このオプションを選択します。構成を続行するには、ID プロバイダー (IdP) から SAML メタデータ XML ファイルと、使用されているハッシュ・アルゴリズム(SHA-1 または SHA-256) を取得する必要があります。

   メタデータ XML ファイル (Metadata XML file)

   「選択」をクリックして、IdP から取得した SAML メタデータ XML ファイルを選択します。

   SAML メッセージの署名に使用するアルゴリズム (Algorithm used to sign SAML messages)

   ID プロバイダー (IdP) とこのサービス・プロバイダー、つまり BigFix® Remote Control サーバー の間の通信でメッセージに署名するために使用する署名アルゴリズム (SHA-1 または SHA-256) を選択します。

   拡張パラメーター (Advanced parameters) (オプション)

   その他の構成オプションを入力します。属性名を*[keyword]="[keyword-value]*" 形式でスペース区切りリストに追加します。ここで *[keyword]* は、属性名、は *[keyword-value]* 属性値です。

   SAML データを強制的に再生成します (IdP を使用して再登録する必要があります)。

   SSO を最初に有効にしたときに、新しいデフォルトの SAML 証明書鍵ストアが作成されています。今後のアップグレードでは、新しいデフォルトの証明書鍵ストアを作成するための再生成オプションを選択できます。現在の鍵ストアは削除され、新しい鍵ストアが保存されます。このオプションを選択する場合、サーバーの再始動後に SP と IdP の間の接続を再確立する必要があります。
3. インストールを完了します。インストール・プログラムの**「概要」**ウィンドウで**「インストール」**をクリックした後、**「重要」**ウィンドウが表示されます。**「重要」**ウィンドウの URL と情報を書き留めます。サーバーが始動した後、その URL をブラウザーに入力して、SP メタデータをダウンロードします。このメタデータを IdP に提供して、サーバーと IdP の間の連携を確立する必要があります。

インストール後のシングル・サインオン用のサーバーの構成

Remote Control サーバーをインストールした後、SAML 2.0 認証をサポートするように構成することができます。

構成を開始する前に、単一の自己署名証明書を使用して鍵ストアを作成する必要があります。**「鍵サイズ」**として 2048 を選択し、**「署名アルゴリズム」**として sha256 を選択します。鍵ストア・ファイルは、`.p12` または `.jks` のファイルにできます。このファイルをサーバーのインストール・ディレクトリーに保存しないでください。そうすると、サーバーの自己署名証明書との間で競合が生じる可能性があるためです。鍵ストアには長い有効期間を設定してください。鍵ストア・ファイルの作成について詳しくは、自己署名証明書の作成を参照してください。

注: Remote Control では、WebSphere Liberty の samlWebSso20 機能によって SSO がサポートされます。デフォルトでは、ID プロバイダーからサービスに返される **NameID** に、以下の形式の E メール・フィールドが含まれている必要があります。

```
URI: urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
```

Liberty で samlWeb-2.0 フィーチャーを有効にすることにより、Liberty サーバーを SAML Web ブラウザー・シングル・サインオン (SSO) サービス・プロバイダーとして構成できます。

Remote Control サーバーを構成するには、以下の手順を実行します。

1. 以下のディレクトリーに `sso.xml` ファイルを作成します。

   Windows™ オペレーティング・システム

   `C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver`

   Linux™ オペレーティング・システム

   `/opt/BigFix/TRC/server/wlp/usr/servers/trcserver`

2. 以下のコンテンツを `sso.xml` ファイルに追加します。

```
<server>
<featureManager> }}
<feature>samlWeb-2.0</feature>}}
</featureManager> }}
<samlWebSso20 id="defaultSP" keyStoreRef="samlKeyStore" httpsRequired="true"
signatureMethodAlgorithm="SHA256" spHostAndPort="https://[hostname:port]"/>
<keyStore id="samlKeyStore" location="[samlKey.file]"
password="[yourkeystorepassword]" type="[filetype]"/>
</server>
```

   [hostname:port]

   Remote Control サーバーのホスト名および SSL ポートを定義します。例えば、https://example.com:443/ です。

   [samlKey.file]

   鍵ストア・ファイルへのパスを定義します。例えば、`c:\trc\samlKey.jks` です。

   [yourkeystorepassword]

   鍵ストア・ファイルのパスワードを定義します。例えば、password="mypassword" です。

   [filetype]

   鍵ストア・ファイルのファイル・タイプを定義します。`.p12` ファイルの場合は、タイプを PKCS12 に設定します。`.jks` ファイルの場合は、タイプを JKS に設定します。

keyStore*id* 値は、**<samlWebSso20>** エレメントの **keyStoreRef** 値と一致していなければなりません。

さらに構成パラメーターを追加できます。詳しくは、「SAML WEB SSO 2.0 認証 (samlWebSso20)」を参照してください。

デフォルトの構成では、以下の値が使用されます。

AssertionConsumerService URL

`https://<hostname>:<sslport>/ibm/saml20/defaultSP/acs`.

サービス・プロバイダー (SP) メタデータ URL

`https://<hostname>:<sslport>/ibm/saml20/defaultSP/samlmetadata`

ここで、**<hostname>** は Remote Control サーバーのホスト名、**<sslport>** は SSL ポート値です。例えば、443 です。

3. 以下のディレクトリーの `application.xml` ファイルを編集します。

Windows™ オペレーティング・システム

`C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver`

Linux™ オペレーティング・システム

`/opt/BigFix/TRC/server/wlp/usr/servers/trcserver`

このファイルに以下の **<application-bnd>** ステートメントを追加します。

```
<server>
 <application   context-root="/trc" type="ear" id="trcserver"
 location="TRCAPP.ear" name="trcserver"  autoStart="true" >
 <application-bnd>
  <security-role name="any-authenticated">
  <special-subject type="ALL_AUTHENTICATED_USERS" />
  </security-role>
 </application-bnd>
 </application>
 <application   context-root="/" type="ear" id="trcredir"
 location="REDIR.ear" name="trcredir"  autoStart="true" />
 <applicationMonitor updateTrigger="disabled" dropinsEnabled="false" />
</server>
```

4. ID プロバイダー (IdP) から SAML メタデータ XML ファイルを取得します。
このファイルの取得方法は、IdP によって異なります。ファイルの名前を `idpMetadata.xml` に変更して、サーバー上の以下のディレクトリーにコピーします。

Windows™ オペレーティング・システム

`C:\Program Files (x86)\BigFix\TRC\server\wlp\usr\servers\trcserver\resources\security`

Linux™ オペレーティング・システム

```
/opt/BigFix/TRC/server/wlp/usr/servers/trcserver/resources/security
```

5. `common.properties` ファイルを編集して、**sso.enabled** を *True* に設定します。
   このファイルは以下のディレクトリーにあります。

   Windows™ システム

   ```
   [installdir]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF
   \classes
   ```

   ここで、*[installdir]* は、Remote Control サーバーがインストールされているディレクトリーです。

   Linux™ システム

   ```
   [installdir]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/
   classes
   ```

   ここで、*[installdir]* は、Remote Control サーバーがインストールされているディレクトリーです。

6. Remote Controlサーバーを再始動します。
7. サーバーが再始動した後、以下の URL をブラウザーに入力して、このサービス・プロバイダー (SP)、つまり BigFix® Remote Control サーバー のメタデータをダウンロードします。
   `https://<hostname>:<sslport>/ibm/saml20/defaultSP/samlmetadata`、ここで *<hostname>* は Remote Control サーバーのホスト名で、*<sslport>* はサーバーの SSL ポートです。このメタデータを SAML ID プロバイダーに提供して、この SP と ID プロバイダー (IdP) の間の連携を確立します。

Remote Control サーバー・アプリケーションにアクセスするときに、以前にログオンしたことがない場合は、IdP にリダイレクトされます。以前に同じ IdP を使用してログオンしたことがある場合は、Remote Control サーバー・アプリケーションに自動的にログオンします。

注: SAML 2.0 認証を有効にした後にサーバーの再インストールまたはアップグレードを実行する場合は、開始前に `sso.xml` ファイルを一時ディレクトリーにコピーする必要があります。アップグレード中にインストールされる `sso.xml` ファイルをバックアップ・ファイルに置き換えます。また、`common.properties` ファイルで **sso.enabled** が *True* に設定されていることを確認してください。

セキュア・ターゲット登録の有効化

無許可のターゲットが Remote Control サーバーに登録されないよう、セキュア登録機能を有効にし、トークンを使用してターゲットを認証できます。

サーバーをインストールした後に、サーバーで登録トークンを作成し、ターゲットのインストール時にそのトークンを配布します。このトークンは、新規のターゲット登録を制限したり、ターゲットの再インストール時に既存のターゲット詳細の更新を制限したりするために使用します。ターゲットを登録すると、サーバーはエンドポイント・トークンをそのターゲットに送信し、登録時に使用されたトークンを置き換えます。ターゲットは、サーバーに接続するたびにエンドポイント・トークンを使用してサーバーで認証を受けます。

新しいインストール・シナリオ

以下のシナリオでは、サーバーとターゲットの新規インストールについて説明します。

- サーバー・インストーラー・タスクを作成し、**「セキュア登録トークンを使用してターゲットを登録する」**を選択します。**「デフォルトでターゲットの URL に HTTPS を使用」**も選択されていることを確認します。タスクを実行します。サーバー・インストーラー・タスクの作成について詳しくは、『Remote Control サーバー・インストール・タスクの作成』を参照してください。
- サーバー UI でセキュア登録トークンを作成します。
    1. **「アドミニストレーター」 > 「セキュア登録トークンの作成」**をクリックします。
    2. トークンに関する以下の情報を入力します。デフォルト期間は現在の日時から次の日の 23:59 までです。
        - 「トークンの説明」。トークンの説明を入力します。
        - 「開始日」。カレンダーのプルダウンをクリックし、トークンの有効期間の開始日を選択します。開始時刻を入力するか、デフォルト時刻のままにします。
        - 「終了日」。カレンダーのプルダウンをクリックし、トークンの有効期間の終了日を選択します。終了時刻を入力するか、デフォルト時刻のままにします。
    3. 「**送信**」をクリックします。ページを終了する前に、必ず登録トークンをコピーしてください。トークンは機密情報として安全に保管してください。
- 関連するターゲット・デプロイメント・タスクを実行して、登録トークンを入力します。詳しくは、Windows ターゲットのデプロイ またはLinux ターゲットのデプロイを参照してください。

アップグレードのシナリオ

以下のシナリオでは、サーバーとターゲットのアップグレードについて説明します。

- サーバー構成タスクを作成します。**「セキュア登録トークンを使用してターゲットを登録する」**は選択しないでください。**「既存のプロパティー・ファイルから値を移行する」**を選択します。タスクを実行します。サーバー・インストーラー・タスクの作成について詳しくは、『Remote Control サーバー・インストール・タスクの作成』を参照してください。
- サーバー UI でセキュア登録トークンを作成します。
    1. **「アドミニストレーター」 > 「セキュア登録トークンの作成」**をクリックします。
    2. トークンに関する以下の情報を入力します。デフォルト期間は現在の日時から次の日の 23:59 までです。
        - 「トークンの説明」。トークンの説明を入力します。
        - 「開始日」。カレンダーのプルダウンをクリックし、トークンの有効期間の開始日を選択します。開始時刻を入力するか、デフォルト時刻のままにします。
        - 「終了日」。カレンダーのプルダウンをクリックし、トークンの有効期間の終了日を選択します。終了時刻を入力するか、デフォルト時刻のままにします。
    3. 「**送信**」をクリックします。ページを終了する前に、必ず登録トークンをコピーしてください。トークンは機密情報として安全に保管してください。

- ターゲットをアップグレードするには、ご使用のオペレーティング・システムに関連する更新タスクを実行します。詳しくは、Windows ターゲットの更新 またはLinux ターゲットの更新を参照してください。
- **「Remote Control ターゲットのセキュア登録トークンを設定する」**タスクを実行して、登録トークンを入力します。詳しくは、『ターゲットへのセキュア登録トークンの配布』を参照してください。
- サーバー UI では、セキュア登録機能が有効になっています。
    1. サーバーの UI で、**「アドミニストレーター」 > 「プロパティー・ファイルを編集」**を選択します。
    2. リストから `trc.properties` を選択します。
    3. **rc.enforce.secure.registration** を true に設定します。**enforce.secure.endpoint.callhome** プロパティーと **enforce.secure.endpoint.upload** プロパティーも true に設定されていることを確認します。
    4. 「**送信**」をクリックします。
    5. **「アドミニストレーター」 > 「アプリケーションをリセット」**をクリックします。

ターゲットへのセキュア登録トークンの配布

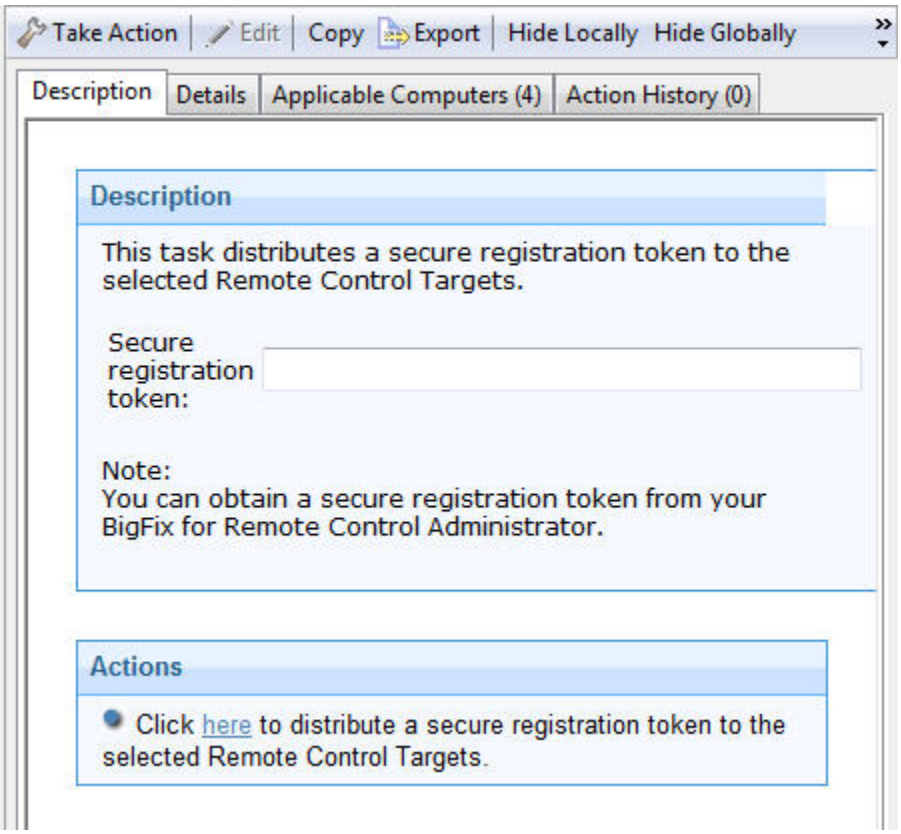
「Remote Control ターゲットのセキュア登録トークンを設定する」タスクを使用して、選択したターゲットにセキュア登録トークンを配布します。ターゲットはトークンを使用して、Remote Control サーバーに安全に登録できます。

タスクを実行するには、有効なセキュア登録トークンが必要です。トークンの作成について詳しくは、 の『*BigFix® Remote Control* 管理者ガイド**セキュア登録トークンの作成**』を参照してください。

セキュア・ターゲット登録のために、Remote Control サーバーでもこの機能を有効にする必要があります。`trc.properties` ファイルの **rc.enforce.secure.registration** プロパティーは true に設定する必要があります。**enforce.secure.endpoint.callhome** プロパティーと **enforce.secure.endpoint.upload** プロパティーも true に設定されていることを確認します。サーバーでのセキュア登録の有効化について詳しくは 、 の『*BigFix® Remote Control* インストール・ガイド**サーバーでのセキュア・ターゲット認証の有効化**』を参照してください。

セキュア登録トークンを配布するには、以下の手順を実行します。

1. **「システム・ライフサイクル」**ドメイン内で、**「Remote Control の設定」 > 「Remote Control」**を展開します。
2. **[更新]** を選択します。
3. **「更新」**ペインで、**「Remote Control ターゲットのセキュア登録トークンを設定する」**タスクを選択します。
4. **「タスク」**ペインで、説明を確認します。セキュア登録トークンを入力します。**「アクション」**ボックス内の指示に従ってタスクを開始します。



5. **「アクションの実行」**ペインの**「対象」**タブで、セキュア登録トークンを配布するコンピューターを決定するための関連オプションを選択します。

次回ターゲットがサーバーに接続するときに、ターゲットはセキュア登録トークンを送信します。サーバーでセキュア認証機能が有効になっている場合、サーバーはトークンを検証します。トークンが有効であれば、ターゲットはサーバーに登録され、サーバーはエンドポイント・トークンをターゲットに送り返します。

Web レポートの表示

Remote Control は、アプリケーションの**「Web レポート」**コンポーネント内で使用可能なレポートを提供します。この Web レポートは、コントローラーから収集されたログ・データと、特定の対象コンピューターに関連するターゲット・ログを提供するように作成されています。このデータは監査目的に使用したり、環境内の特定のコンピューターについてのリモート・コントロール・アクティビティーをモニターしたりするために使用できます。

Remote Control Web レポートにアクセスするには、次に示す手順を実行します。

1. **「ツール」 > 「Web レポートの起動」**をクリックします。
2. **Web レポート**のユーザー名とパスワードを入力します。
   ユーザー名またはパスワードがわからない場合は、管理者に確認してください。ログオンすると、Web レポートのメイン・ページが新規ブラウザー・ウィンドウで開きます。
3. **「システム・ライフサイクル」**を選択して、Remote Control レポートを含むレポートのリストを表示します。

Remote Control イベントのエントリーは、**「レポート一覧」**メニューの下のレポート・リストに表示されます。

4. **「Remote Control イベント」**をクリックします。
5. 情報を表示する対象のコンピューター名を入力し、**「イベントの表示」**をクリックします。

指定された対象コンピューターについて、コントローラーおよびターゲット・ログから収集されたすべてのログ・データが関連するセクションに表示され、リモート・コントロール・イベントを確認することができます。

よくある質問

1. ターゲット・ソフトウェアをターゲットにインストールしましたが、BigFix® コンソールでコンピューターを右クリックしたときにリモート・コントロール・セッションを開始するメニュー・オプションが表示されません。

   この方法を使用してリモート・コントロール・セッションを開始するには、以下の条件が満たされていることを確認してください。
   - BigFix® コンソールがインストールされているシステムに、コントローラー・コンポーネントもインストールされていること。
   - メニュー項目が表示されるようにするには、**「Remote Control のインストールおよびセキュリティー・オプション」**分析が、選択されたコンピューターについてアクティブであり、Remote Control ターゲットがアクティブであると報告している必要があります。
   - コントローラーがインストールされたとき、メニュー項目の表示権限があるのは、インストール対象のコンピューターにログオンしている現行ユーザーのみです。その他のユーザーには表示されません。以下のレジストリー・キーも作成することができます。

     キー名: `HKEY_CURRENT_USER\Software\BigFix\Enterprise Console\Settings\ComputerListContextMenuExtensions\TivoliRC`

     以下の値を使用します。

     ```
     ComputerApplicabilityRelevance (REG_SZ) = value of results (current computer, property 1 of
      fixlet 4 of bes site whose (name of it starts with "BigFix Remote Control")) = "True"
     ```

     ```
     MaxComputerSetSize (REG_DWORD) = 1
     ```

     ```
     MenuDisplayName (REG_SZ) = &BigFix Remote Control
     ```

     ```
     ShellCommandRelevance (REG_SZ) = "%22C:\Program Files\BigFix\Remote
      Control\Controller\jre\bin\javaw.exe%22 -jar %22C:\Program Files\BigFix\Remote
      Control\Controller TRCConsole.jar%22 --host " & ip address of current computer as string
     ```

2. ターゲット・ソフトウェアを P2P モードでインストールしました。次は、ターゲットを Remote Control サーバーに登録する必要があります。どのようにしたら、このサーバーに接続できますか?

Remote Control ターゲット・ウィザードを使用して構成タスクを作成し、必要なサーバーのサーバー URL を指定します。選択したターゲットでこのタスクを実行すると、ターゲットが再構成され、サーバーに接続できるようになります。タスクの作成について詳しくは、Remote Control ターゲット構成タスクの作成を参照してください。

3. Remote Control の使用についての詳細な情報はどこで見つけられますか?

   Remote Control のインストール、使用、および管理に関する情報は、HCL Knowledge Center の Remote Control 資料で見つけることができます。

4. Remote Control サーバー・コンポーネントがインストールされている場合、Remote Control の追加の機能を使用できますが、サーバー・コンポーネントはどこから取得できますか?

   Remote Control サーバー・インストーラー・ウィザードを使用してサーバー・インストール・タスクを作成し、Remote Control サーバー構成を作成することができます。サーバー・タスクの作成の詳細については、Remote Control サーバー・インストール・タスクの作成を参照してください。

   また、インストール済みの DB2®、MS SQL、または Oracle データベースを使用する、インストール済みの Websphere Application Server インスタンスを指すサーバーをインストールすることもできます。サーバーのインストールについて詳しくは、「*BigFix® Remote Control* インストール・ガイド」、および『サーバーのインストール』と示されているセクションを参照してください。

5. 環境に適したサーバー・インストールのタイプはどのように判別できますか?

   インストールの計画時に考慮すべきガイドラインについては、「*BigFix® Remote Control* インストール・ガイド」を参照してください。

6. ブローカーとゲートウェイのアップグレード Fixlet が MSI エラー・コード 1638 で失敗する場合のトラブルシューティング方法を教えてください。

   詳細と手順については、『ブローカーとゲートウェイのアップグレード Fixlet が失敗する』を参照してください。

Support

For more information about this product, see the following resources:

- BigFix Support Portal
- BigFix Developer
- BigFix Playlist on YouTube
- BigFix Tech Advisors channel on YouTube
- BigFix Forum

Notices

This information was developed for products and services offered in the US.

HCL may not offer the products, services, or features discussed in this document in other countries. Consult your local HCL representative for information on the products and services currently available in your area. Any reference to an HCL product, program, or service is not intended to state or imply that only that HCL product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any HCL intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-HCL product, program, or service.

HCL may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

For license inquiries regarding double-byte character set (DBCS) information, contact the HCL Intellectual Property Department in your country or send inquiries, in writing, to:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

HCL TECHNOLOGIES LTD. PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. HCL may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-HCL websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this HCL product and use of those websites is at your own risk.

HCL may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

HCL
330 Potrero Ave.
Sunnyvale, CA 94085
USA
Attention: Office of the General Counsel

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by HCL under terms of the HCL Customer Agreement, HCL International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-HCL products was obtained from the suppliers of those products, their published announcements or other publicly available sources. HCL has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-HCL products. Questions on the capabilities of non-HCL products should be addressed to the suppliers of those products.

Statements regarding HCL's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to HCL, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. HCL, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS," without warranty of any kind. HCL shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from HCL Ltd. Sample Programs.

Trademarks

HCL Technologies Ltd. and HCL Technologies Ltd. logo, and hcl.com are trademarks or registered trademarks of HCL Technologies Ltd., registered in many jurisdictions worldwide.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other product and service names might be trademarks of HCL or other companies.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the HCL website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of HCL.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of HCL.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

HCL reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by HCL, the above instructions are not being properly followed.

索引