IBM Endpoint Manager for Remote Control

Console Users Guide

Version 9 Release 0

IBM Endpoint Manager for Remote Control

Console Users Guide

Version 9 Release 0

Note
Before using this information and the product it supports, read the information in "Notices" on page 83.

This edition applies to version 9, release 0, modification level 0 of IBM Endpoint Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview of the IBM Endpoint Manager for Remote Control system

The IBM® Endpoint Manager for Remote Control system includes the following main components:

IBM Endpoint Manager for Remote Control Target
The target is installed on every computer that you want to control remotely with IBM Endpoint Manager for Remote Control. It listens for connection requests that come from the controller. The target can also be used to start a remote control session over the internet, by using a broker.

Targets that are outside of your intranet can be configured to register their details with the server. Sessions with these targets are managed by server policies. The targets must be deployed with the **Managed** property set to Yes. The **ServerURL** and **BrokerList** properties must also be configured. If you are using version 9.0.1, targets can also be configured so that they do not send their details to the server. These targets are classed as unregistered targets. There are two ways to configure unregistered targets. You can install the target software and set the **Managed** property to No. The **BrokerList** property must also be set. You can also use the on-demand target features to start a remote control session with a computer that does not have any target software preinstalled. Server policies are used to manage the on-demand sessions. The target software is deleted at the end of the session.The IBM Endpoint Manager for Remote Control target can run in Windows, Linux, and Solaris operating systems.

IBM Endpoint Manager for Remote Control Controller
Can be installed by using the Fixlet or installer that is provided for use in peer to peer sessions. It can also be launched in context from the remote control server or the IBM Endpoint Manager console. In all instances, the controller can be used to allow the user to control a remote computer on which the remote control target is installed. The controller delivers an interface to several actions, available to the controller user, like remote control, guidance, chat, file transfer, collaboration, and many more. IBM Endpoint Manager for Remote Control controller supports JRE versions: Sun 1.6, Oracle 1.6, 1.7 or IBM® 1.5, 1.6, 1.7.

IBM Endpoint Manager for Remote Control Server
A web application that manages all the deployed targets that are configured to be in managed mode and to point to the IBM Endpoint Manager for Remote Control Server 's URL. The server is a web application that can be deployed on an existing WebSphere® server, or installed through the installer package along with an embedded version of WebSphere. The server listens for HTTP or HTTPS connections by default. When it is installed with the embedded WebSphere option, it listens on ports 80 and 443. When it is deployed on top of an existing WebSphere server, the IBM Endpoint Manager for Remote Control server listens on ports 9080 and 9443. The server requires a database server: embedded Derby, only for proof of concept deployments, DB2®, SQL Server, and Oracle are the supported options. Additionally, it can also be configured to synchronize and authenticate user and group data from an LDAPv3 server, like Active Directory or Tivoli Directory Server. This deployment scenario has the same networking characteristics as peer to peer. Therefore, direct TCP connectivity is required between all the controllers and all the targets.

However, the IBM Endpoint Manager for Remote Control server provides a method of centralized, and finer, policy control, where targets can have different policies that are determined by the user who is trying to start the remote control session. The Server also provides for centralized audit and storage of full session automatic recordings. In this scenario, the controller is not a stand-alone application.but is started as a Java™ Web Start application from the IBM Endpoint Manager for Remote Control server's web interface to start the remote control session.

Note: Peer to peer and managed are not exclusive modes. The IBM Endpoint Manager for Remote Control target can be configured in the following ways.

- Configured to be strictly managed.
- Configured to fail back to peer to peer mode when the server is not reachable.
- Configured to accept both peer to peer and managed remote control sessions.

The following components can be used only in managed mode:

IBM Endpoint Manager for Remote Control CLI tools
Are always installed as part of the target component but it is also possible to install them separately. The CLI provides command-line tools for the following tasks:

- Script or integrate the launch of managed remote control sessions.
- Run remote commands on computers with the managed target installed.

IBM Endpoint Manager for Remote Control Gateway
A service that is installed in computers in secure network boundaries, where there is strict control of traffic flows between the secure networks. For example, the firewall at the boundary allows only traffic between a pair of specific IP address and ports. In these scenarios, a network of gateways can be deployed. The gateway routes and tunnels the remote control traffic from the controller that is sitting in a particular network zone, to the target that is in a different network zone. The gateway is a native service that can be installed on a computer that has a Windows or Linux operating system installed. It does not have a default listening port, although 8881 is a usual choice, and can be configured for multiple incoming listening ports and outgoing connections.

IBM Endpoint Manager for Remote Control Broker
A service that is installed in computers typically in a DMZ so that computers out of the enterprise network, in an Internet cafe or at home, can reach it. The IBM Endpoint Manager for Remote Control broker receives inbound connections from the controller and the target and tunnels the remote control session data between the two components. The broker is a native service that can be installed on a Windows or a Linux computer. It does not have a default listening port, but 443 is a recommended option because usually this port is open for outbound connections and has fewer issues with content filtering than, for example, 80 would have.

Chapter 2. Definitions

This section defines some common terms used when using IBM Endpoint Manager for Remote Control.

Remote control session
Establishing a connection to a computer in your environment to observe or actively control the computer remotely. In the session the controller user's keyboard and mouse become the primary keyboard and mouse for the remote system. Functionality such as chat, guidance, reboot, and file transfer are some of the options available for use in a remote control session. See the IBM Endpoint Manager for Remote Control Controller User's Guide for more details of the types of session that can be established, the functionality of the controller GUI and the features available within these sessions.

Peer to peer session
A remote control session that is established directly between the controller and the target. The controller user starts the controller component locally and specifies the target that they want to takeover remotely. The local properties that have been set on the target will be used for the session. See "Managing target and server configurations" on page 49 for more information. For details about using the controller GUI once the session is established see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Managed remote control session
A remote control session in which the controller user initiates the session from the IBM Endpoint Manager for Remote Control server. From here the controller component is initiated and contacts the target to send the session request. The target contacts the server to authenticate the request and obtain the policies and permissions that will be set for the session. For more information on policies and permissions for a managed remote control session, see the IBM Endpoint Manager for Remote Control Administrator's Guide. If the target cannot reach the server, the session is refused.

Session policies
Session policies define the actions that can be carried out by the controller user and the features available on the target system during a remote control session. In a peer to peer session these are determined by the local properties defined on the target and in a managed session they are determined by policies and permissions resolved from user and target group relationships. For more information on how policies and permissions are derived for a managed remote control session, see IBM Endpoint Manager for Remote Control Administrator's Guide.

Chapter 3. Using the IBM Endpoint Manager for Remote Control console

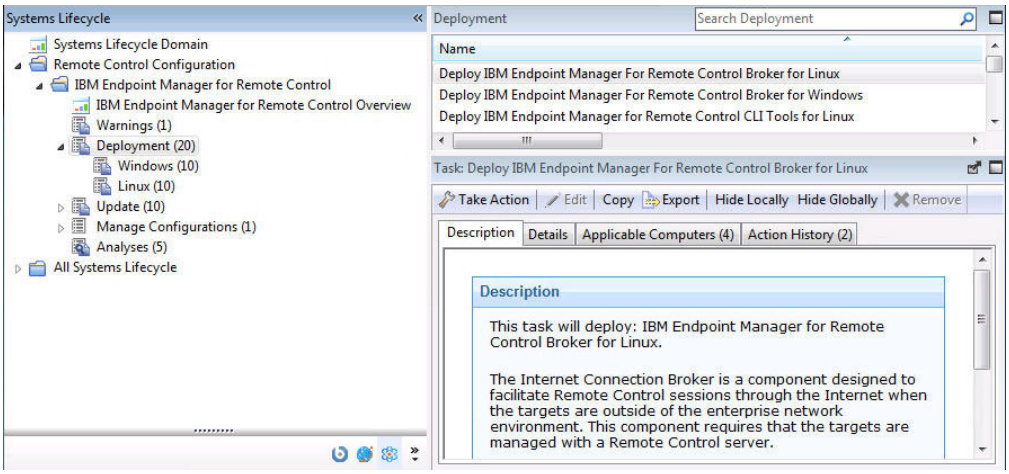
IBM Endpoint Manager for Remote Control encompasses a host of new features that provide the components required for remote takeover and monitoring of workstations and servers in your deployment.

In addition, the IBM Endpoint Manager Console changed after version 7.2 which resulted in several new navigation updates for accessing your data. This section will address how to get around in the new Console. The navigation tree in the IBM Endpoint Manager Console, which is available for all IBM Endpoint Manager products, will serve as your central command for all IBM Endpoint Manager for Remote Control functionality. The navigation tree gives you easy access to all reports, wizards, Fixlet messages, analyses and tasks related to controlling and managing the target machines in your network.

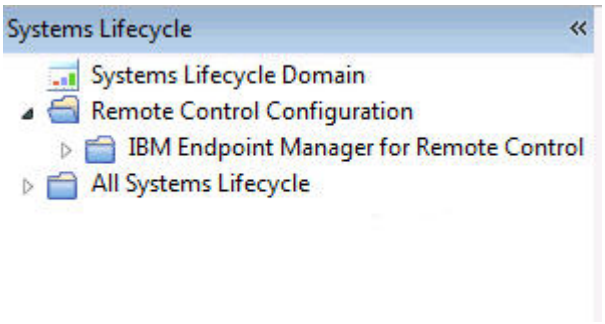
Components

The IBM Endpoint Manager Console organizes content into four parts:

- Domain Panel – Includes navigation tree and list of all domains.
- Navigation Tree – Includes list of nodes and sub-nodes containing site content.
- List Panel – Contains listing of tasks and Fixlets.
- Work Area – Work window where Fixlet and dialogs display.

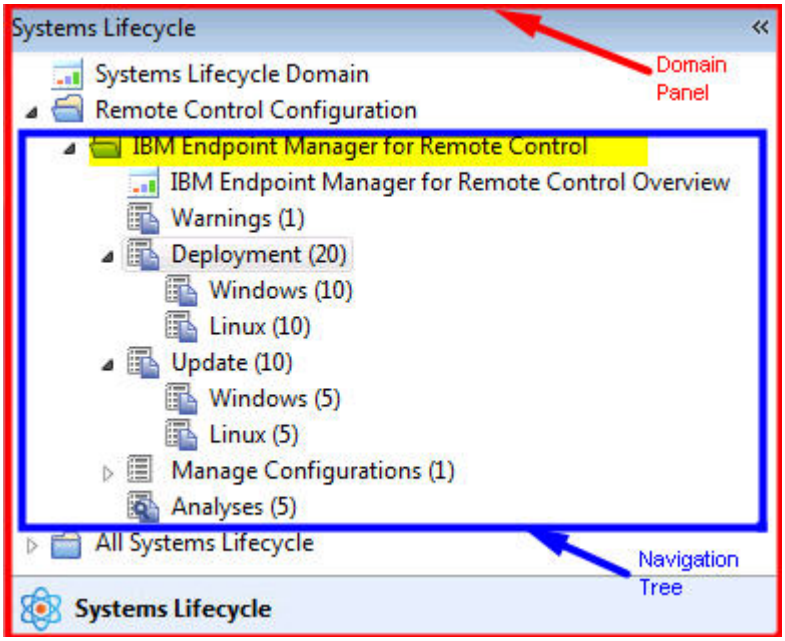


In the context of the IBM Endpoint Manager Console, products or sites are grouped by categories or domains. For example, IBM Endpoint Manager for Remote Control is one of the sites contained within the Systems Lifecycle domain, as part of the Remote Control Configuration node.



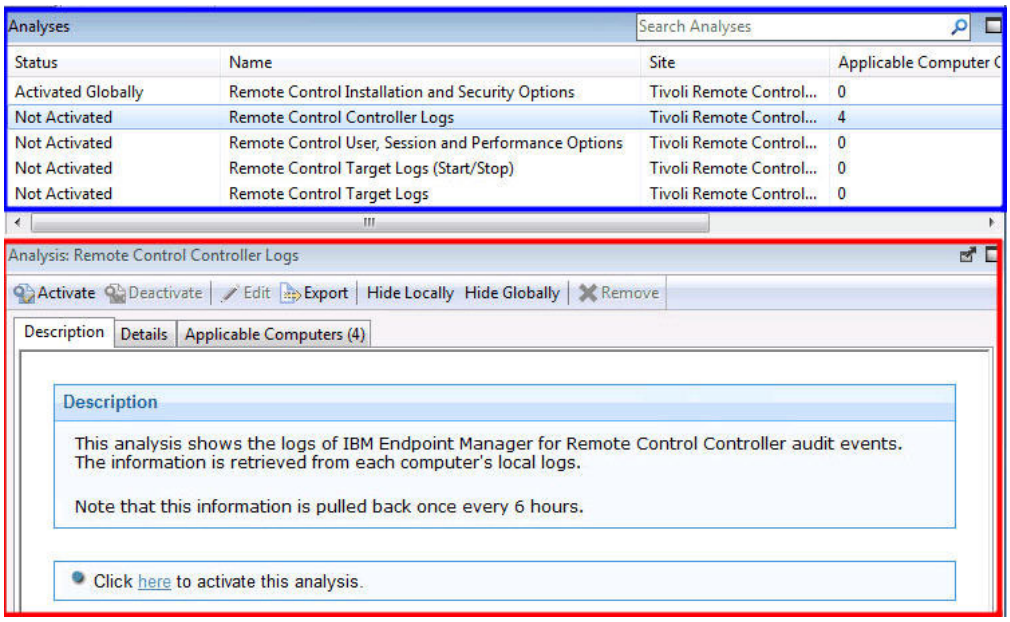
The Domain Panel is the area on the left side of the Console that includes a navigation tree and a list of all domains. The Navigation Tree includes a list of nodes and sub-nodes containing site content.

In the image below, you will see a navigation "tree" at the top with expandable and collapsible nodes, and a list of domains at the bottom. By clicking the Systems Lifecycle domain at the bottom of the domain panel, a list of sites associated with that particular domain will display in the navigation tree at the top.



The red outlined area represents the entire Domain Panel (including the navigation tree and list of domains), and the blue outlined area contains just the Navigation Tree for the IBM Endpoint Manager for Remote Control site.

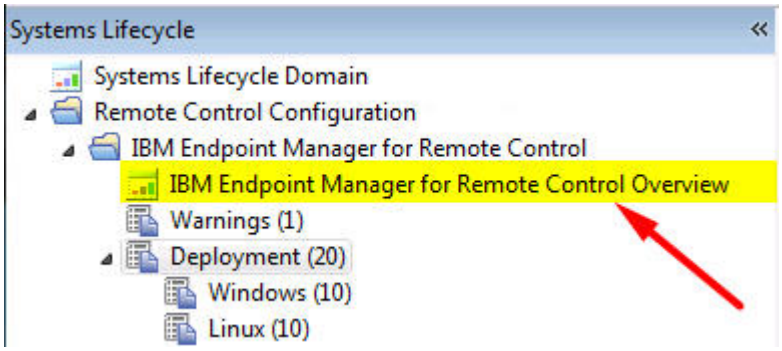
IBM Endpoint Manager for Remote Control tasks are sorted through upper and lower task windows, which are located on the right side of the Console.



The upper panel (blue), called the List Panel , contains columns that sort data according to type, for example, Status, Name, Site, Applicable Computer Count. The lower panel or Work Area (red) presents the fixlet, task screen from which you will be directed to take specific actions to customize the content in your deployment.

Chapter 4. Dashboards overview

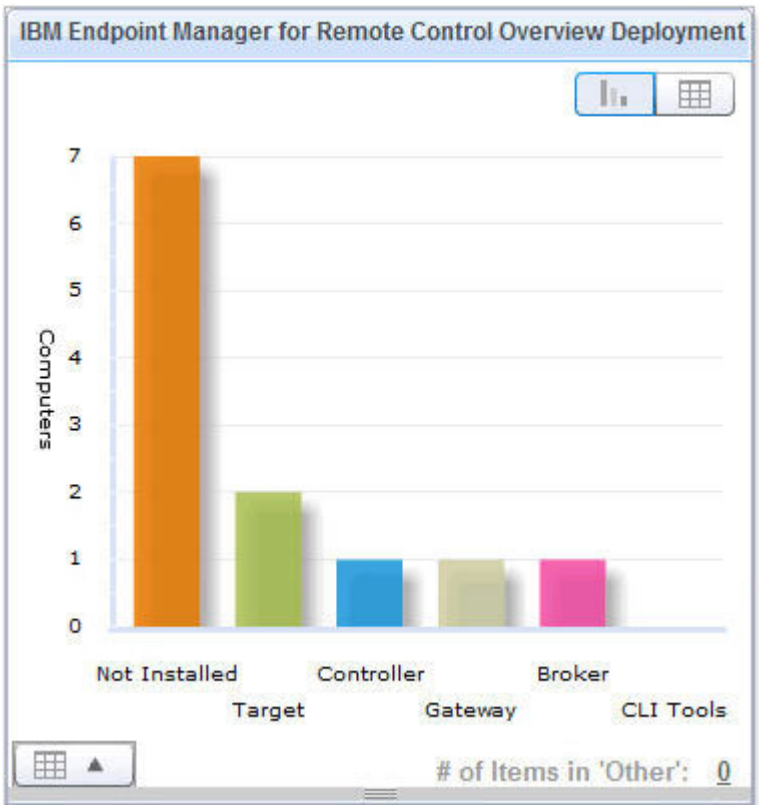
IBM Endpoint Manager for Remote Control offers a convenient dashboard for viewing the deployment distribution of the IBM Endpoint Manager for Remote Control components in your environment and the distribution of the type of target deployment carried out. You can access this dashboard from the top of the IBM Endpoint Manager for Remote Control navigation tree by selecting **IBM Endpoint Manager for Remote Control Overview**.



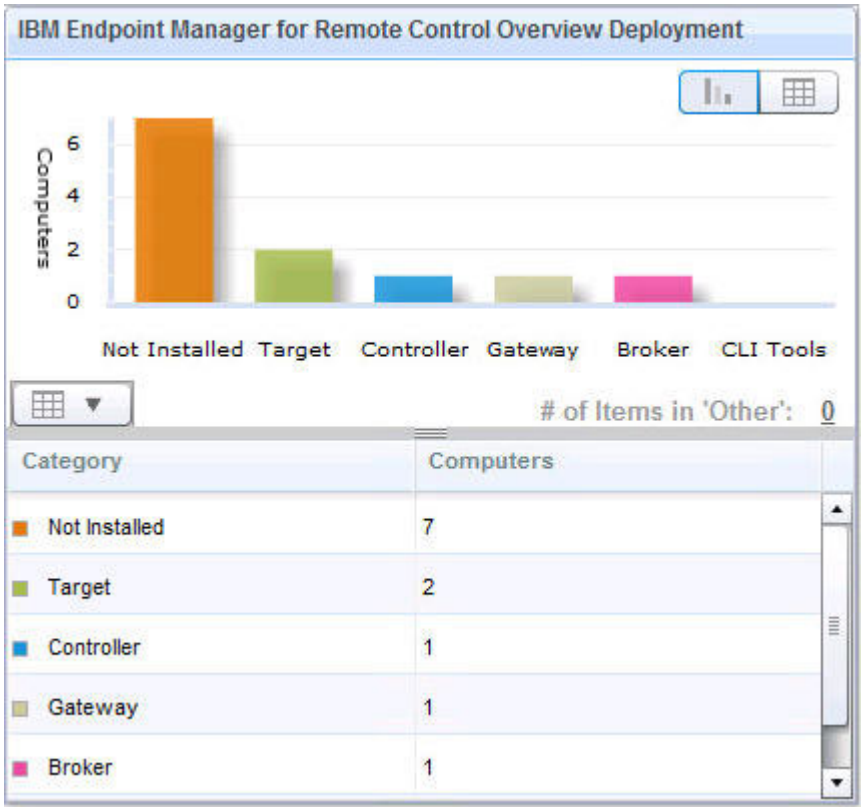
Viewing deployment distribution data

The IBM Endpoint Manager for Remote Control Overview dashboard includes two separate sections showing the deployment distribution of IBM Endpoint Manager for Remote Control and the target deployment type, distribution . Each section is explained below:

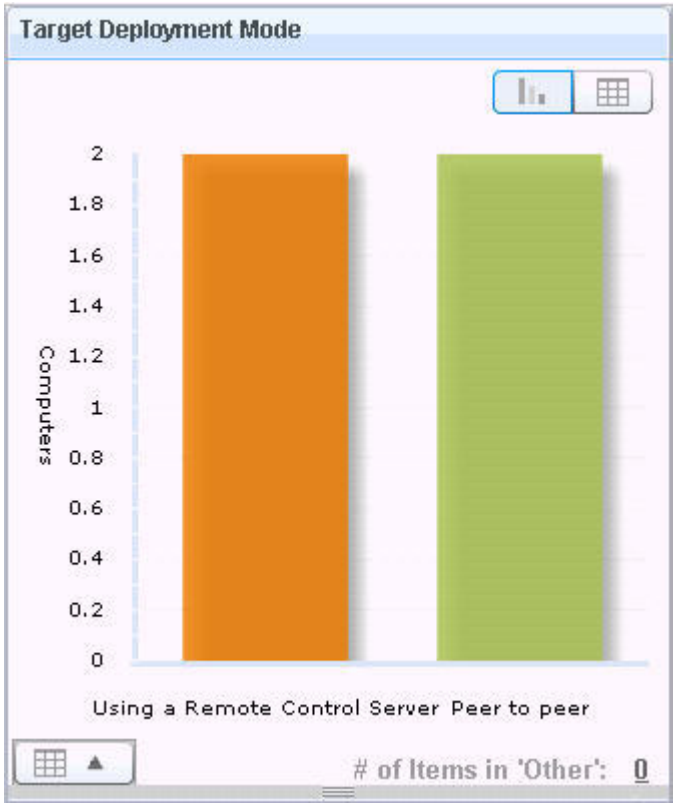
The **IBM Endpoint Manager for Remote Control Overview Deployment** section displays the number of computers in your environment having the various IBM Endpoint Manager for Remote Control components installed. You can view different representations of the data by clicking on the buttons at the top right of the section to display a graphical version or data table version.



You can also view both representations of the data by clicking the button on the bottom left of the graph.



The **Target Deployment Mode** section shows the distribution of the type of target deployment that was carried out, on the computers in your environment which have the IBM Endpoint Manager for Remote Control agent software running. See "Deploying the IBM Endpoint Manager for Remote Control components" on page 13 for details of the different target deployment types. You can view different representations of the data by clicking on the buttons at the top right of the section to display a graphical version or data table version.



Both representations of the data can be viewed using the same instructions as in the previous section.

There are two icons on the top right of the dashboard that you can use for displaying the latest graphical data or for printing the data .

The refresh icon  can be used to display the latest deployment distribution data.

The print icon  can be used to print the dashboard data. The data will be printed to a pdf file that you can save to a specified location for future printing.

Chapter 5. Using IBM Endpoint Manager for Remote Control

The IBM Endpoint Manager for Remote Control navigation tree provides a suite of fixlets, tasks and wizards that you can use for deploying, updating and gathering data from the components required to configure, monitor and control the computers in your environment.

Deploying the IBM Endpoint Manager for Remote Control components

The **Deployment** node in the IBM Endpoint Manager for Remote Control navigation tree provides two sub-nodes which are operating system specific. These sub-nodes provide the components you need to establish a remote control session as well as other utilities that you can use, to connect to targets by using the command line and for installing support for accessing machines on different networks. Select the node which is relevant to your operating system to view a list of tasks that you can use to deploy or remove the required IBM Endpoint Manager for Remote Control components and utilities.

Note: The IBM Endpoint Manager for Remote Control can also be deployed using the installation media. For more details, see the IBM Endpoint Manager for Remote Control Installation Guide.

Controller
The controller component must d be deployed on the computers that will initiate the remote control session when you do not have access to a IBM Endpoint Manager for Remote Control server.

Target The target component must be deployed on the computers that will be controlled during a remote control session. IBM Endpoint Manager for Remote Control offers two ways of deploying the target component depending on how you will establish a connection with the target. Both of these session types are explained in the Chapter 2, “Definitions,” on page 3 section and in more detail in the IBM Endpoint Manager for Remote Control Controller User's Guide.

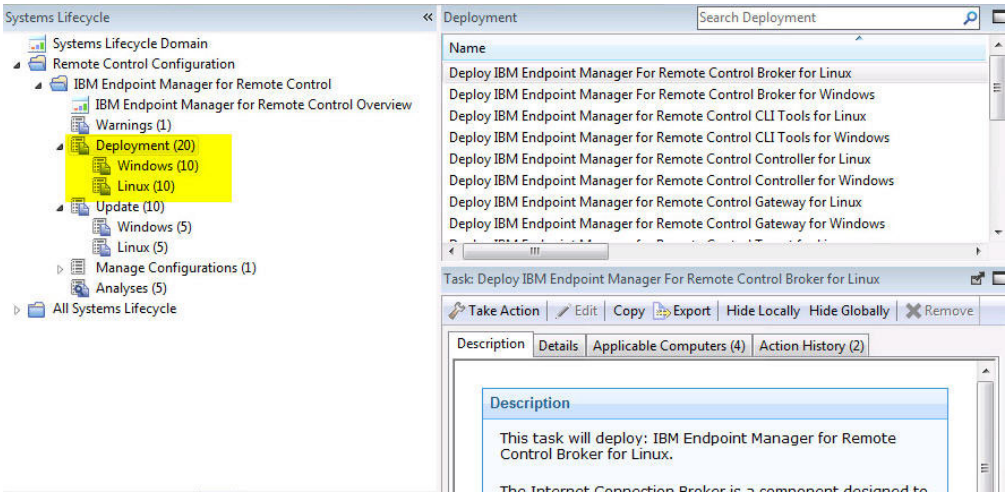
Note: It should be noted that the 'Using the IBM Endpoint Manager for Remote Control server' method requires a IBM Endpoint Manager for Remote Control server to have already been installed in your environment.

CLI tools
The command line tools contain two utilities that can be run from the command line. You can use these utilities to start a remote control session with a target or run commands on a target system without target user interaction. Once installed, these tools can be useful if you want to connect to a target without accessing the IBM Endpoint Manager for Remote Control Server interface or for using as part of a script to run multiple commands in an automated fashion.

Note: To deploy the CLI Tools you need to have the URL of a IBM Endpoint Manager for Remote Control server that you have access to.

Gateway
If you have targets, controllers and severs on different networks that cannot directly contact each other you can install and configure gateway

support. With the gateway support you can configure your network to allow these connections to be established.



Windows deployment

The Windows deployment node provides a set of tasks you can use to install or remove the following components in a Windows environment.

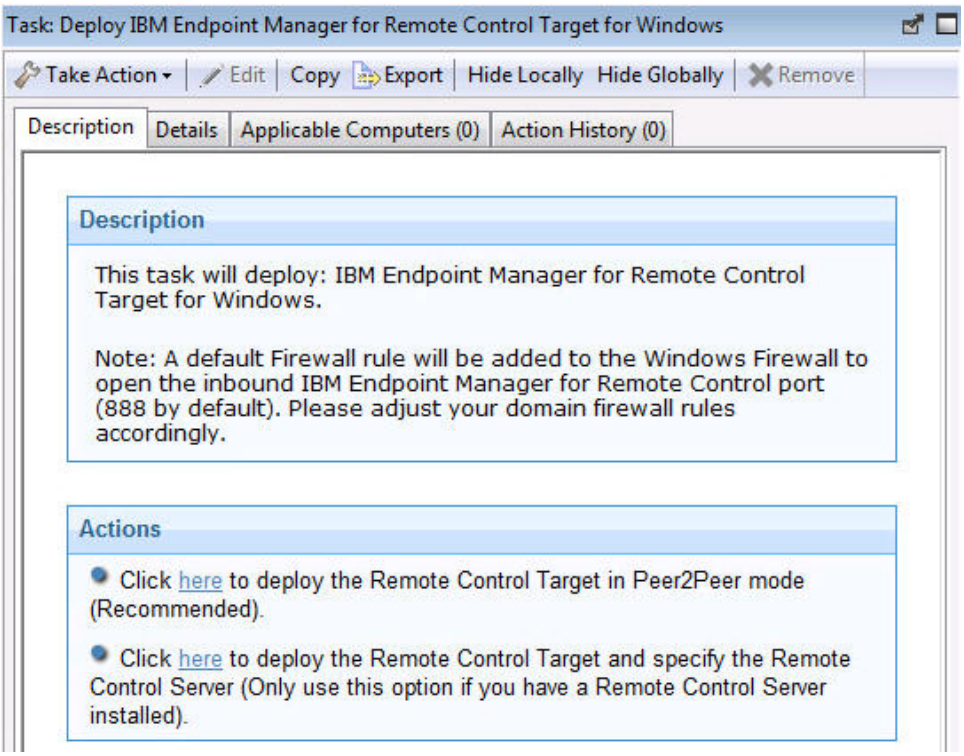
- target and controller software
- CLI tools
- gateway support
- broker support

Deploying the Windows target

You can use the **Deploy IBM Endpoint Manager for Remote Control Target for Windows** task to install the target software onto a Windows computer. To initiate this task complete the following steps:

1. In the navigation tree, click **Deployment** > **Windows**.
2. Click **Deploy IBM Endpoint Manager for Remote Control target for Windows**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.

   There are two actions available for this task. Determine your required installation method and follow the instructions given.



Deploy the remote control target in Peer2Peer mode

With this installation method you can establish remote control sessions directly between the controller and the target without the need for a IBM Endpoint Manager for Remote Control server. This deployment method installs the target without requiring a IBM Endpoint Manager for Remote Control server URL to be specified and the local target policies set by this installation method are used when a remote control session is established. For details of the target installation properties, see "Managing target and server configurations" on page 49.

In the Take Action window on the Target tab, select the required option for determining which targets to deploy the IBM Endpoint Manager for Remote Control target on.

Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

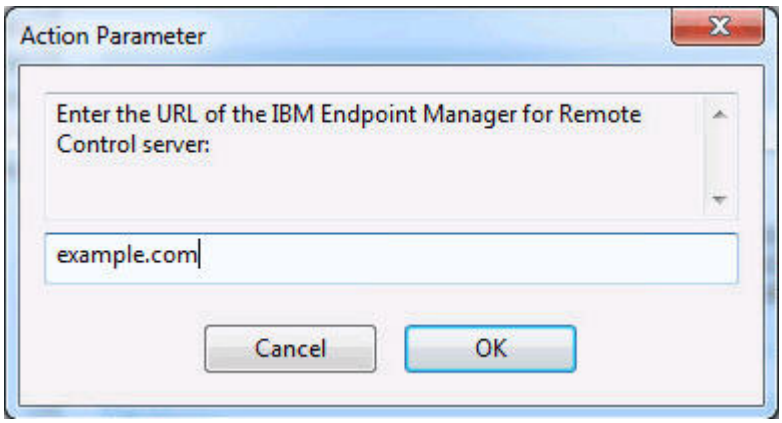
Note: If you want the target to register with the IBM Endpoint Manager for Remote Control server in the future you can use the IBM Endpoint Manager for Remote Control Target Wizard to create a configuration task and specify the server URL of the required server. Running this task on the selected target will re configure it so that it can contact the server. For more details, see "Creating IBM Endpoint Manager for Remote Control target configuration tasks" on page 55.

Deploy the remote control target and specify the IBM Endpoint Manager for Remote Control Server

Chose this installation option for targets to register with the IBM Endpoint Manager for Remote Control server and take part in remote control sessions initiated from the server. This deployment method will require a IBM Endpoint Manager for Remote Control server URL to be

specified. If a remote control session, initiated from the Remote Control server, is requested with this target the specified server will be contacted to authenticate the request. When the request is authenticated, the policies set for the session will be passed from the Remote Control server to the target and the session will be established. See “Managing target and server configurations” on page 49 for details of the target installation properties.

Enter the URL of your IBM Endpoint Manager for Remote Control server and click **OK**.



In the Take Action window on the Target tab, select the required option for determining which targets to deploy the IBM Endpoint Manager for Remote Control target on.

Click **OK** and enter your Private Key Password.

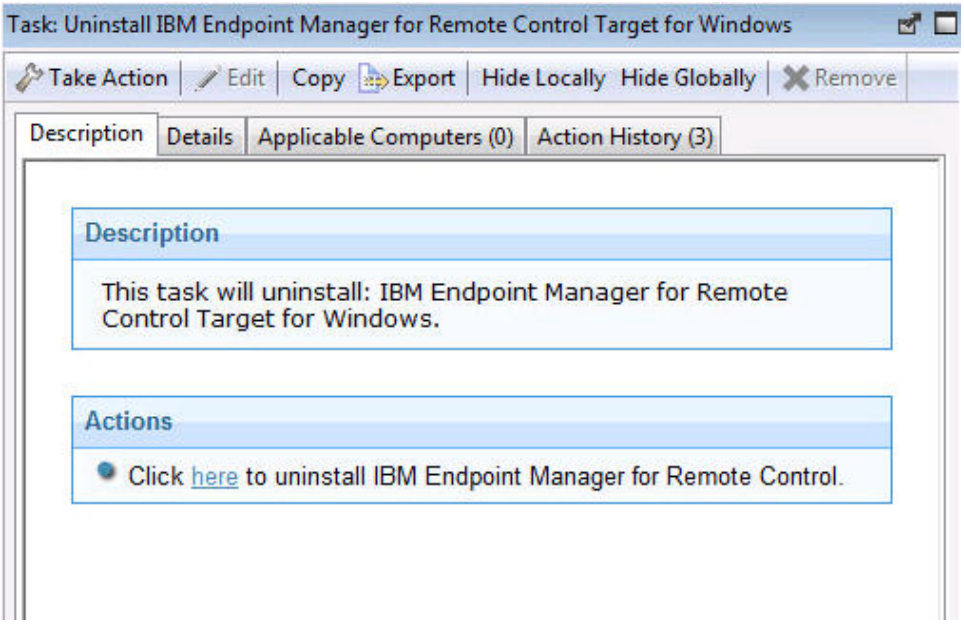
The summary screen will show the progress of the task and will show status complete when it is finished.

Note: This installation option should only be chosen if you have the IBM Endpoint Manager for Remote Control server component installed and running.

Removing the Windows target

You can use the **Uninstall IBM Endpoint Manager for Remote Control Target for Windows** task to remove the target software from a Windows computer which has the target software already installed. To initiate this task complete the following steps:

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control target for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window, on the Target tab, select the required option for determining which targets to remove the IBM Endpoint Manager for Remote Control target from.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

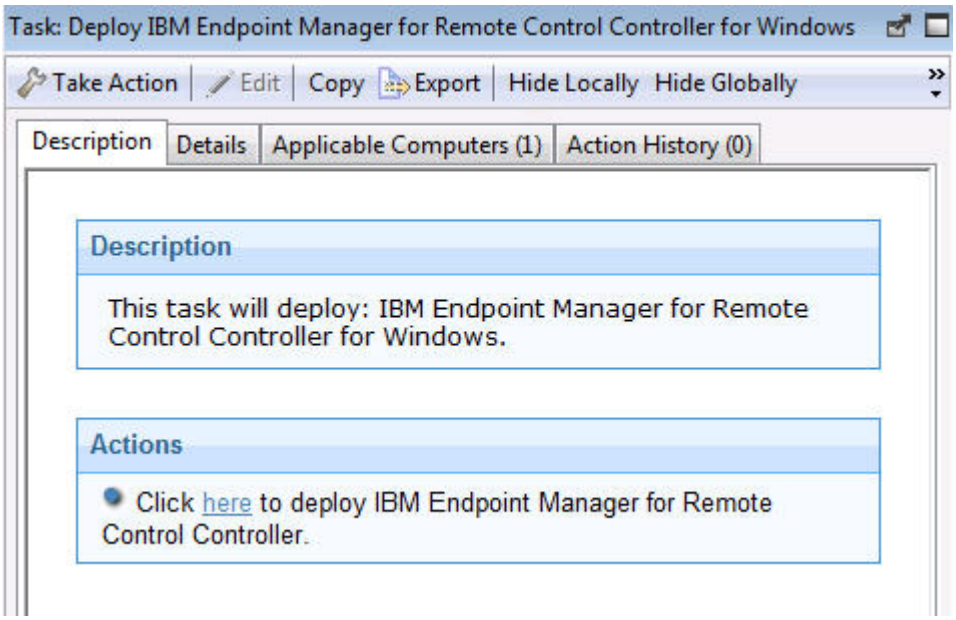
Note: It should be noted that after the removal of the target there might be some files, which were created as part of the normal execution of the target program, that are not deleted automatically. These files are located in `Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control`.

Deploying the Windows controller

You can use the **Deploy IBM Endpoint Manager for Remote Control Controller for Windows** task to install the controller software onto a Windows computer.

Note: If you want to be able to start a remote control session with targets from the IBM Endpoint Manager console, deploy the controller to the same machine as the console is installed on. However it should be noted that when the controller is deployed it is only the current user who is logged on to the machine that you are deploying to that will have the rights to see the menu item that allows you to start a session, it will not be visible to other users.
To initiate this task complete the following steps:

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control Controller for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



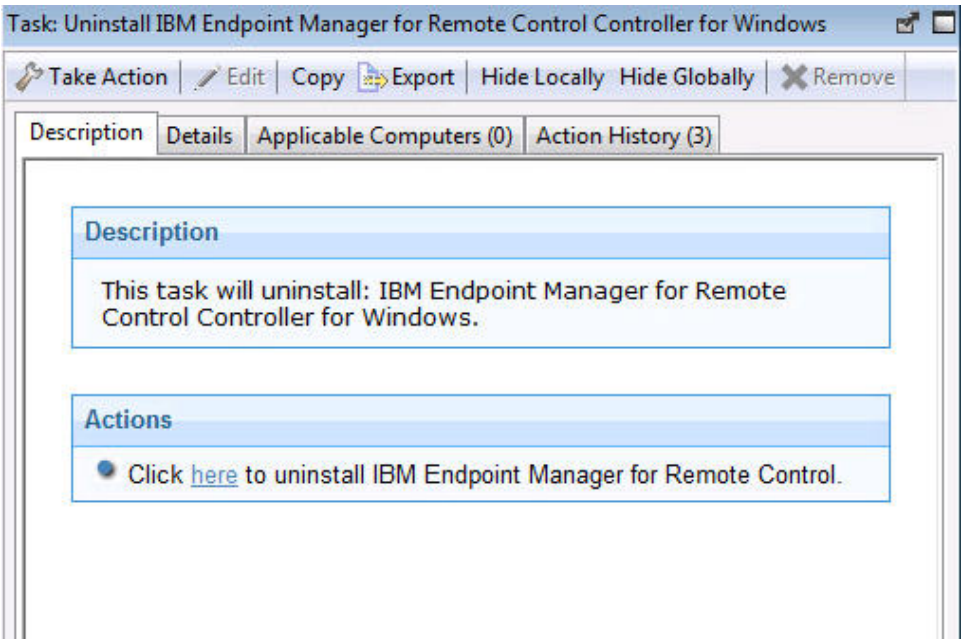
4. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the controller on.
5. Click **OK** and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

Removing the Windows controller

You can use the **Uninstall IBM Endpoint Manager for Remote Control Controller for Windows** task to remove the controller software from a Windows computer which has the controller software already installed. To initiate this task complete the following steps:

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control Controller for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window, in the Target tab, select the required option for determining which targets to remove the IBM Endpoint Manager for Remote Control controller from.
5. Click **OK** and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

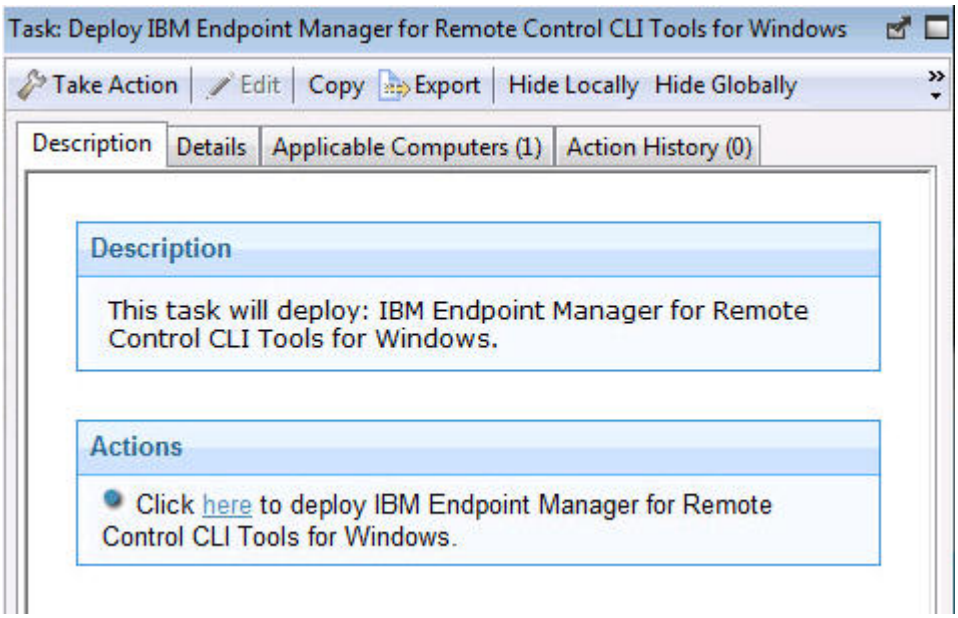
Deploying the Windows CLI tools

You can use the **Deploy IBM Endpoint Manager for Remote Control CLI Tools for Windows** task to install the CLI tools onto a Windows computer. To initiate this task complete the following steps:

Note:

1. You do not need to deploy the CLI tools on any computers that you have deployed the target on as these computers will already have the CLI tools installed along with the target.
2. To deploy this task you need the URL for a IBM Endpoint Manager for Remote Control server that you have access to.

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control CLI Tools for Windows**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. Enter the URL of the IBM Endpoint Manager for Remote Control server and click OK.
5. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the CLI tools on.
6. Click **OK** and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

You should now have the following two CLI utilities installed in the `\Program Files\IBM\tivoli\Remote Control\Target` directory on the targets that were selected when you ran the deployment task.

wrc.exe
: Use this tool to start a remote control session with a target.

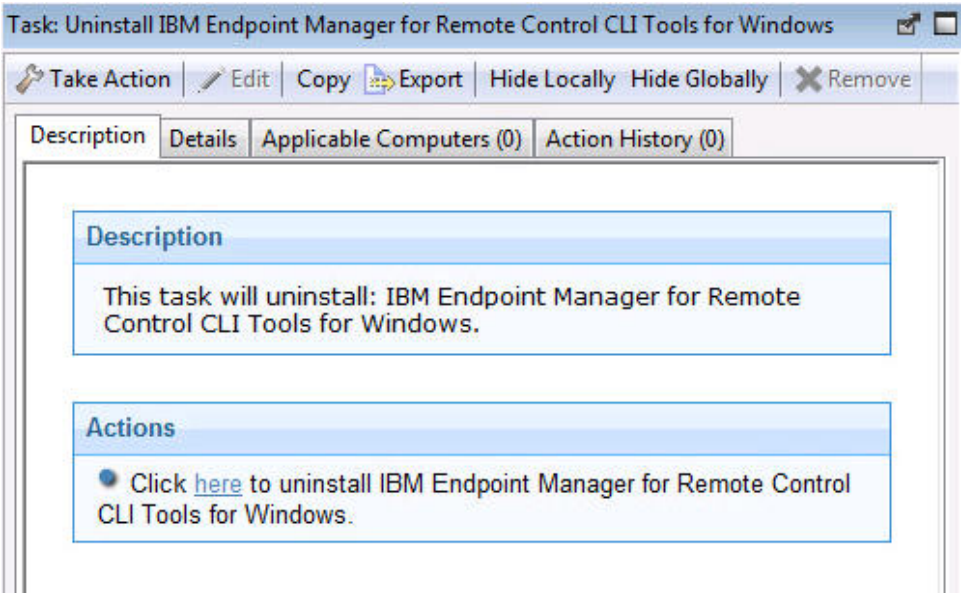
wrcmdpcr.exe
: Use this tool to run a command on a target and see the output from the command on the machine that you issued the command from.

For more details on how to use the command line tools see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Removing the Windows CLI tools

You can use the **Uninstall IBM Endpoint Manager for Remote Control CLI Tools for Windows** task to remove the CLI tools from a Windows computer which has the CLI tools already installed. To initiate this task complete the following steps:

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control CLI Tools for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window, in the Target tab , select the required option for determining which targets to remove the CLI tools from.
5. Click **OK** and enter your Private Key Password.

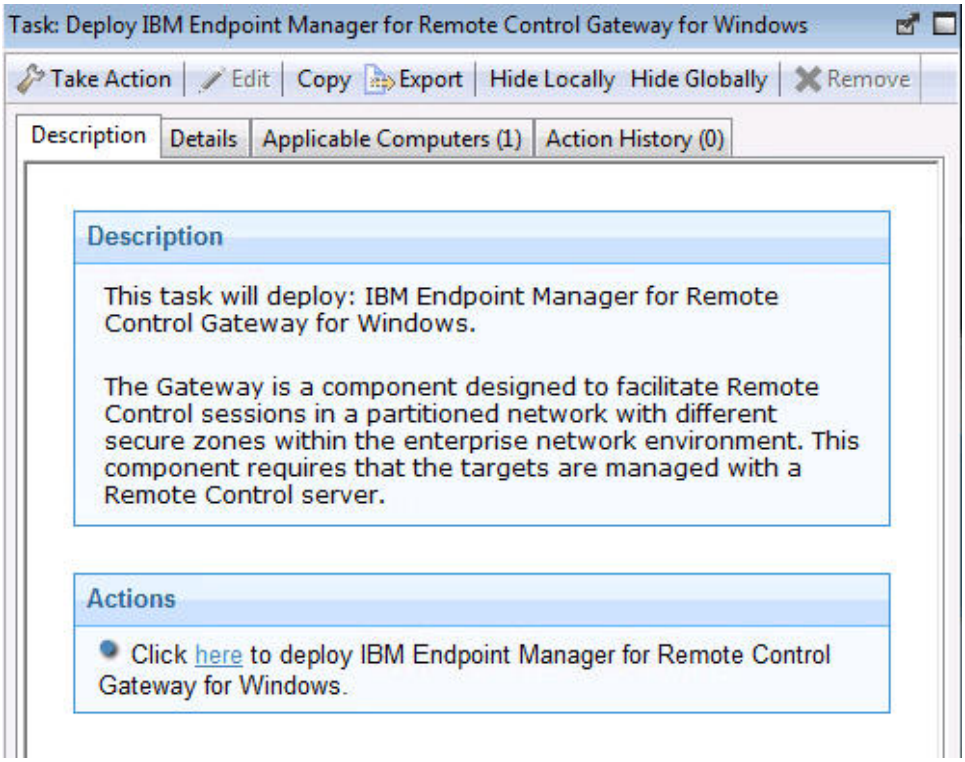
The summary screen will show the progress of the task and will show status complete when it is finished. The CLI tools should no longer be present on the selected targets.

Note: It should be noted that after the removal of the cli tools there could be some files, which were created as part of the normal execution of the cli installation program, that are not deleted automatically. These files are located in `Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control`.

Deploying the Windows gateway support

You can use the **Deploy IBM Endpoint Manager for Remote Control Gateway for Windows** task to install gateway support onto a Windows computer. To initiate this task complete the following steps:

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control Gateway for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the gateway support on.
5. Click **OK** and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

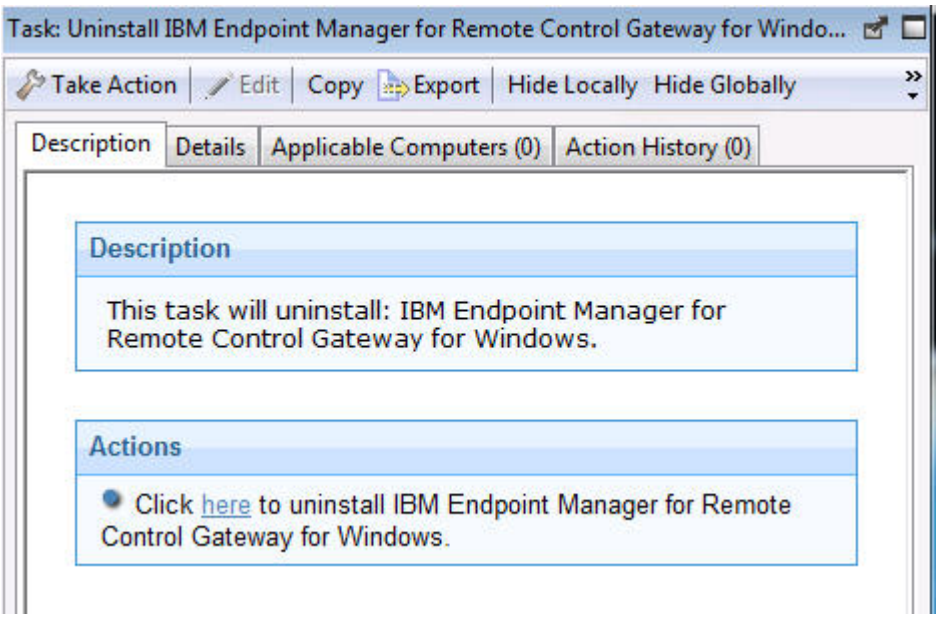
You should now have gateway support installed on the targets that were selected when you ran the deployment task. The files for this have been installed in the `\Program Files\IBM\tivoli\Remote Control\Gateway` directory on the selected targets.

To make use of the gateway support you will need to setup a gateway configuration for your environment. For more details see the IBM Endpoint Manager for Remote Control Administrator's Guide

Removing the Windows gateway support

You can use the **Uninstall IBM Endpoint Manager for Remote Control Gateway support for Windows** task to remove the gateway support files from a Windows computer which has these files already installed. To initiate this task complete the following steps:

1. Click **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control Gateway for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window, in the Target tab , select the required option for determining which targets to remove the gateway support from.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

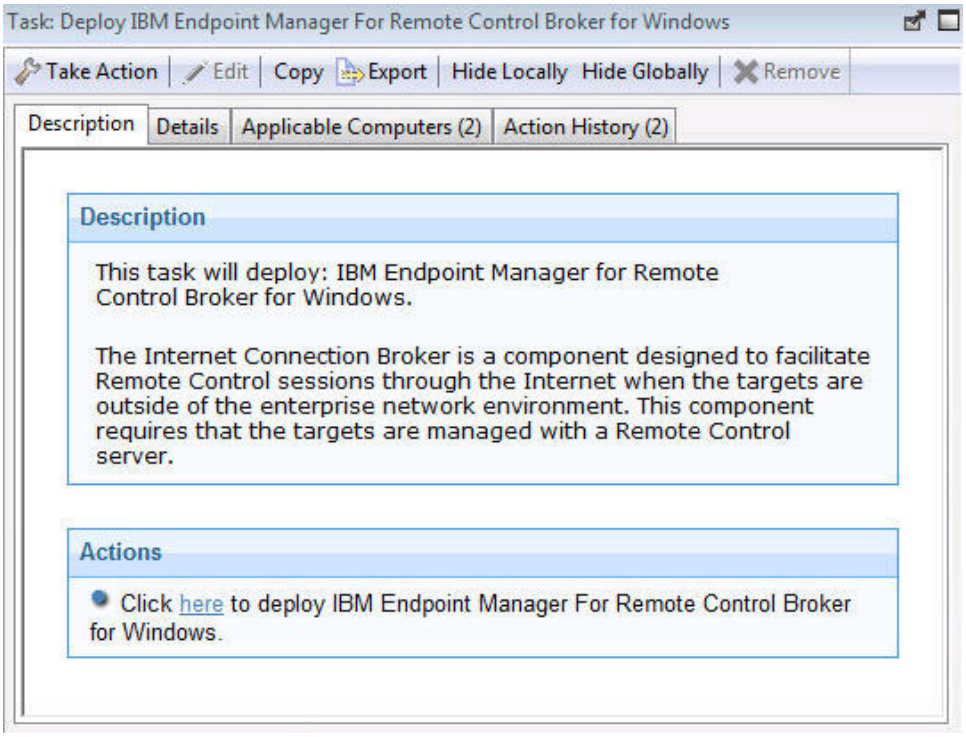
The gateway support files should no longer be present on the selected targets.

Deploying Windows broker support

You can use the Deploy IBM Endpoint Manager for Remote Control Broker for Windows task to install broker support on a Windows computer

To initiate this task complete the following steps:

1. Click on **Deployment** > **Windows** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control Broker for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the broker support on.
5. Click **OK** and enter your Private Key Password.

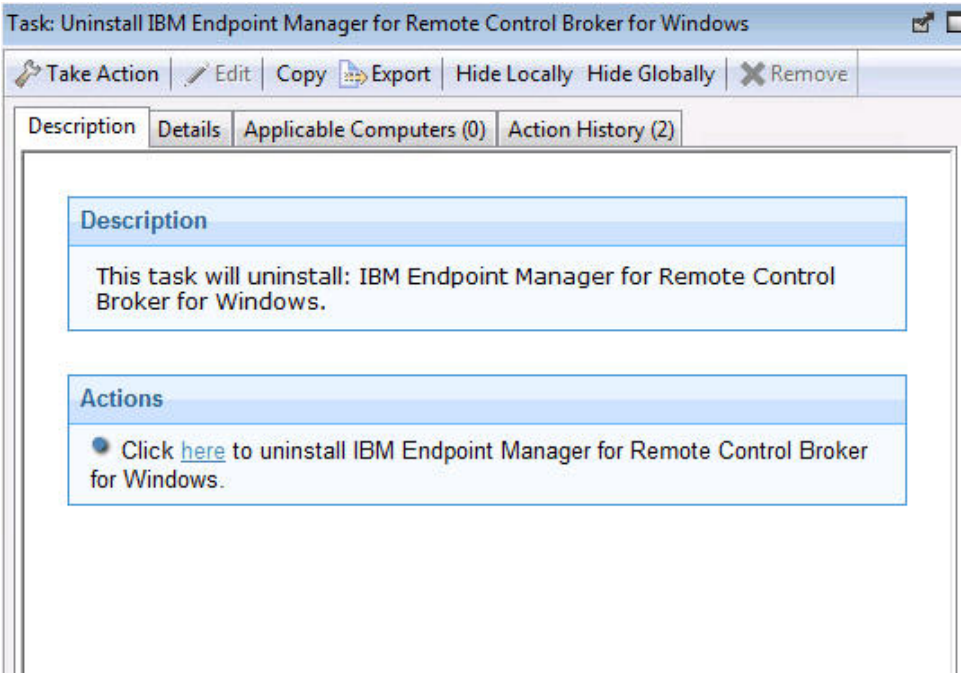
The summary screen will show the progress of the task and will show status complete when it is finished. You should now have broker support installed on the targets that were selected when you ran the deployment task. The files for this will have been installed in the *[working dir]*`\Broker` directory on the selected targets, where *[working dir]* is determined by the version of Windows that you are installing the broker support on. For example `C:\Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control`. To make use of the broker support you will need to setup a broker configuration for your environment. For more details see the IBM Endpoint Manager for Remote Control Administrator's Guide.

Removing Windows broker support

You can use the Uninstall IBM Endpoint Manager for Remote Control Broker for Windows task to remove broker support from a Windows computer

To initiate this task complete the following steps:

1. Click on **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control Broker for Windows** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to remove the broker support from.
5. Click **OK** and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished. The broker support files will have been removed from the chosen targets.

Linux deployment

The Linux deployment node provides a set of tasks that you can use to install or remove the following components in a Linux environment.

- target and controller software
- CLI tools
- gateway support
- broker support

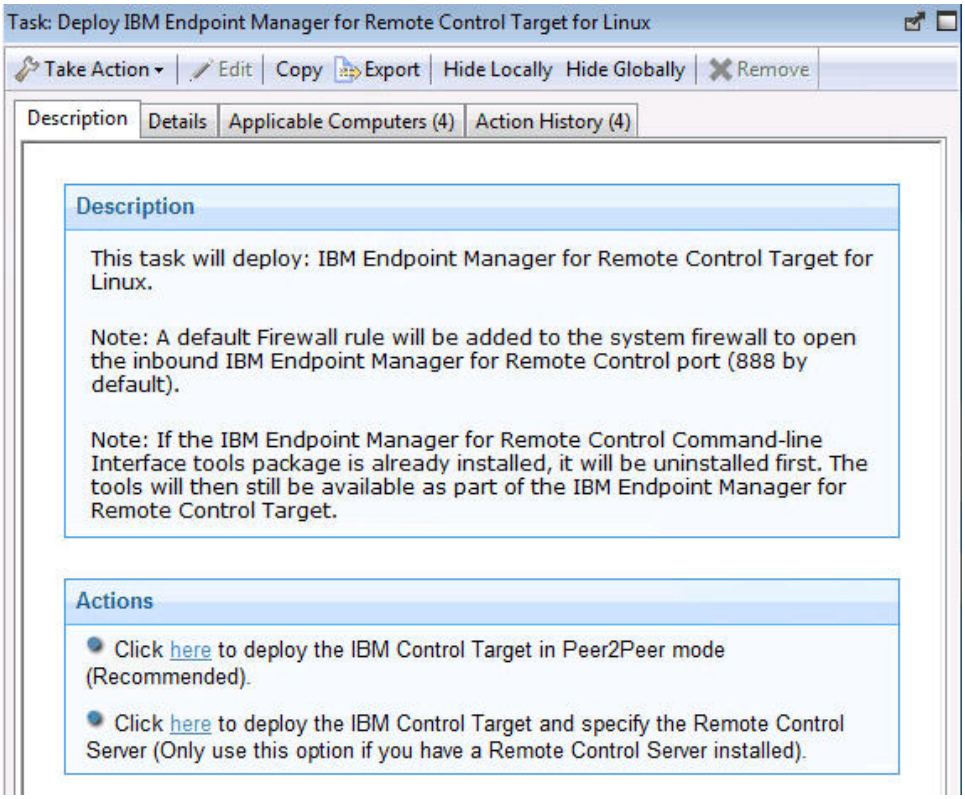
Note: If you are installing the target, cli and gateway components on a Red Hat 6.0 64 bit machine the following libraries along with their dependencies, need to be installed if they are not already installed. For all: glibc.i686 and additionally for the target component: libXmu.i686, libXi.i686, libXtst.i686.

Deploying the Linux target

You can use the **Deploy IBM Endpoint Manager for Remote Control Target for Linux** task to install the target software onto a Linux computer. To initiate this task complete the following steps:

1. Click **Deployment** > **Linux** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control target for Linux** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.

   There are two actions available for this task. Determine your required installation method and follow the instructions given.



Deploy the remote control target in Peer2Peer mode

With this installation method you can establish remote control sessions directly between the controller and the target without the need for a IBM Endpoint Manager for Remote Control server. This deployment method installs the target without requiring a IBM Endpoint Manager for Remote Control server URL to be specified and the local target policies set by this installation method are used when a remote control session is established. See “Managing target and server configurations” on page 49 for details of the target installation properties.

In the Take Action window on the Target tab, select the required option for determining which targets to deploy the IBM Endpoint Manager for Remote Control target on.

Click OK and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

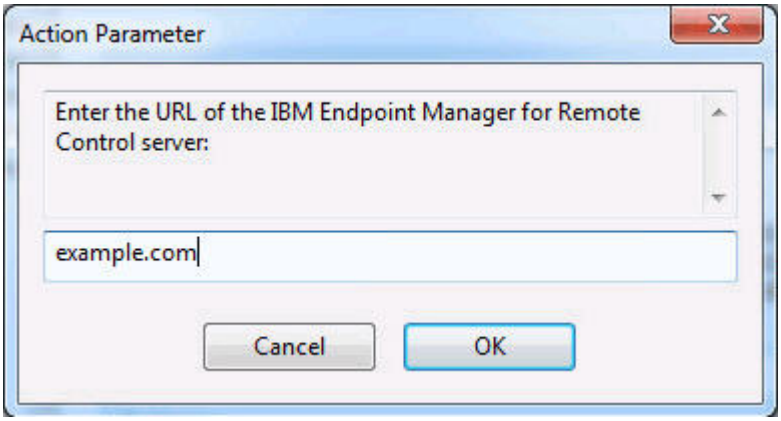
Note: If you want the target to register with the IBM Endpoint Manager for Remote Control server in the future you can use the IBM Endpoint Manager for Remote Control Target Wizard to create a configuration task and specify the server URL of the required server. Running this task on the selected target will re configure it so that it can contact the server. See “Creating IBM Endpoint Manager for Remote Control target configuration tasks” on page 55.

Deploy the remote control target and specify the IBM Endpoint Manager for Remote Control Server

Choose this installation option for targets to register with the IBM Endpoint Manager for Remote Control server and take part in remote control sessions initiated from the server. This deployment method will

require a IBM Endpoint Manager for Remote Control server URL to be specified. If a remote control session, initiated from the Remote Control server, is requested with this target the specified server will be contacted to authenticate the request. When the request is authenticated, the policies set for the session are passed from the Remote Control server to the target and the session is established. For details of the target installation properties, see "Managing target and server configurations" on page 49.

Enter the URL of your IBM Endpoint Manager for Remote Control server and click OK.



In the Take Action window on the Target tab, select the required option for determining which targets to deploy the IBM Endpoint Manager for Remote Control target on.

Click OK and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

Note: This installation option should only be chosen if you have the IBM Endpoint Manager for Remote Control server component installed and running.

Removing the Linux target

You can use the **Uninstall IBM Endpoint Manager for Remote Control Target for Linux** task to remove the target software from a Linux computer which has the target software already installed. To initiate this task complete the following steps:

1. Click **Deployment** > **Linux** > in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control target for Linux**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.

4. In the Take Action window, on the Target tab, select the required option for determining which targets to remove the IBM Endpoint Manager for Remote Control target from.
5. Click **OK** and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

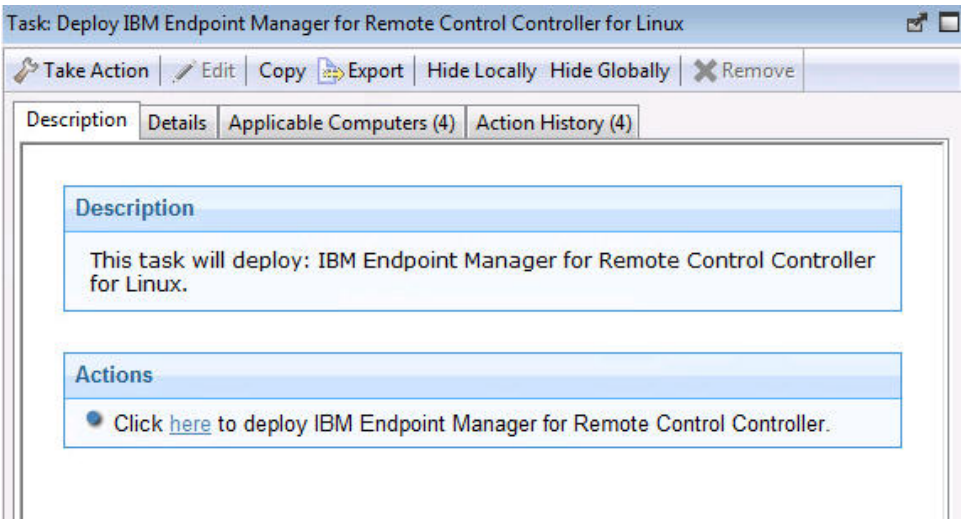
Note: It should be noted that after the removal of the target there might be some files, which were created as part of the normal execution of the target program, that are not deleted automatically. These files are located in the following directories `/opt/ibm` and `/var/opt/ibm/trc/target`.

Deploying the Linux controller

You can use the **Deploy IBM Endpoint Manager for Remote Control Controller for Linux** task to install the controller software onto a Linux computer.

Note: If you are installing the controller on a Red Hat 6.0 64 bit machine you require the following additional libraries, along with all their dependencies, to be installed: libXft.i686 libXmu.i686 libXp.i686 libXtst.i686 .
To initiate this task complete the following steps:

1. Click **Deployment** > **Linux** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control Controller for Linux** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



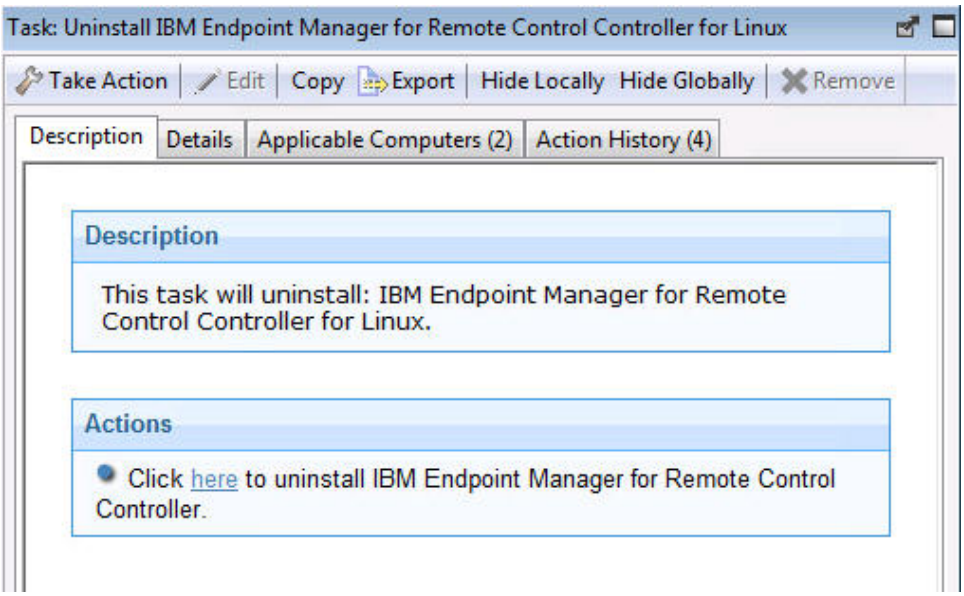
4. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the controller on.
5. Click OK and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

Removing the Linux controller

You can use the **Uninstall IBM Endpoint Manager for Remote Control Controller for Linux** task to remove the controller software from a Linux computer which has the controller software already installed. To initiate this task complete the following steps:

1. Click **Deployment** > **Linux** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control Controller for Linux** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window, in the Target tab, select the required option for determining which targets to remove the IBM Endpoint Manager for Remote Control controller from.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

Deploying the Linux CLI tools

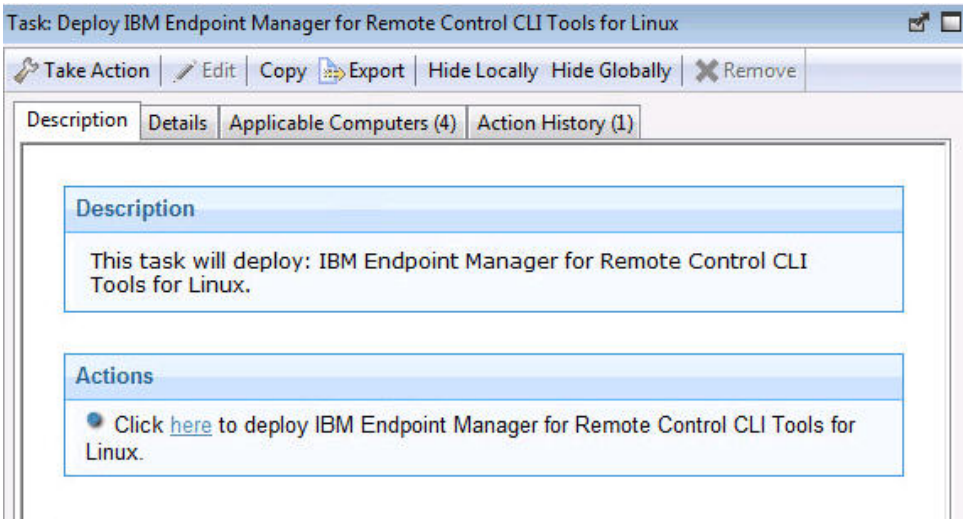
You can use the **Deploy IBM Endpoint Manager for Remote Control CLI Tools for Linux** task to install the CLI tools onto a Linux computer.

Note:

1. You do not need to deploy the CLI tools on any computers that you have deployed the target on as these computers will already have the CLI tools installed along with the target.
2. In order to deploy this task you need the URL for a IBM Endpoint Manager for Remote Control server that you have access to.

To initiate this task complete the following steps:

1. Click **Deployment** > **Linux** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control CLI Tools for Linux**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. Enter the URL of the IBM Endpoint Manager for Remote Control server and click **OK**
5. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the CLI tools on.
6. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

You should now have the following two CLI utilities installed in the `/opt/IBM/trc/target` directory on the targets that were selected when you ran the deployment task.

wrc Use this tool to start a remote control session with a target.

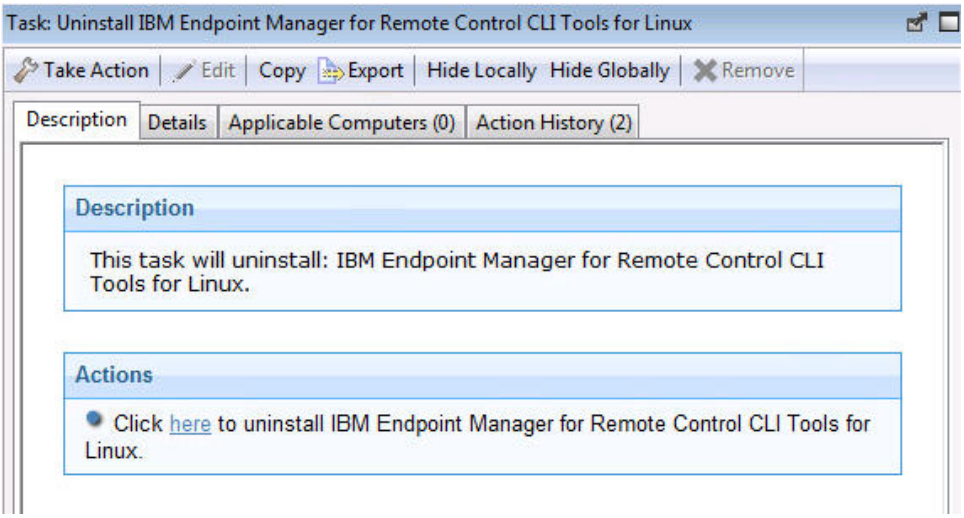
wrcmdpcr
Use this tool to run a command on a target and see the output from the command on the machine that you issued the command from.

For more details on how to use the command line tools see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Removing the Linux CLI tools

You can use the **Uninstall IBM Endpoint Manager for Remote Control CLI Tools for Linux** task to remove the CLI tools from a Linux computer which has the CLI tools already installed. To initiate this task complete the following steps:

1. Click on **Deployment** > **Linux** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control CLI Tools for Linux** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window, in the Target tab, select the required option for determining which targets to remove the CLI tools from.
5. Click **OK** and enter your Private Key Password.

The summary screen will show the progress of the task and will show status complete when it is finished.

The CLI tools should no longer be present on the selected targets.

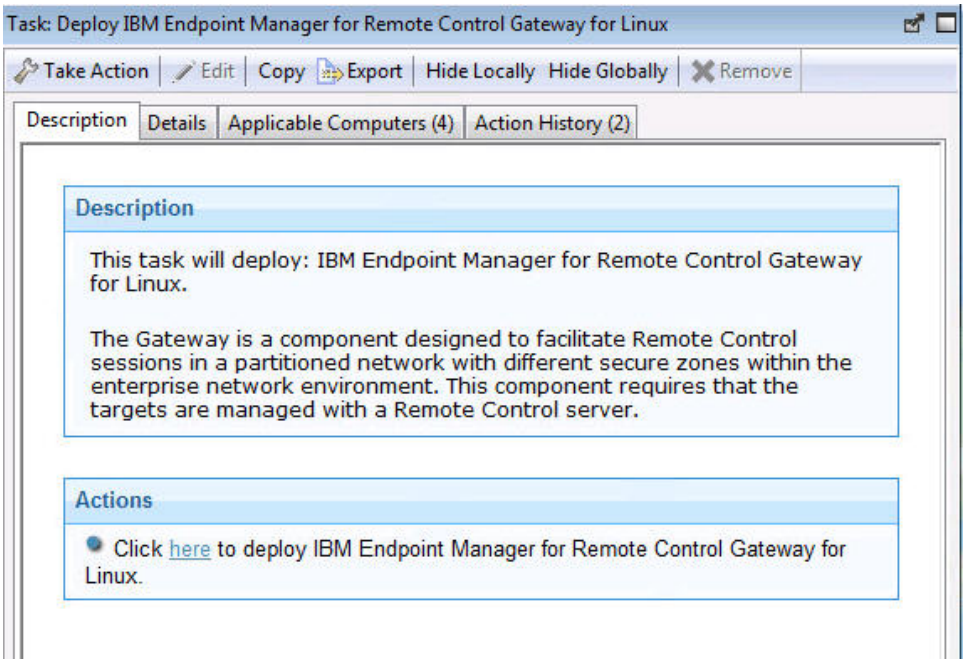
Note: It should be noted that after the removal of the CLI tools there might be some files, which were created as part of the normal execution of the CLI tools program, that are not deleted automatically. These files are located in the following directories `/etc`, `/opt/ibm`, `/var/opt/ibm/trc/cli` and `/var/opt/ibm/trc/target`.

Deploying the Linux gateway support

You can use the **Deploy IBM Endpoint Manager for Remote Control Gateway for Linux** task to install gateway support onto a Linux computer. To initiate this task complete the following steps:

1. Click **Deployment** > **Linux** in the navigation tree.

2. Click **Deploy IBM Endpoint Manager for Remote Control Gateway for Linux** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the gateway support on.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

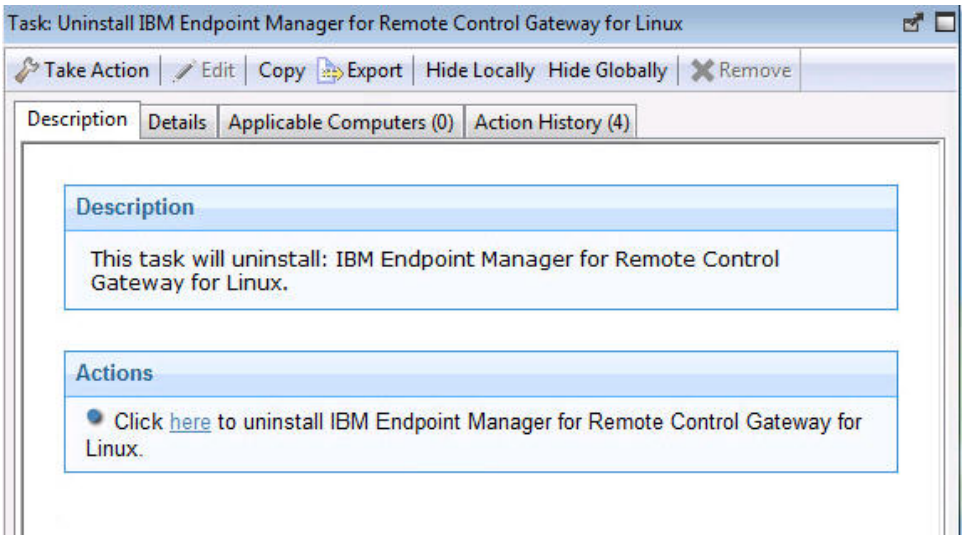
You should now have gateway support installed on the targets that were selected when you ran the deployment task. The files for this will have been installed to the `/opt/IBM/trc/gateway` directory on the selected targets.

To make use of the gateway support you will need to setup a gateway configuration for your environment. See the IBM Endpoint Manager for Remote Control Administrator's Guide.

Removing the Linux gateway support

You can use the **Uninstall IBM Endpoint Manager for Remote Control Gateway support for Linux** task to remove the gateway support files from a Linux computer which has these files already installed. To initiate this task complete the following steps:

1. Click **Deployment** > **Linux** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control Gateway for Linux** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window, in the Target tab, select the required option for determining which targets to remove the gateway support from.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

The gateway support should no longer be present on the selected targets.

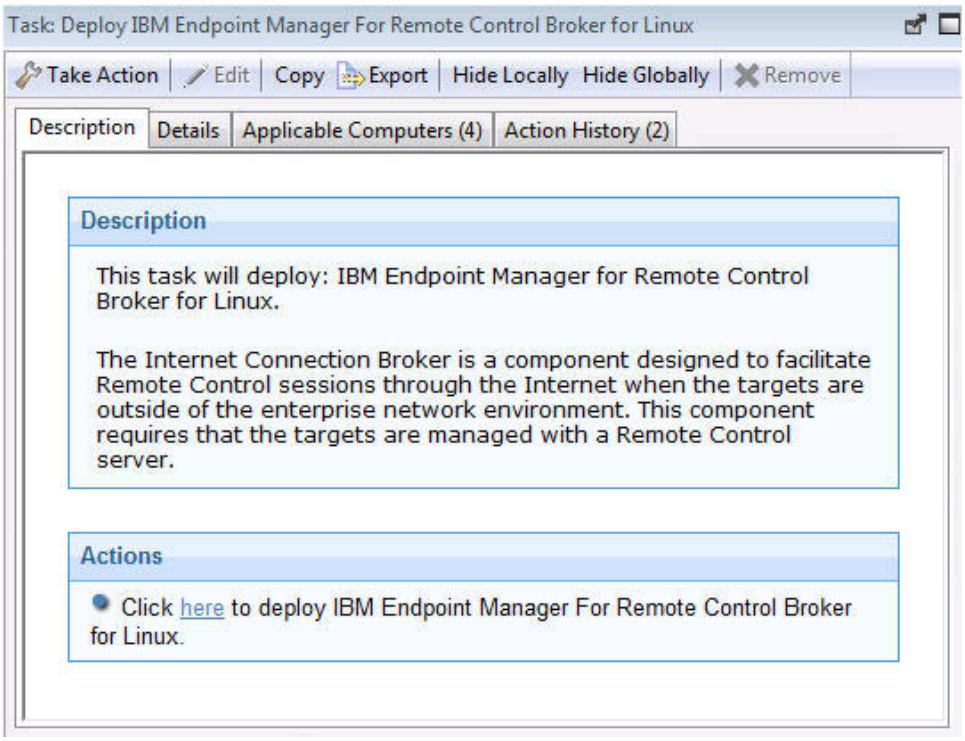
Note: It should be noted that after the removal of the gateway support there might be some files, which were created as part of the normal execution of the gateway support program, that are not deleted automatically. These files are located in `/opt/ibm` and `/var/opt/ibm/trc/gateway` .

Deploying Linux broker support

You can use the Deploy IBM Endpoint Manager for Remote Control Broker for Linux task to install broker support on a Linux computer.

To initiate this task complete the following steps:

1. Click on **Deployment** > **Linux** in the navigation tree.
2. Click **Deploy IBM Endpoint Manager for Remote Control Broker for Linux**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to deploy the broker support on.
5. Click **OK** and enter your Private Key Password.

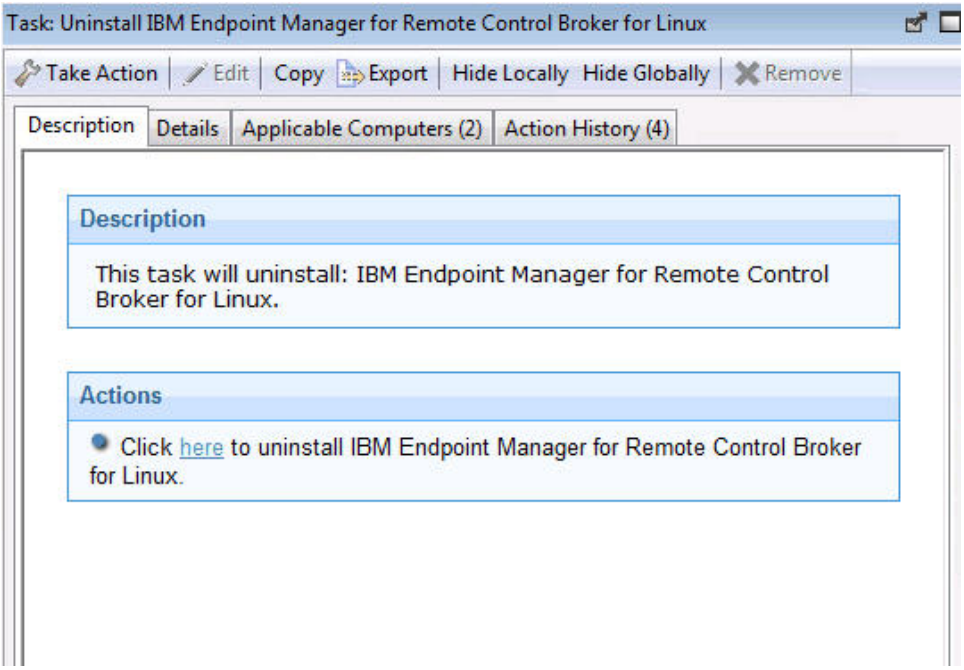
The summary screen will show the progress of the task and will show status complete when it is finished. You should now have broker support installed on the targets that were selected when you ran the deployment task. The files for this will have been installed in the `/opt/IBM/trc/broker` directory on the selected targets. To make use of the broker support you will need to setup a broker configuration for your environment. For more details see the IBM Endpoint Manager for Remote Control Administrator's Guide.

Removing Linux broker support

You can use the Uninstall IBM Endpoint Manager for Remote Control Broker for Linux task to remove broker support from a Linux computer

To initiate this task complete the following steps:

1. Click on **Deployment** > **Linux** in the navigation tree.
2. Click **Uninstall IBM Endpoint Manager for Remote Control Broker for Linux**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.

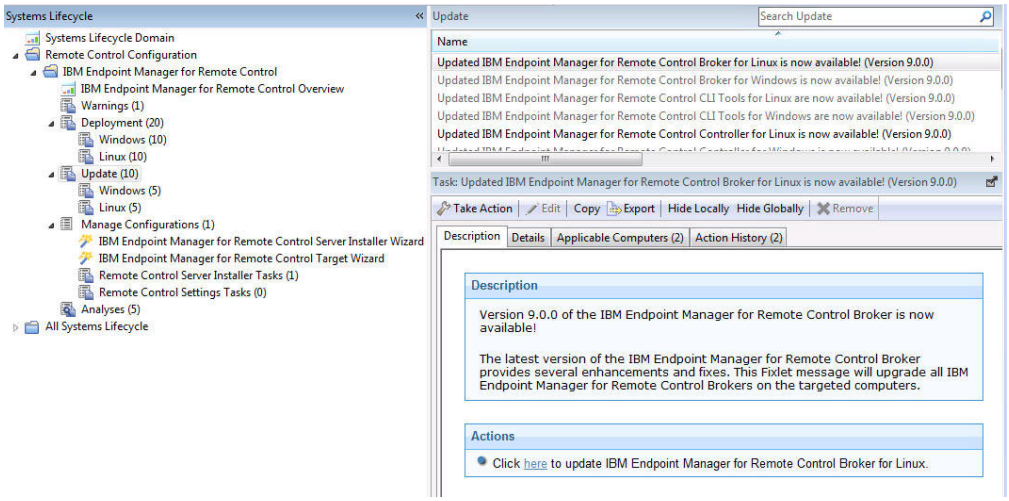


4. In the Take Action window on the Target tab, select the required option for determining which targets to remove the broker support from.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished. The broker support files is removed from the chosen targets.

Updating IBM Endpoint Manager for Remote Control components

The **Update** node in the IBM Endpoint Manager for Remote Control navigation tree provides two sub-nodes which are operating system specific. These sub-nodes provide the latest levels of the target and controller components. If you have an older version of the IBM Endpoint Manager for Remote Control target and controller components already installed in your environment use the **Update** node to upgrade these components to a newer version. Select the relevant operating system node to view a list of tasks that you can use to upgrade the relevant IBM Endpoint Manager for Remote Control components.



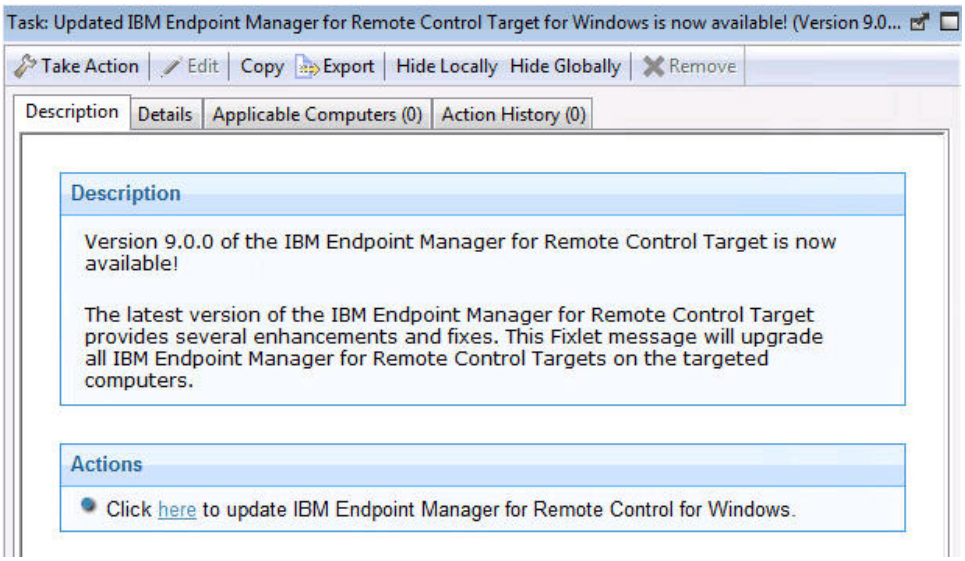
Updating Windows components

The **Windows** sub-node provides the latest levels of IBM Endpoint Manager for Remote Control component software for use in a windows environment. These components contain the latest enhancements and fixes that have been applied to IBM Endpoint Manager for Remote Control.

Updating the Windows target

You can use the windows tasks to update the target software, on a Windows computer. These tasks will install any new enhancements and fixes that have been applied to the chosen version whilst keeping the same target configuration currently installed. For example: choose the version 9.0.0 task to keep your current target configuration and apply any new enhancements or fixes contained in version 9.0.0, to that. To initiate this task complete the following steps:

1. Click **Updates** > **Windows** in the navigation tree.
2. Select the required windows target update. For example: **Updated IBM Endpoint Manager for Remote Control Target for Windows is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the target update on.
5. Click **OK** and enter your Private Key Password.

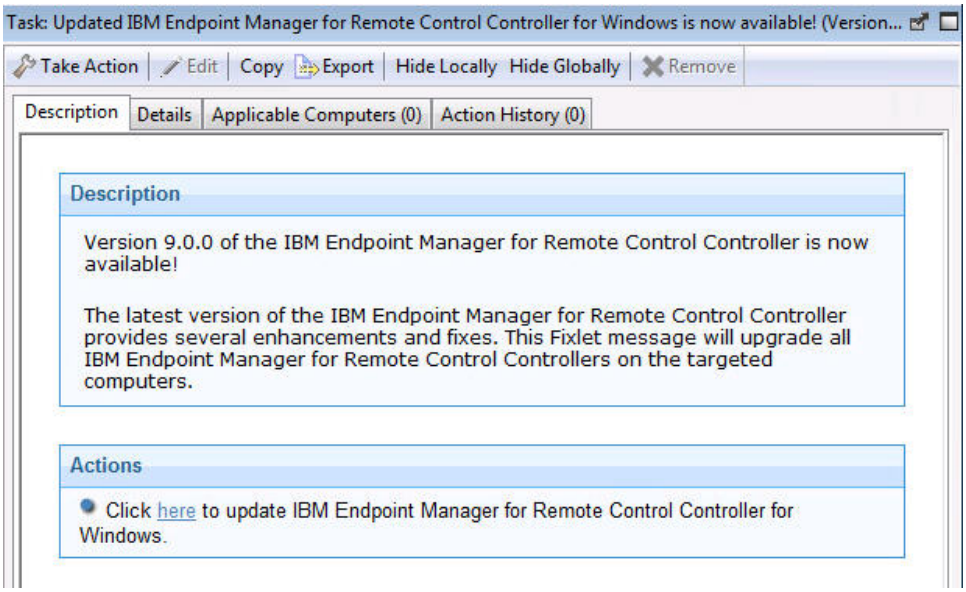
The summary screen shows the progress of the task and displays status complete when it is finished.

The selected targets are upgraded to the version of target software applicable to the chosen update.

Updating the Windows controller

Use the windows tasks to update the controller software, on a Windows computer. These tasks will upgrade your currently installed controller to the version that the task applies to. For example: choose the version 9.0.0 task will apply any new enhancements or fixes, contained in the version 9.02.0 controller to your current controller. To initiate this task complete the following steps:

1. Click **Updates** > **Windows** in the navigation tree.
2. Select the required windows controller update. For example: **Updated IBM Endpoint Manager for Remote Control Controller for Windows is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the controller update on.
5. Click **OK** and enter your Private Key Password.

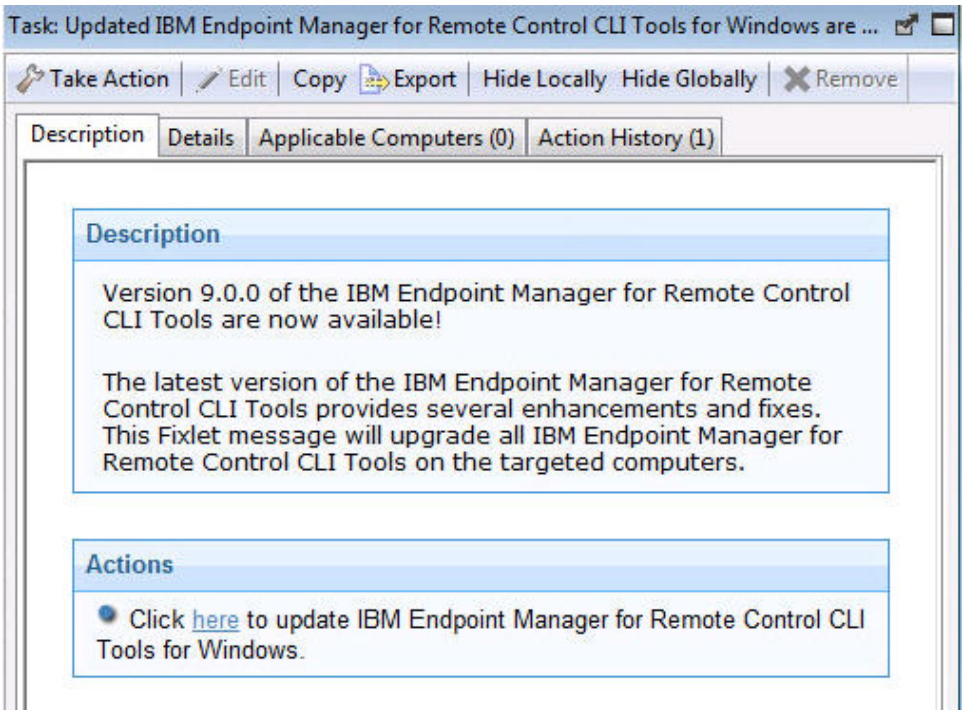
The summary screen shows the progress of the task and displays status complete when it is finished.

The controller software on the selected targets is upgraded to the version of the chosen update.

Updating the Windows command line tools

Use the windows tasks to update the cli tools, on a Windows computer. These tasks will install any new enhancements and fixes that have been applied to the chosen version whilst keeping the same cli tools configuration currently installed. For example: choose the version 9.0.0 task to keep your current cli tools configuration and apply any new enhancements or fixes contained in version 9.0.0, to that. To initiate this task complete the following steps:

1. Click **Updates** > **Windows** in the navigation tree.
2. Select the required windows cli update. For example: **Updated IBM Endpoint Manager for Remote Control CLI tools for Windows is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the cli update on.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

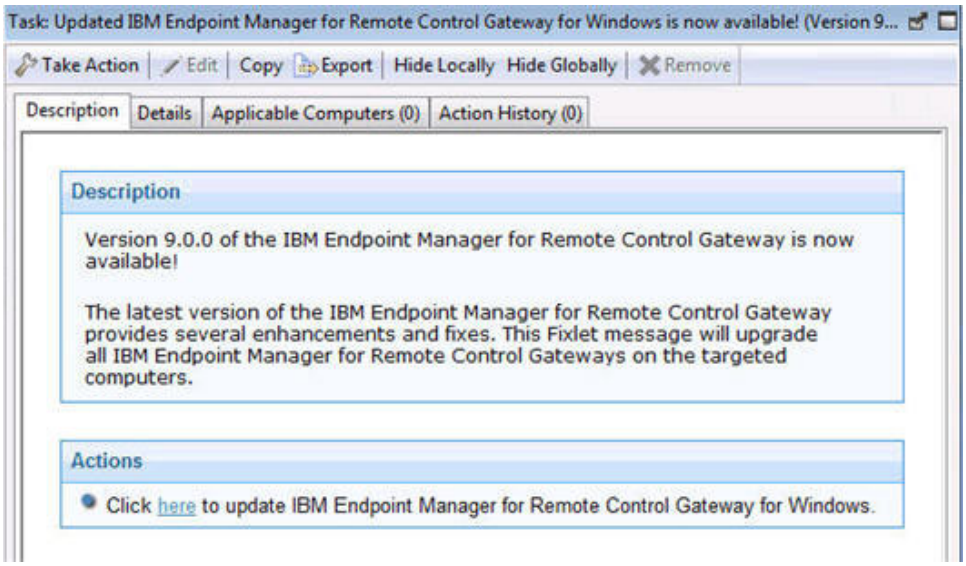
The cli tools on the selected targets are upgraded to the version of the chosen update.

Updating the Windows gateway support

Use the windows tasks to update the gateway support files, on a Windows computer. These tasks install any new enhancements and fixes that have been applied to the chosen version whilst keeping the same gateway configuration currently installed. For example: choose the version 9.0.0 task to keep your current gateway

configuration and apply any new enhancements or fixes contained in version 9.0.0, to that. To initiate this task complete the following steps:

1. Click **Updates** > **Windows** in the navigation tree.
2. Select the required windows gateway update. For example: **Updated IBM Endpoint Manager for Remote Control Gateway for Windows is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the gateway update on.
5. Click **OK** and enter your Private Key Password.

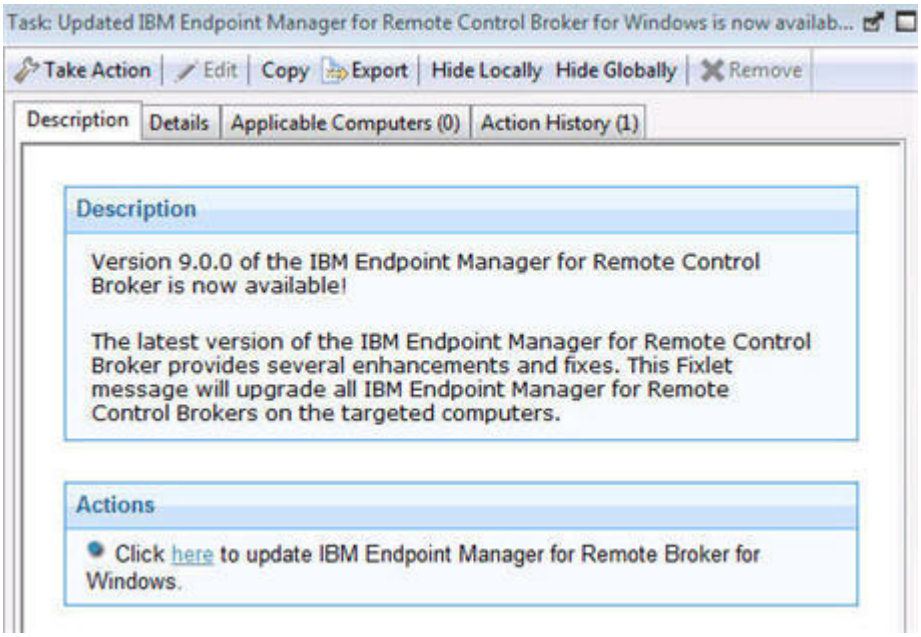
The summary screen shows the progress of the task and displays status complete when it is finished.

The gateway support on the selected targets is upgraded to the version of the chosen update.

Updating the Windows broker support

You can use the windows tasks to update the broker software, on a Windows computer. These tasks will upgrade your currently installed broker support files to the version that the task applies to. For example: choose the version 9.0.0 task to apply any new enhancements or fixes, contained in the version 9.0.0 broker to your current broker files. To initiate this task complete the following steps:

1. Click **Updates** > **Windows** in the navigation tree.
2. Select the required windows broker update. For example: **Updated IBM Endpoint Manager for Remote Control Broker for Windows is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the broker update on.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

The broker software on the selected targets is upgraded to the version of the chosen update.

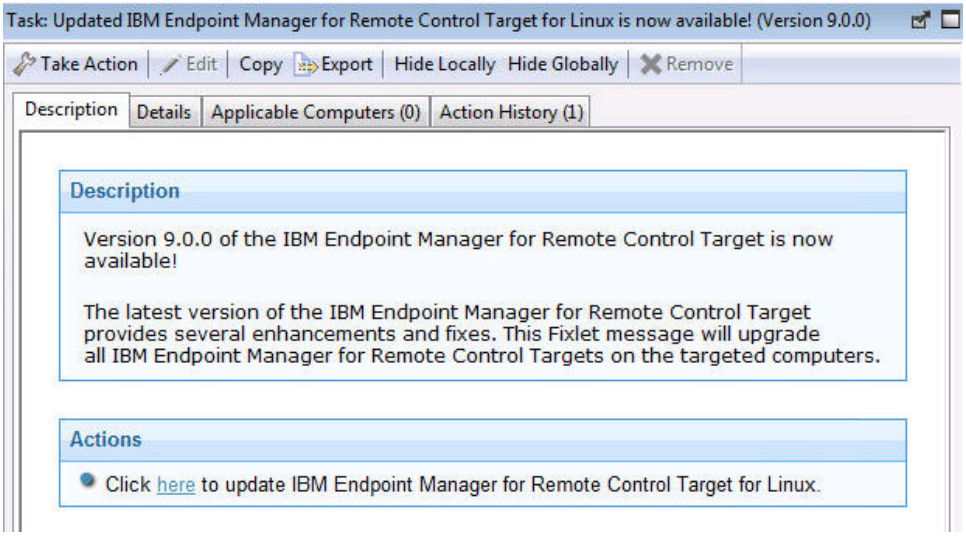
Updating Linux components

The Linux sub-node provides the latest levels of IBM Endpoint Manager for Remote Control component software for use in a Linux environment. These components contain the latest enhancements and fixes that have been applied to IBM Endpoint Manager for Remote Control.

Updating the Linux target

You can use the linux tasks to update the target software, on a Linux computer. These tasks will install any new enhancements and fixes that have been applied to the chosen version whilst keeping the same target configuration currently installed. For example: choosing the version 9.0.0 task will keep your current target configuration and apply any new enhancements or fixes, contained in version 9.0.0, to that. To initiate this task complete the following steps:

1. Click **Updates** > **Linux** in the navigation tree.
2. Select the required linux target update. For example: **Updated IBM Endpoint Manager for Remote Control Target for Linux is now available! (Version 9.0.0)** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



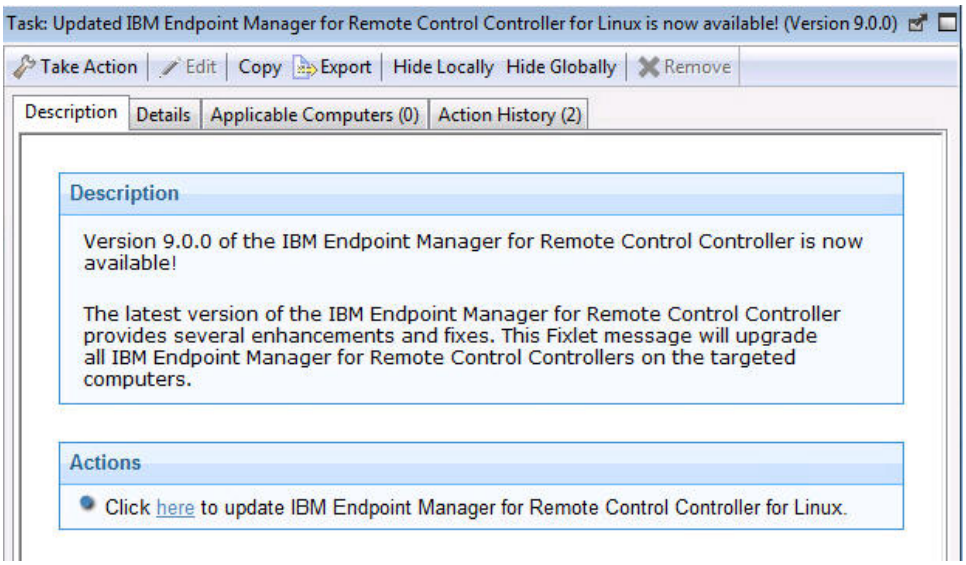
4. In the Take Action window on the Target tab, select the required option for determining which targets to install the target update on.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

Updating the Linux controller

You can use the linux tasks to update the controller software, on a Linux computer. These tasks upgrade your currently installed controller to the version that the task applies to. For example: choosing the version 9.0.0 task will apply any new enhancements or fixes, contained in the version 9.0.0 controller to your current controller. To initiate this task complete the following steps:

1. Click **Updates** > **Linux** in the navigation tree.
2. Select the required linux controller update. For example: **Updated IBM Endpoint Manager for Remote Control Controller for Linux is now available! (Version 9.0.0)** .
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



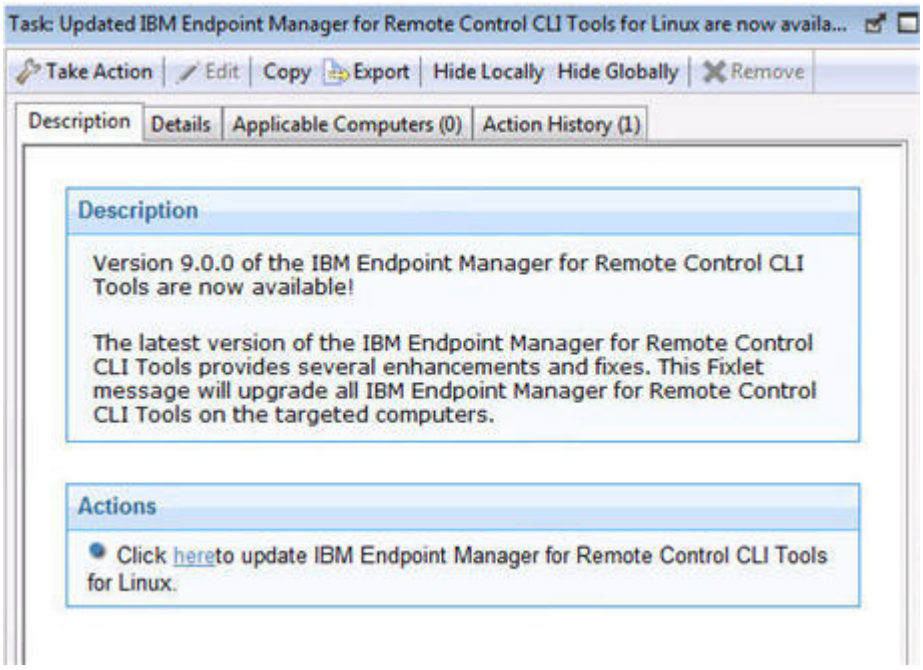
4. In the Take Action window on the Target tab, select the required option for determining which targets to install the controller update on.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished. The controller software on the selected targets is upgraded to the version of the chosen update.

Updating the Linux command line tools

Use the Linux tasks to update the cli tools, on a Linux computer. These tasks will install any new enhancements and fixes that have been applied to the chosen version whilst keeping the same cli tools configuration currently installed. For example: choose the version 9.0.0 task to keep your current cli tools configuration and apply any new enhancements or fixes contained in version 9.0.0, to that. To initiate this task complete the following steps:

1. Click **Updates** > **Linux** in the navigation tree.
2. Select the required Linux cli update. For example: **Updated IBM Endpoint Manager for Remote Control CLI tools for Linux is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the cli update on.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

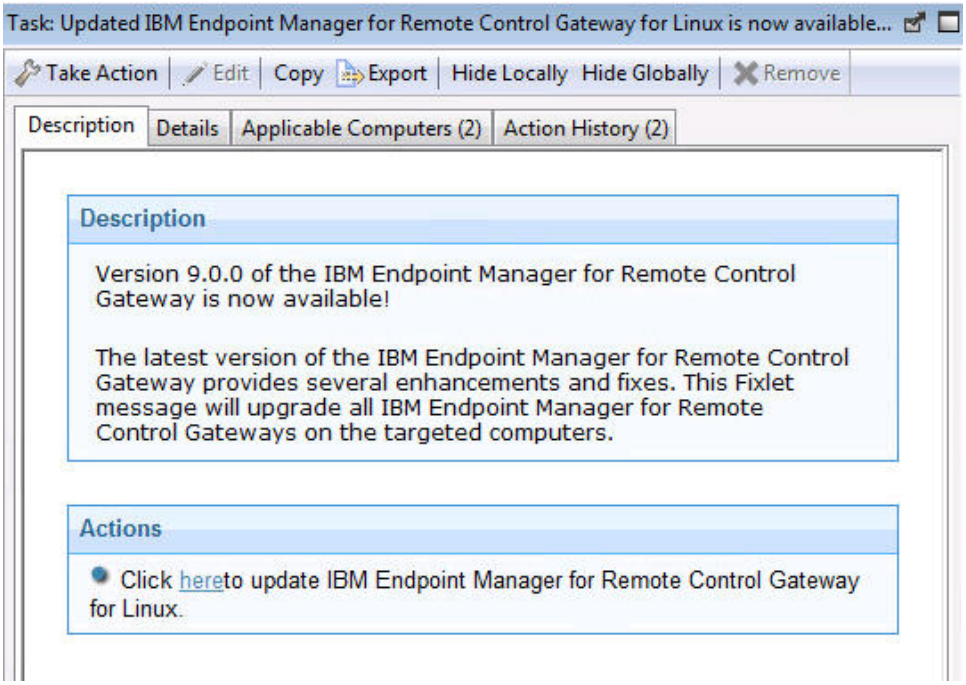
The cli tools on the selected targets are upgraded to the version of the chosen update.

Updating the Linux gateway support

Use the Linux tasks to update the gateway support files, on a Linux computer. These tasks install any new enhancements and fixes that have been applied to the chosen version whilst keeping the same gateway configuration currently installed. For example: choose the version 9.0.0 task to keep your current gateway

configuration and apply any new enhancements or fixes contained in version 9.0.0, to that. To initiate this task complete the following steps:

1. Click **Updates** > **Linux** in the navigation tree.
2. Select the required Linux gateway update. For example: **Updated IBM Endpoint Manager for Remote Control Gateway for Linux is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the gateway update on.
5. Click **OK** and enter your Private Key Password.

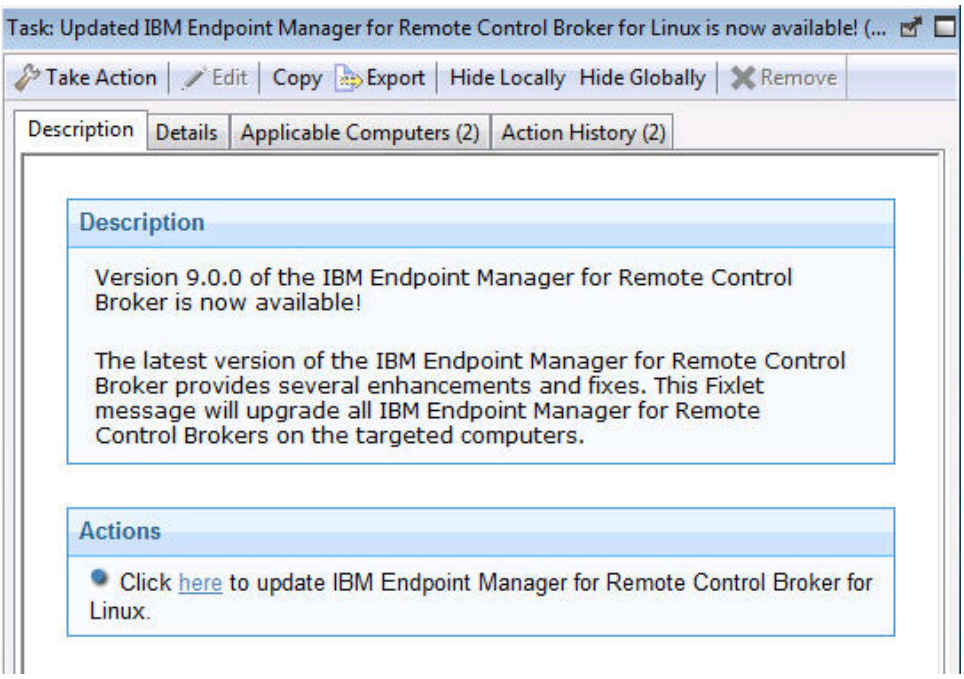
The summary screen shows the progress of the task and displays status complete when it is finished.

The gateway support on the selected targets is upgraded to the version of the chosen update.

Updating the Linux broker support

You can use the Linux tasks to update the broker software, on a Linux computer. These tasks will upgrade your currently installed broker support files to the version that the task applies to. For example: choose the version 9.0.0 task to apply any new enhancements or fixes, contained in the version 9.0.0 broker to your current broker files. To initiate this task complete the following steps:

1. Click **Updates** > **Linux** in the navigation tree.
2. Select the required Linux broker update. For example: **Updated IBM Endpoint Manager for Remote Control Broker for Linux is now available! (Version 9.0.0)**.
3. In the Task window, review the description and follow the instructions in the Actions box to initiate the task.



4. In the Take Action window on the Target tab, select the required option for determining which targets to install the broker update on.
5. Click **OK** and enter your Private Key Password.

The summary screen shows the progress of the task and displays status complete when it is finished.

The broker software on the selected targets is upgraded to the version of the chosen update.

Starting a remote control session

The IBM Endpoint Manager for Remote Control controller and target components can be used to establish remote connections between each other to monitor or control the target system. There are two modes of establishing a remote control session: a peer to peer session made directly between the target and controller and a managed session initiated from the IBM Endpoint Manager for Remote Control server, as explained in Chapter 2, “Definitions,” on page 3.

For details of how to end a remote control session see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Starting a peer to peer session

There are two ways to start a peer to peer remote control session between a controller and a target.

- From the IBM Endpoint Manager console
- By using the controller component

Starting a peer to peer session from the IBM Endpoint Manager console

The IBM Endpoint Manager console provides a method for starting a peer to peer session directly from the console in the form of a menu option which appears when you right-click on the target machine that you want to start a session with.

Note:

1. If you want to be able to start a remote control session with targets from the IBM Endpoint Manager console you should deploy the controller to the same machine as the console is installed on. However it should be noted that when the controller is deployed it is only the current user who is logged on to the machine, that you are deploying to, that will have the rights to see the menu item to start a session, it will not be visible to other users. For more information, see Appendix A, “Frequently Asked Questions,” on page 79.
2. The **Remote Control Installation and Security Options** Analysis needs to be active for the selected computer and reporting that the IBM Endpoint Manager for Remote Control target is active, for the menu item to be enabled.

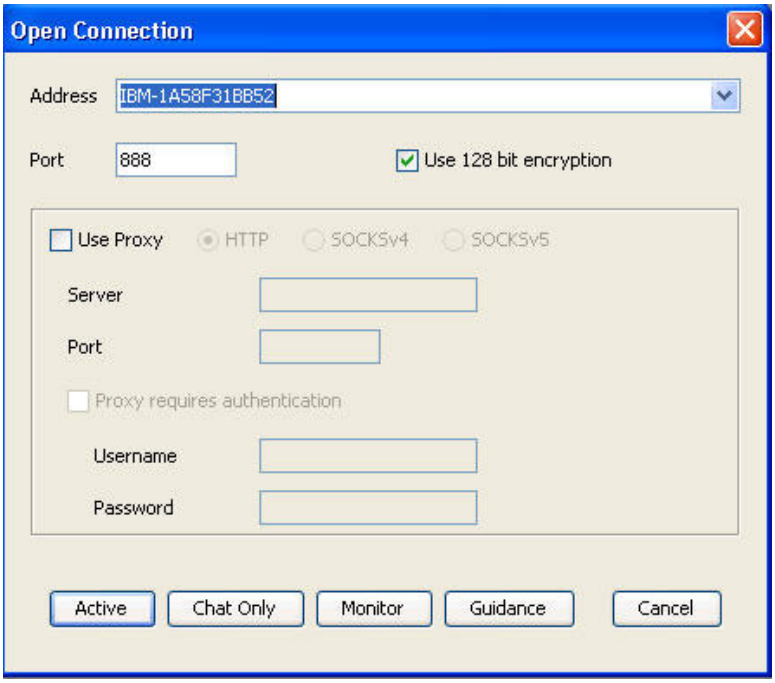
To establish a peer to peer session complete the following steps:

1. From the list of target computers **right-click** the target you want to start a remote control session with.
2. Select **IBM Endpoint Manager for Remote Control**

   Note:

   a. This action can be carried out on any section of the console in which the list of computers is displayed.

   b. If you have an older version of the controller installed on the target system you might see Tivoli® Remote Control as the menu item instead.
3. The Open connection window is displayed with the IP address or URL of the target that you want to connect to.



4. Select **Use proxy** if you will be using a proxy, select the required protocol and enter the relevant information.

   Server the hostname or IP address of the proxy server

   Port the port required for the proxy server

   Proxy requires authentication
   Select this option to authenticate with the proxy server. Provide the username and password that is required for authentication.

5. Select the session type required. For more information on the session types that can be established, see the IBM Endpoint Manager for Remote Control Controller User's Guide .

   Note:

   a. If a login window is displayed, enter a valid windows id and password to continue.
   b. A user acceptance window might be displayed on the target, depending on the policies set on the target. The target user can accept or reject the session.

When the session is accepted and started, the policies set locally on the target determine what actions can be carried out during the session. For more information on peer to peer sessions and the functions available in the controller UI, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Starting a peer to peer session using the controller

You can start a peer to peer session from any computers that you have deployed the controller component on. To start a peer to peer session using the controller component complete the following steps:

1. Start the controller

   Windows

   a. Click **Start** > **All Programs**
   b. Click **IBM Endpoint Manager for Remote Control** > **Controller**

   Linux To start the controller locate the IBM Endpoint Manager for Remote Control controller application from the operating system application interface or issue the following command

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

2. Follow from step 3 on page 46 in "Starting a peer to peer session from the IBM Endpoint Manager console" on page 46 to start the session.

When the session is accepted and started, the policies that are set locally on the target determine what actions can be carried out during the session. For more information on peer to peer sessions and the functions available in the controller UI, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Starting a server initiated remote control session

To start a remote control session initiated from the IBM Endpoint Manager for Remote Control server UI you require the server component to be installed and running. For details of creating and running server installation configurations tasks, see "Creating IBM Endpoint Manager for Remote Control server installation tasks" on page 49.

Note: The server can also be installed using the installation files. For more details see the IBM Endpoint Manager for Remote Control Installation Guide

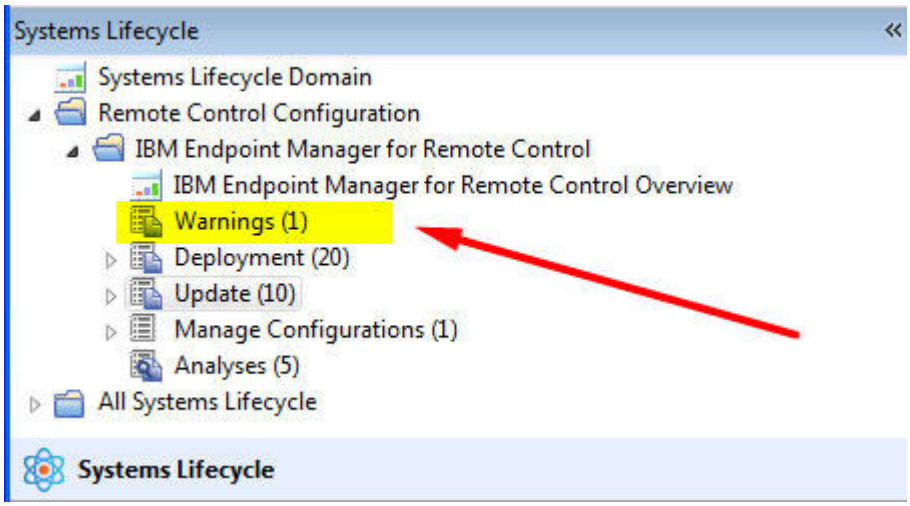
After the server component is installed use the IBM Endpoint Manager for Remote Control Controller User's Guide for details of how to access and log on to the server UI. Remote control sessions initiated from the IBM Endpoint Manager for Remote Control server require that permissions links have been set up, between the groups that the controller user and the targets are members of. These permissions links determine what policies are effective for the session. For creating user and target groups, creating permissions links and how policies are resolved for a remote control session, see the IBM Endpoint Manager for Remote Control Administrator's Guide.

When you have installed the server component and created the relevant groups and permissions links you can start a remote control session using the IBM Endpoint Manager for Remote Control server UI. For more details, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Responding to warnings

During the discovery process if there are any issues found which interfere with the normal operation of the IBM Endpoint Manager for Remote Control components, a **Warnings** node is displayed in the IBM Endpoint Manager for Remote Control navigation tree.

Note: If there are no issues found during the discovery process this node does not appear in the navigation panel.



This node displays relevant fixlets that you can use to take action and resolve the issues on any applicable computers. When the IBM Endpoint Manager for Remote Control target software is installed, a default firewall rule is created to open the inbound IBM Endpoint Manager for Remote Control port. If the target operating system is blocking this port you will see a set of fixlets that you can use to add a rule to enable inbound TCP connections for IBM Endpoint Manager for Remote Control.

Note: The SUSE firewall fixlet is not relevant when the firewall is started manually it is only relevant when the firewall is in automatic mode .

Managing target and server configurations

IBM Endpoint Manager for Remote Control provides two wizards that you can use to create tasks to install IBM Endpoint Manager for Remote Control server or target configurations. These tasks can be performed on all, or specific, servers or targets.

Creating IBM Endpoint Manager for Remote Control server installation tasks

With the **IBM Endpoint Manager for Remote Control Server Installer Wizard** you can create an installation task that can be used on Windows® and Linux® (Redhat and SUSE) to install a fully functional self contained IBM Endpoint Manager for Remote Control server with either of the following component setup.

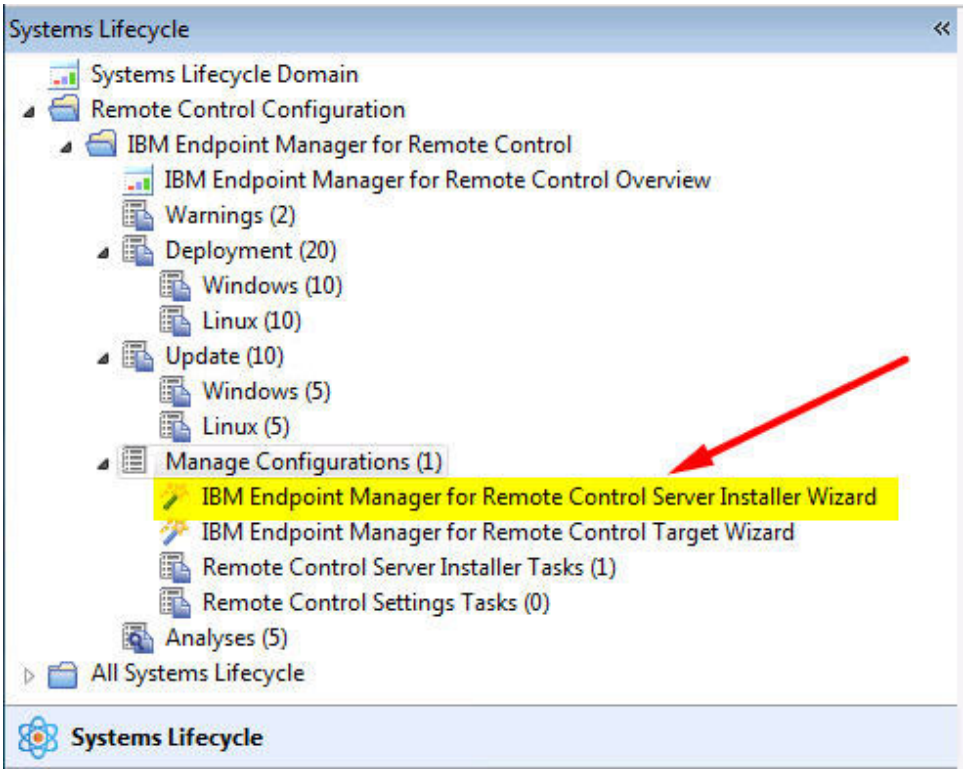
- IBM Endpoint Manager for Remote Control server with WebSphere Application Server 8.5 Liberty Profile and a Derby database.
- IBM Endpoint Manager for Remote Control server with WebSphere Application Server 8.5 Liberty Profile and IBM DB2 8.x, 9.x or 10.1 Workgroup(WSE) and Enterprise Edition(ESE), Oracle 9i / 10g / 11g or MSSQL 2000/2003/2008/2012.

Note:

1. If you choose the DB2, MS SQL or Oracle database options you should have already installed the database and created a database instance before running the server installation task.
2. If you are using DB2 9.7 GA version you should upgrade to DB2 9.7 fixpack 1 due to a DB2 issue where NULL values are returned in generated key values.

To access the **IBM Endpoint Manager for Remote Control Server Installer Wizard** complete the following steps:

1. In the IBM Endpoint Manager for Remote Control navigation tree select **Manage Configurations** > **IBM Endpoint Manager for Remote Control Server Installer Wizard**.



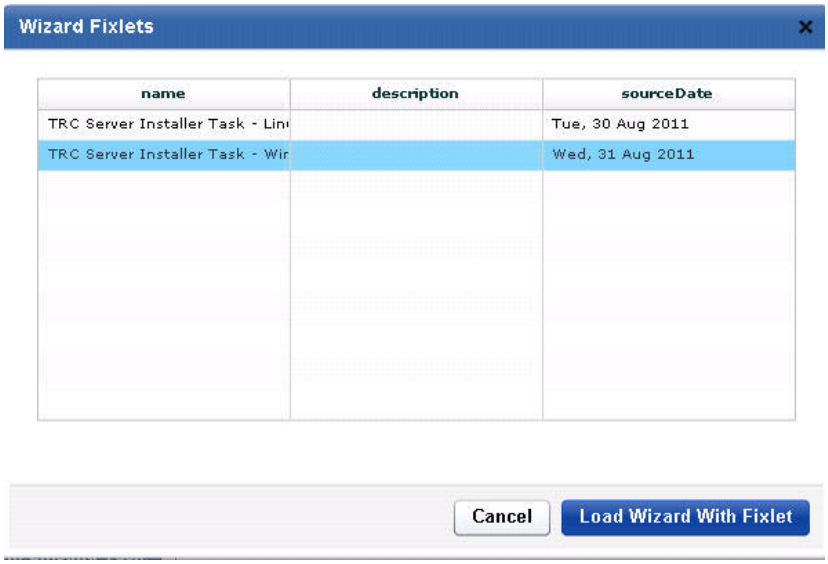
2. Set your configuration values.

Load Settings from Existing Task

The wizard initially displays server configuration default values which you can change to your own requirements. If you have already created and saved server configurations you can chose to display the saved values by clicking **Load Settings from Existing Task**.

a. Click **Load Settings from Existing Task**.

b. On the Wizard Fixlets screen select the required task.



c. Click **Load Wizard with Fixlet**. The configuration values will be loaded into the wizard.

Reset to default values
You can use this feature to clear any selections made and return the values in the wizard to the default configuration values.

Create a configuration task
Select the database and set your required values

- Derby installation - See "Creating a default server configuration"
- DB2 - See "Creating a DB2 server configuration" on page 52
- MSSQL - See "Creating an MS SQL server configuration" on page 54
- Oracle - See "Creating an Oracle server configuration" on page 55

3. When you have set your required values, save the installation task. See step 5 on page 52

Creating a default server configuration

A default server configuration installs and use the embedded Derby database which is included as part of the IBM Endpoint Manager for Remote Control installation. The database is installed locally. To create a default installation task complete the following steps:

1. Select the required operating system.
2. Enter the installation directory for the IBM Endpoint Manager for Remote Control server to be installed to or accept the default that is given.

   Note: There is a limitation that Websphere Application Server cannot be installed in a directory whose name contains Non English characters. This installation will install an embedded version of Websphere Application Server therefore you should not choose a destination for the installation files which contains Non English characters.
3. Select Derby and enter the relevant database parameter values.

   Name of the Database to use
   Specify the name for the database that will be used with IBM Endpoint Manager for Remote Control server or accept the default that is given.
4. Enter the required server installation parameter values

   HTTPS as Default for Target URL
   Select whether the server will tell the target software to communicate via http or https. If selected, https will be used.

   Note: If using https you must use a fully qualified domain name in the **Address of the Websphere server** field.

   Address of the Websphere server
   The fully qualified name for the IBM Endpoint Manager for Remote Control server. For example `trcserver.example.com`

   Note: Make sure that you enter the fully qualified name here as this is used for creating the URL in the trc.properties file that is passed to the target when it contacts the server for the first time. If the fully qualified name is incorrect, the target might not be able to contact the server successfully when it is next due to contact it.

   Web path of URL
   Specify the web path for the server URL, http://trcserver.example.com/*webpath*. For example, `trc`

HTTP port
Specify a port for the server. Default is 80.

HTTPS port
Specify a port if using SSL. Default is 443.

Administrator email
Specify an administrator email address. For example `admin@company.com`

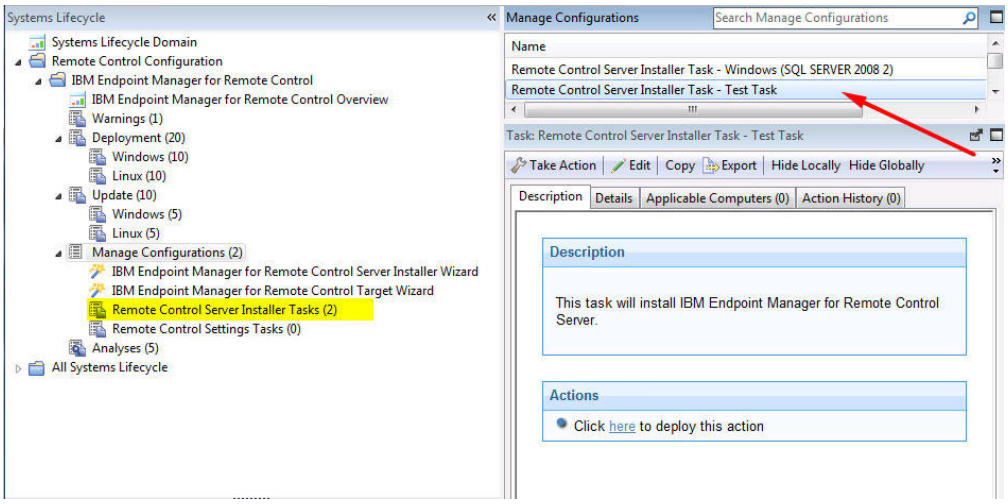
Note: To use the email function within the IBM Endpoint Manager for Remote Control server you must have a mail server installed. For more details on enabling email, see the IBM Endpoint Manager for Remote Control Installation Guide

FIPS Select this to enable FIPS compliancy on the server. For more details on enabling FIPS compliance, see the IBM Endpoint Manager for Remote Control Installation Guide

Adjust some advanced web parameters
Select this option to set additional port values.

5. Save the configuration by completing the following steps :
   a. Click **Create Server Installation Task**
   b. Fill in the required information for your task and click **OK**.
   c. Enter your private key password and click OK.

Your task is displayed in the list panel of the Remote Control Server Installer Tasks sub- node.



Creating a DB2 server configuration

You can create a server installation configuration which will use a DB2 database. This database must be installed, either locally or remotely and a database instance created prior to installing the IBM Endpoint Manager for Remote Control server. To create a DB2 server configuration task complete the following steps:-

1. Select the required operating system.
2. Enter the installation directory for the IBM Endpoint Manager for Remote Control server to be installed to or accept the default that is given.
3. Select the relevant DB2 version and enter the relevant database parameters.

Database server address
The IP address or hostname of your database server.

Note: 127.0.0.1 can be used when DB2 is installed locally. If you have installed DB2 on a remote system, type the IP address of the remote system.

Port on which to connect to the database
Port on which DB2 is installed

Note:

a. DB2 Windows® default port is 50000, Linux® is 50001
b. A remote DB2 installation is limited to type 4 connections. A local installation can use type 2 or 4. For type 2 connections set the port value to 0.

Name of the Database to use
Specify the name for the database that will be used with the IBM Endpoint Manager for Remote Control server or accept the default that is given.

Database Administrator Userid
Specify the Administrator userid used for logging on to the database. The userid needs to have admin access to the database.

Database Administrator Password
Specify the Administrator password for connecting to the database.

Path to the JDBC drivers
Specify the path to the DB2 jar files, db2jcc.jar and db2jcc_license.jar

Path to db2profile script
Specify the path to the db2profile for the DB2 instance. For example : `/home/db2inst1/sqllib/db2profile`

Note: This field is only available when installing on Linux and if you are selecting to create the database.

Path to the DB2 libraries
Specify the path to the DB2 libraries. For example : `/home/db2inst1/sqllib/lib32`

Note: This field is only available when installing on Linux and if you are selecting to create the database.

If Local, create the database
If DB2 is installed locally (127.0.0.1) you can select to have the server installation create a blank database; you can also select to drop an existing local database and create a new database.

Note: Do not select create database if you are using a remote database

If Local, drop an existing database
If DB2 is installed locally (127.0.0.1) you can select to drop the database and create a new one.

Note: Do not select drop the database if you are using a remote database

New database location (Drive name) / (Path name)
Specify the path where the database can be installed. If the installation is local and you selected to create the database the Admin user

specified above must have appropriate authority to do so. When using DB2 in Windows the **db2admin** user, and in Linux, a member of **db2grp1**.

Note:

Linux specify a directory which the admin User ID has read and write permissions for.

Windows
specify a drive letter.

4. Enter the required server installation parameters as in step 4 on page 51
5. Save your server installation task by following the steps in step 5 on page 52

Creating an MS SQL server configuration

You can create a server installation configuration to use an MS SQL database. This database must be installed, either locally or remotely and a database instance created prior to installing the IBM Endpoint Manager for Remote Control server. To create an MS SQL server configuration task complete the following steps:

1. Select the required operating system.
2. Enter the installation directory for the IBM Endpoint Manager for Remote Control server to be installed to or accept the default that is given.
3. Select the relevant MS SQL version and enter the relevant database parameters.

Database server address
The IP address or hostname of your database server.

Note: 127.0.0.1 can be used when MS SQL is installed locally on Windows only.

Port on which to connect to the database
Port on which MS SQL is installed.

Name of the Database to use
Specify the name for the database to be used with the IBM Endpoint Manager for Remote Control server or accept the default that is given.

Database Administrator Userid
Specify the Administrator user ID used for logging on to the database. The user ID needs to have admin access to the database.

Database Administrator Password
Specify the Administrator password for connecting to the database.

Path to the JDBC drivers
Specify the path to the MS JDBC java files. The `sqljdbc4.jar` file is recommended. The following version of driver can be downloaded from Microsoft. **`Microsoft JDBC Driver 4.0 for SQL Server - sqljdbc_4.0.2206.100_enu.exe`**.

If Local, create the database
If MS SQL is installed locally you can select to have the server installation to create a blank database, you can also select to drop an existing local database and create a new database. Do not select create database if you are using a remote database

If Local, drop an existing database
If MS SQL is installed locally you can select to drop the database and create a new one. Do not select drop the database if you are using a remote database.

New database location (existing directory required)
Specify the database installation path. If the instalation is local and you selected to create the database the Admin user specified above must have appropriate authority to do so.

Linux Specify a directory that the admin User ID has read and write permissions for.

Windows
Specify an existing directory.

4. Enter the required server installation parameters as in step 4 on page 51
5. Save your server installation task by following the steps in step 5 on page 52

Creating an Oracle server configuration

You can create a server installation configuration to use an Oracle database. This database must be installed, either locally or remotely and a database instance created prior to installing the IBM Endpoint Manager for Remote Control server. To create an Oracle server configuration task complete the following steps:

1. Select the required operating system.
2. Enter the installation directory for the IBM Endpoint Manager for Remote Control server to be installed to or accept the default that is given.
3. Select the relevant Oracle version and enter the relevant database parameters.

Database server address
The IP address or hostname of your database server. 127.0.0.1 can be used when Oracle is installed locally. If you have installed Oracle on a remote system, type in the IP address of the remote system.

Port on which to connect to the database
Port on which Oracle is installed.

Name of the Database to use
Specify a name for the database. This is the SID name on the server, not in **tnsnames.ora**. For example, `TRCDB`.

Database Administrator Userid
Specify the Administrator userid used for logging on to the database. The userid needs to have admin access to the database. For an Oracle installation a user called **asset** needs to exist.

Database Administrator Password
Specify the Administrator password for connecting to the database.

Path to the JDBC drivers
Specify the path to the oracle java JDBC library. This can be obtained from the Oracle server installation or downloaded from the Oracle website. For example `c:\oracle\ora92\jdbc\lib\ojdbc14.jar`

4. Enter the required server installation parameters as in step 4 on page 51
5. Save your server installation task by following the steps in step 5 on page 52

Creating IBM Endpoint Manager for Remote Control target configuration tasks

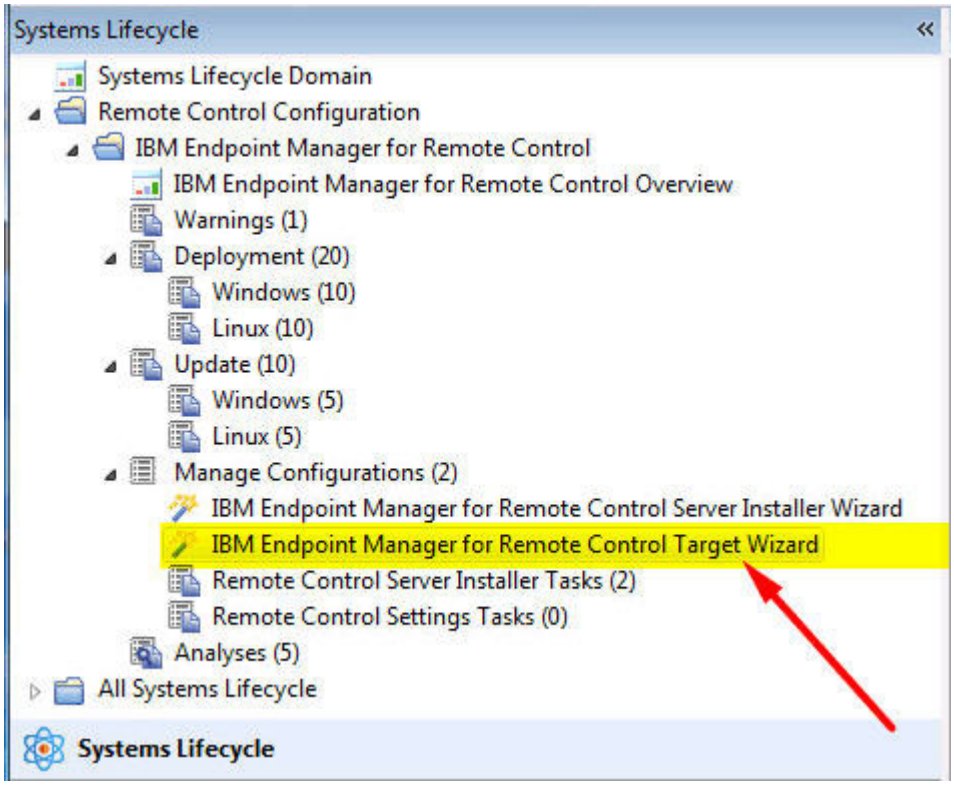
Use the IBM Endpoint Manager for Remote Control Target Wizard to create a set of target configuration parameters. The parameters can be applied to all or selected targets which have the IBM Endpoint Manager for Remote Control target software already installed, by running a task. The configurations determine what types of session the targets can take part in and the actions can be carried out by the

controller user during a remote control session. For more details about the options, see the IBM Endpoint Manager for Remote Control Installation Guide.

To create a configuration task, complete the following steps:

Note: The configuration values set here are only in effect when a peer to peer session is requested with a target. If a remote control session is initiated from the IBM Endpoint Manager for Remote Control server, the session policies are passed to the target from the server.

In the IBM Endpoint Manager for Remote Control navigation tree select **Manage Configurations** > **IBM Endpoint Manager for Remote Control Target Wizard**.

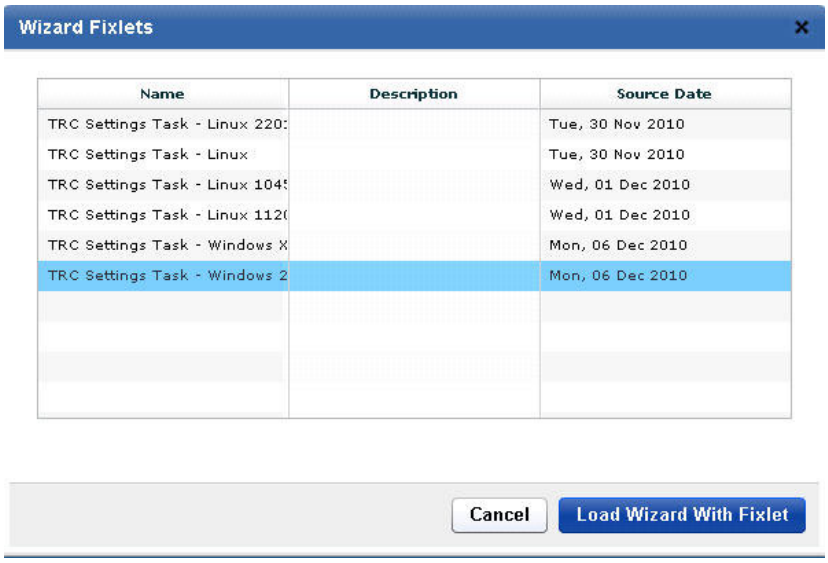


1. Select the relevant operating system.
2. Set your configuration values.

   Load settings from an existing task

   Use this feature to load previously created configuration settings.

   a. Click **Load settings from an existing task**.
   b. On the Wizard Fixlets screen, select the task.



Click **Load Wizard with Fixlet**. The configuration values are loaded into the wizard.

Reset to default values

Use this feature to clear any selections that are made and return the values in the wizard to the default configuration values.

Selecting configuration values

The wizard is loaded with default configuration values that you can change to your own requirements by selecting or clearing the relevant options.

Installation Options.

Table 1. Installation option descriptions.

Installation option	Target property	Default Value	Description
Server URL	ServerURL	blank	If you want the target to register with the server and take part in remote control sessions initiated from the server, provide the IBM Endpoint Manager for Remote Control server url. In the format: `http://servername/trc` where *servername* is the fully qualified name of theIBM Endpoint Manager for Remote Control server. For example: `http://trcserver.example.com/trc` **Note:** If you provide a server url and want the targets that this task is relevant for to take part only in remote control sessions initiated from the server, select **never** for **Allow peer to peer mode**.
Proxy URL	ProxyURL	blank	Host name or IP address for a proxy server, if you are using one.
Broker List	BrokerList	blank	The list of host names or IP addresses of the brokers and their ports, that you want the target to connect to. In the format **`hostname1:port,hostname2:port,hostname3:port.`**

Table 1. Installation option descriptions. (continued)

Installation option	Target property	Default Value	Description
Trusted certificates for Broker connections		n/a	Select this option to configure the truststore that is used for verifying broker certificates. To add a certificate, complete the following steps. 1. Open the certificate file in a text editor. 2. Select the certificate and copy it to the clipboard. **Note:** You must select everything and include the BEGIN CERTIFICATE and END CERTIFICATE lines. 3. Click **Save**.
Register target in group	GroupLabel	blank	Enter a target group name that the target will be made a member of when the configuration is applied. The arget group must exist in the IBM Endpoint Manager for Remote Control database. **Note:** The **GroupLabel** property can be used only if the target is not already registered with the server. If the target is already registered, it is not assigned to the target group. The **allow.target.group.override** property in the trc.properties file on the server must be set to true for the **GroupLabel** property value to be applied.
Remote Control port	PortToListen	888	Specify the TCP port that the target listens on.
Allow peer to peer mode	AllowP2P	Never	Used to enable peer to peer mode. **Never** A peer to peer session cannot be established between a controller and this target. If a **ServerURL** is provided, the targets can take part only in remote control sessions initiated from the server. **Only if server is unreachable.** A peer to peer session can be established between a controller user and this target only when the IBM Endpoint Manager for Remote Control server is down or unreachable. **Always** A peer to peer session can be established between a controller user and this target. **Note:** If this option is selected and a server url is provided, the targets can take part in both peer to peer sessions and sessions initiated from the server.
FIPS compliance	FIPSCompliance	not selected	Select this option to enable the use of a FIPS certified cryptographic provider for all cryptographic functions. For more information on enabling FIPS compliancy, see the IBM Endpoint Manager for Remote Control Installation Guide. **Note:** If you enable FIPS compliance on the target, also enable FIPS compliance on the controller components that are installed. Only the IBM Java Run-time Environment (JRE) is supported in FIPS-compliant mode and the JRE is installed when you install the controller software. To enable FIPS compliance on the controller, complete the following steps. 1. Edit the trc_controller.properties file on the system that the controller is installed on. **Windows** *[controller installation dir]*\trc_controller.properties where *[controller installation dir]* is the directory that the controller is installed in. **Linux** opt/ibm/trc/controller/trc_controller.properties 2. Set the **fips.compliance** property to true and save the file.
Accessibility	Accessibility	not selected	Select this option to enable the accessibility UI. Available when Windows is selected as the operating system.

Session Options

Table 2. Session option descriptions

User options	Target property	Default Value	Description
Allow monitor mode	AllowMonitor	selected	Determines whether the target can take part in monitor peer to peer sessions. For details of the different types of remote control session that can be established, see the IBM Endpoint Manager for Remote Control Controller User's Guide. **selected** The target can take part in monitor peer to peer sessions. The Monitor option is available for selection in the session type list in the controller window. The Open connection window also lists a Monitor option. **not selected** The target cannot take part in monitor peer to peer sessions. The Monitor option is not available in the session type list in the controller window.
Allow guidance mode	AllowGuidance	selected	Determines whether the target can take part in guidance peer to peer sessions. **selected** The target can take part in guidance peer to peer sessions. The Guidance option is available in the session type list in the controller window. The Open connection window also lists a Guidance option. **not selected** The target cannot take part in guidance peer to peer sessions. The Guidance option is not available in the session type list in the controller window.
Allow active mode	AllowActive	selected	Determines whether the target can take part in active peer to peer sessions. **selected** The target can take part in active peer to peer sessions. The Active option is available in the session type list in the controller window. The Open connection window also lists an Active option. **not selected** The target cannot take part in active peer to peer sessions. The Active option is not available in the session type list in the controller window.
Disable chat	DisableChat	not selected	Determines the ability to start a chat session with the target and also chat to the controller user during a peer to peer session. **selected** If ChatOnly is chosen as the connection type on the open connection screen, the session is refused. During the session, the chat icon is not available in the controller window. **not selected** A Chat Only session can be initiated from the open connection window. During the session, the chat icon is available in the controller window.

Table 2. Session option descriptions (continued)

User options	Target property	Default Value	Description
Disable file transfer to Controller	DisableFilePull	not selected	Determines the ability to transfer files from the target to the controller during the session. **selected** Files can be transferred from the target to the controller. **not selected** Files cannot be transferred from the target to the controller.
Disable file transfer to target	DisableFilePush	not selected	Determines the ability to transfer files from the controller to the target during the session. **selected** Files can be transferred from the controller to the target. **not selected** Files cannot be transferred from the controller to the target.
Disable clipboard transfer	DisableClipboard	not selected	Determines the availability of the clipboard transfer menu. Use the menu to transfer the clipboard content between the controller and target during a remote control session. **selected** The clipboard transfer menu is available during the session to transfer the clipboard content to and from the target. **not selected** The clipboard transfer menu is not available during the session.
Allow local recording	AllowRecording	selected	The controller user can make and save a local recording of the session in the controlling system. **selected** The record button is available in the controller window. **not selected** The record button is not available in the controller window.
Allow collaboration	AllowCollaboration	selected	Use this property to allow more than one controller to join a session. Determines the availability of the collaboration icon on the controller window. **selected** The collaboration icon is available in the controller window. **not selected** The collaboration icon is not available in the controller window.
Allow handover	AllowHandover	selected	The master controller, in a collaboration session, can hand over control of the session to a new controller. Determines the availability of the **Handover** button on the collaboration control panel. **selected** The **Handover** button is displayed in the collaboration control panel. **not selected** The **Handover** button is not visible in the collaboration control panel.

Table 2. Session option descriptions (continued)

User options	Target property	Default Value	Description
Allows requests to disconnect session	AllowForceDisconnect	not selected	Determines whether a **Disconnect session** button is available in the message window that is displayed when you attempt to connect to the target. You can use the **Disconnect session** option to disconnect the current session. **selected** The disconnect button is displayed in the message window. **not selected** The disconnect button is not displayed in the message window.
Disconnect grace time	ForceDisconnectTimeout	45	Number of seconds you must wait for the current controller to respond to the prompt to disconnect the current session. If they do not respond in the time that is given, they are automatically disconnected from the session. The timer takes effect only when **AllowForceDisconnect** and **CheckUserLogin** are set to Yes. The default value is 45.
Connect at logon	AutoWinLogon	selected	Determines whether the user acceptance window is displayed on a target where the target user is not logged on. **selected** The acceptance window is not visible on the target and the session is established. **not selected** The session is refused because no user is logged on at the target to accept the session.
Run pre-session script	RunPreScript	not selected	Determines whether a user-defined script is run before the remote control session starts. The script is run just after the session is allowed but before the controller user has access to the target. The outcome of running the script and the continuation of the session is determined by the value that is set for **Proceed on pre/post-script failure**. **selected** When a remote control session is requested, the defined script is run before the controller user has access to the target. **not selected** No script is run before the session. For more information about setting up pre and post session scripts, see the IBM Endpoint Manager for Remote Control Administrator's Guide.
Run post-session script	RunPostScript	not selected	Determines whether a user-defined script is run after the remote control session finishes. **selected** When a remote control session ends, the user-defined script is run. **not selected** No script is run after the session. For more information about setting up pre and post session scripts, see the IBM Endpoint Manager for Remote Control Administrator's Guide.
Proceed on pre/post-script failure	ProceedOnScriptFail	not selected	Action to take if the pre-script or post-script execution fails. A positive value or 0 is considered a successful run of the pre-script or post-session script. A negative value, a script that is not found, or not finished running within 3 minutes is considered a failure. **selected** If the pre-script or post-script run is a fail, the session continues. **not selected** If the pre-script or post-script run is a fail, the session does not continue and ends.

Table 2. Session option descriptions (continued)

User options	Target property	Default Value	Description
Reset console after RDP console session	WorkaroundW2K3RDP	Not selected	Automatically reset the console after a Remote Desktop console session. When a Remote Desktop user uses the **/admin** or **/console** option to start a Remote Desktop session with a Windows Server 2003 system and a user starts a remote control session with this target before, during or after the Remote Desktop session, remote control is unable to capture the display. The result is that a gray screen is shown in the controller. This issue is a limitation in Windows Server 2003. Therefore, this property introduces a workaround that will reset the Windows session either after each Remote Desktop session ends, or before a remote control session starts, depending on the value selected. **0** The workaround is disabled. This value is the default value. **1** Reset the session automatically when a remote control session is started. **Note:** The Windows session takes a couple of minutes to initialize and the controller sees a blank desktop until the initialization is complete. A message informs the controller user that the session is being reset and it might take a few minutes. **2** Reset the session automatically when the Remote Desktop user logs out.

User Acceptance Options

Table 3. User acceptance option descriptions

User options	Target property	Default Value	Description
Confirm incoming connections	ConfirmTakeOver	selected	Determines whether the acceptance window is displayed on the target, when a remote control session is requested. **selected** The user acceptance window is displayed and the target user can accept or refuse the session. **not selected** The user acceptance window is not displayed and the session is established.
Confirm mode changes	ConfirmModeChange	selected	Determines whether the user acceptance window is displayed when the controller user selects a different session mode from the session mode list on the controller window. **selected** The user acceptance window is displayed each time a session mode change is requested and the target user must accept or refuse the request. **not selected** The user acceptance window is not displayed and the session mode is changed automatically.

Table 3. User acceptance option descriptions (continued)

User options	Target property	Default Value	Description
Confirm file transfers	ConfirmFileTransfer	selected	Determines whether the user acceptance window is displayed when the controller user selects to transfer files between the target and the controller. **selected** The acceptance window is displayed in the following two cases. The target user must accept or refuse the file transfer. • The controller user selects **pull file** from the file transfer menu on the controller window. The target user must select the file, that is to be transferred after they have accepted the request. • The controller user selects **send file to controller** from the **Actions** menu in the target window. **Not selected** The acceptance window is not displayed and files are transferred automatically from the target to the controller system when requested.
Confirm system information	ConfirmSysInfo	selected	Determines whether the user acceptance window is displayed when the controller user requests to view the target system information. **selected** When the controller user clicks **System information** in the controller window, the user acceptance window is displayed. The target user must accept or refuse the request. If the target user clicks accept, the target system information is displayed in a separate window on the controller system. If they click refuse, a message is displayed on the controller and the system information is not displayed. **not selected** The target system information is displayed automatically when the controller user clicks the system information icon.
Confirm recording	ConfirmRecording	selected	Determines whether the user acceptance window is displayed when the controller user clicks the record icon on the controller window. **selected** When the controller user clicks the record icon on the controller window, a message window is displayed. If the target user clicks **Accept**, the controller user can select a directory to save the recording to. If the target user clicks **Refuse**, a recording refused message is displayed to the controller. **Note:** After the target user accepts the request for recording, if the controller user stops and restarts local recording, the acceptance window is not displayed. **not selected** When the controller user clicks the record icon on the controller window, the message window is not displayed. The controller user can select a directory to save the recording to.
Confirm collaboration	ConfirmCollaboration	selected	Determines whether the user acceptance window is displayed when another controller user requests to join a collaboration session with a target. **selected** When the controller user tries to join the collaboration session, the user acceptance window is displayed. The target user must accept or refuse the request to allow the additional controller to join the session. If the target user clicks accept, the additional controller joins the collaboration session. If they click refuse, a message is displayed on the controller and the additional controller cannot join the collaboration session. **not selected** The additional controller automatically joins the collaboration session when they try to connect to the master controller of the session.

Table 3. User acceptance option descriptions (continued)

User options	Target property	Default Value	Description
Acceptance grace time	AcceptanceGraceTime	45	Sets the number of seconds to wait for the target user to respond before a session starts or times out, used with **Confirm incoming connections**. • Acceptable values 0 - 60 - If set to 0, the target user is not asked to respond to the session request. **Note:** If **Confirm incoming connections** is selected,**Acceptance grace time** must be set to a value >0 to provide the target user with enough time to respond.
Proceed on acceptance timeout	AcceptanceProceed	not selected	Action to take if the user acceptance window timeout lapses. The target user did not click accept or refuse within the number of seconds defined for **Acceptance grace time.** **selected** Session is established. **not selected** Session is not established.
Hide windows	HideWindows	not selected	Determines whether the **Hide windows** check box is displayed on the user acceptance window when **Confirm incoming connections** is also selected. **selected** The **Hide windows** check box is displayed on the user acceptance window. **not selected** The **Hide windows** check box is not visible on the user acceptance window.

Security options

Table 4. security option descriptions

Security options	Target property	Default Value	Description
Authenticate using system logon	CheckUserLogin	selected	Determines whether the login window is displayed when a session type is selected on the Open Connection window. **Yes** The login window is displayed and the controller user must log in with a valid windows id and password. If the logon credentials are invalid, the target refuses the session. **No** The user acceptance window is not displayed and the peer to peer session is established.

Table 4. security option descriptions (continued)

Security options	Target property	Default Value	Description

Authorized user group	CheckUserGroup	see description	Default value is:
			Windows
			`BUILTIN\Administrators`
			Linux
			`wheel`
			When **Authorized user group** has a value set, the user name that is used for authentication must be a member of one of the groups that are listed. If the user is not a member, the session is refused. Multiple groups must be separated with a semicolon. For example: `wheel;trcusers`
			Note: By default, on Windows, only the Administrator user is granted access. On Linux, by default no users are granted access. To resolve this, you can complete one of the following steps.
			1. To also grant administrator rights to the users, add them as members to the Administrators group on Windows or the wheel group on Linux.
			2. For users with no administrator rights, complete the following steps
			a. Create a group or use an existing group. For example, the following command can be run as root:
			`groupadd trcusers`.
			b. Add the users to this group. For example, the following command can be run as root to add **bsmith** to **trcusers**:
			`usermod -a -G trcusers <bsmith>`
			c. Add the group to the list in the **Authorized user group** field.

Audit to system log	AuditToSystem	selected	Determines whether the actions that are carried out during remote control sessions are logged to the application event log on the target. This file can be used for audit purposes. **selected** Entries are logged in the application event log of the target corresponding to each action that is carried out during the session. **not selected** No entries are logged to the application event log.
Save chat messages	AutoSaveChat	not selected	Determines whether the dialogue, entered during a chat session, can be saved. **selected** The chat dialogue is saved as an html file. The file name starts with `chat`. The file is saved in the working directory of the target. The location of the working directory is defined by the target property **WorkingDir**. For example, in Windows a file named `chat-m15.html` saved to the following location. `c:\Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control` **not selected** The chat dialogue is not saved to a file.

Table 4. security option descriptions (continued)

Security options	Target property	Default Value	Description
Lock target on disconnect	SessionDisconnect	not selected	Determines whether the target computer is automatically locked when the remote control session ends. **selected** The target computer is automatically locked at the end of the session. **not selected** The target computer is not automatically locked at the end of the session.
Allow privacy	AllowPrivacy	selected	Determines whether a controller user can lock the local input and screen of the target when in a remote control session. Determines the visibility of the **Enable Privacy** option on the controller window. **selected** The **Enable Privacy** option is available in the **Perform Action in target** menu in the controller window. **not selected** The **Enable Privacy** option is not available in the **Perform Action in target** menu in the controller window.
Allow input lock	AllowInputLock	selected	This property works with **Allow privacy** and on its own. You can use **Allow input lock** to lock the target users mouse and keyboard during a remote control session. **selected** The **lock target input** menu item is enabled, in the **Perform action in target** menu in the controller window. Select **lock target input** to lock the target users mouse and keyboard during a remote control session. The target screen is still visible to the target user. **not selected** The lock target input menu item is not enabled in the **Perform action in target** menu in the controller window. **Note:** If the option to **Enable Privacy** is selected during a session, the remote user input is automatically locked. It is not possible to enable privacy without also locking the input.
Enable privacy	EnablePrivacy	not selected	Determines whether the local input and screen are locked for all sessions. Therefore, the target user cannot input or do anything on the target while in a remote control session. **selected** The target screen is blanked out by the privacy bitmap when the session starts, preventing the target user from interacting with the screen while in the session. The target desktop is still visible to the controller user in the controller window. **not selected** The target screen is not blanked out when the session is started and the target user can interact with the screen.

Table 4. security option descriptions (continued)

Security options	Target property	Default Value	Description
Enable input lock	EnableInputLock	not selected	This property works with **Enable privacy**. When privacy mode is enabled, use **Enable input lock** to determine whether the target user can view their screen or not, during a remote control session. **selected** The target screen is visible to the target user during the session, while in privacy mode but their mouse and keyboard control is locked. **not selected** The target screen is not visible to the target user. The privacy bitmap is displayed on the target during the session. The target users mouse and keyboard input is also disabled. **Note: Enable privacy** should be selected for **Enable input lock** to take effect.
DisablePanicKey	DisablePanicKey	not selected	Determines whether the Pause Break key can be used by the target user to automatically end the remote control session. **selected** The target user cannot use the Pause Break key to automatically end the remote control session. **not selected** The target user can use the Pause Break key to automatically end the remote control session.
Enable on-screen session notification	EnableOSSN	not selected	Determines whether a semi-transparent overlay is displayed on the target computer to indicate that a remote control session is in progress. Use this property when privacy is a concern so that the user is clearly notified when somebody can remotely view or control their computer. **selected** The semi-transparent overlay is displayed on the target screen with the text **IBM Endpoint Manager for Remote Control** and what type of remote control session is in progress. `For example : IBM Endpoint Manager for Remote Control - Active Mode.` The overlay does not intercept keyboard or mouse actions, therefore the user is still able to interact with their screen. **not selected** No overlay is displayed on the target computer. **Note:** This policy is only supported on targets that have a Windows operating system installed.
Disable GUI	DisableGUI	not selected	Determines the appearance of the target GUI when the remote control session is starting and also during the session. **Note:** This option works only when the target is installed in peer to peer mode and the **Managed** target property is set to No. This option is ignored when applied to any targets that were installed using the IBM Endpoint Manager for Remote Control server mode when a server URL was supplied. **selected** The target GUI is not visible on the target and the target user is not aware that the session is started. The IBM Endpoint Manager for Remote Control target icon is not visible in the Windows system tray. **not selected** The target GUI is displayed on the target as the session is starting and is available to the target user during the remote control session.

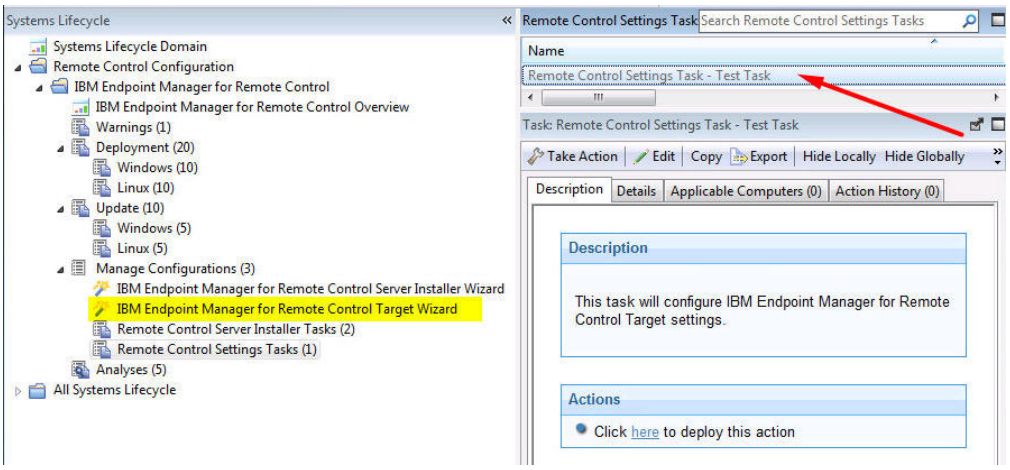
Performance options

Table 5. performance option descriptions

Security options	Target property	Default Value	Description
Inactivity timeout	IdleTimeout	360	Specify the number of seconds to wait until the connection ends if there is no remote control session activity. Set this value to 0 to disable the timer so that the session does not end automatically. The minimum timeout value is 60 seconds. Therefore, a value >0 and <60 times out at approximately 60 seconds and values >60 timeout when value is reached. The default value is 360. Set the value to 0 for sessions that do not involve sending or receiving information from the controller to the target. For example, in Monitor sessions.
Enable true color	EnableTrueColor	not selected	Determines the availability of the **Enable/Disable** true color icon in the controller window. Used with **Lock color depth**. **selected** The **Enable/Disable** true color icon is available in the controller window. Use the icon to enable true colors on the controller windows view of the target desktop if the **Lock color depth** property is not selected. **not selected** The **Enable/Disable** true color icon is not available in the controller window.
Lock color depth	LockColorDepth	not selected	Used along with **Enable true color** to determine the color depth when a remote control session is established. **selected** The chosen color depth, for the remote control session, is locked and cannot be changed during the session. **not selected** If the **Enable true color** property is selected also, the chosen color depth can be changed during the session.
Remove desktop	RemoveBackground	not selected	Determines whether a desktop background image can be removed from view during a remote control session. **selected** The desktop background image, on the target, is not visible during a remote control session. **not selected** The desktop background image, on the target, is visible during a remote control session.
Stop screen saver updates	NoScreenSaver	not selected	Stops the target from sending screen updates when it detects that the screen saver is active. **selected** While the screen saver is active on the target system, the target stops transmitting screen updates. A simulated screen saver is displayed on the controller computer so that the controller user knows that a screen saver is active on the remote screen. The controller user can close the screen saver by pressing a key or moving the mouse. **not selected** No simulated screen saver is displayed in the session window. The target screen is displayed as normal and the target continues to transmit screen updates.

3. Click **Create Configuration Task**. Type the relevant information for your task and click **OK**
4. Enter your private key password and click **OK**.

Your task is displayed in the list panel of the Remote Control Settings Tasks subnode.

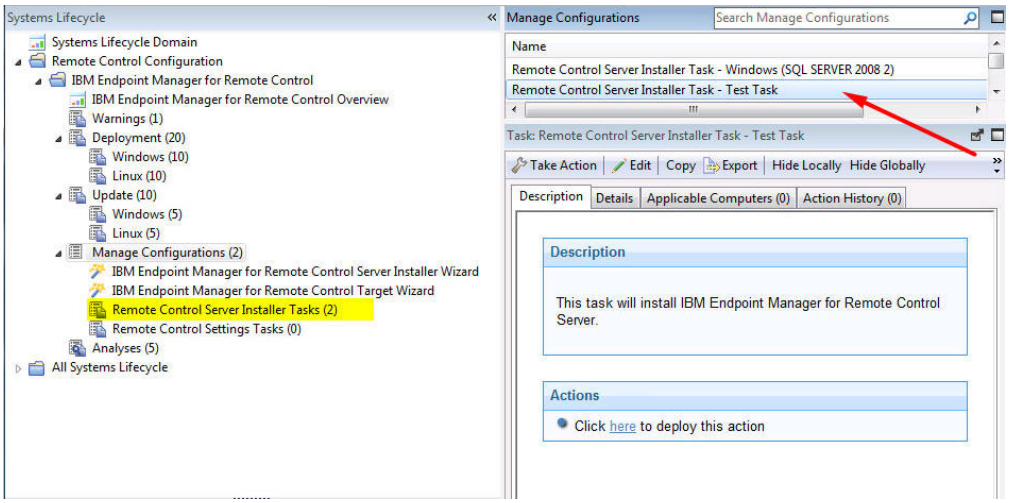


Running IBM Endpoint Manager for Remote Control tasks

When you have used the server and target configuration wizards to create configuration tasks you can run these tasks to install the IBM Endpoint Manager for Remote Control server software on selected targets or change the configuration of already installed targets.

Running server installer tasks

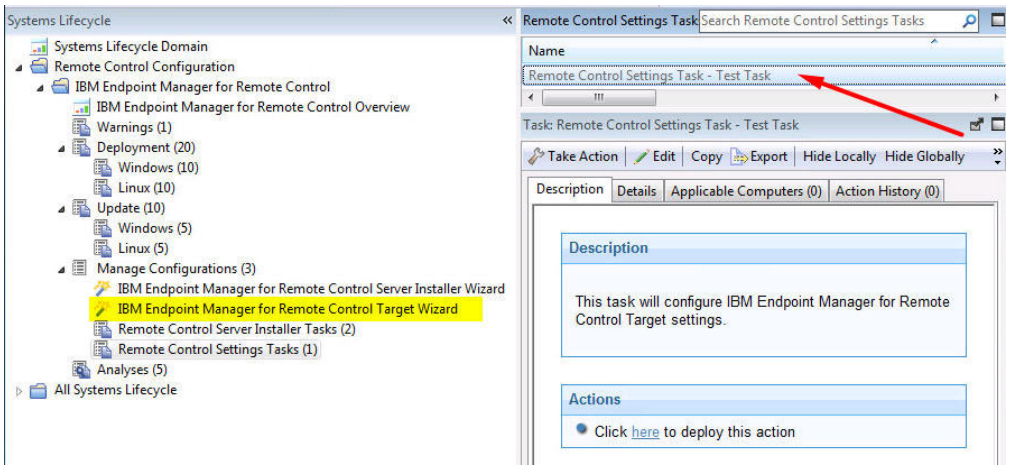
Use the Remote Control Server Installer Tasks subnode to run the tasks that you created using the IBM Endpoint Manager for Remote Control Server Installer Wizard. Select the required task then in the Task window, review the description and follow the instructions in the Actions box to initiate the task. These tasks install the IBM Endpoint Manager for Remote Control server software on to your selected computers.



Note: If the server installer fails, the task will fail and an exit code is displayed.

Running target configuration tasks

Use the Remote Control Settings Tasks sub-node to execute the configuration tasks that you created using the IBM Endpoint Manager for Remote Control Target Wizard. Select the required task then in the Task window, review the description and follow the instructions in the Actions box to initiate the task.

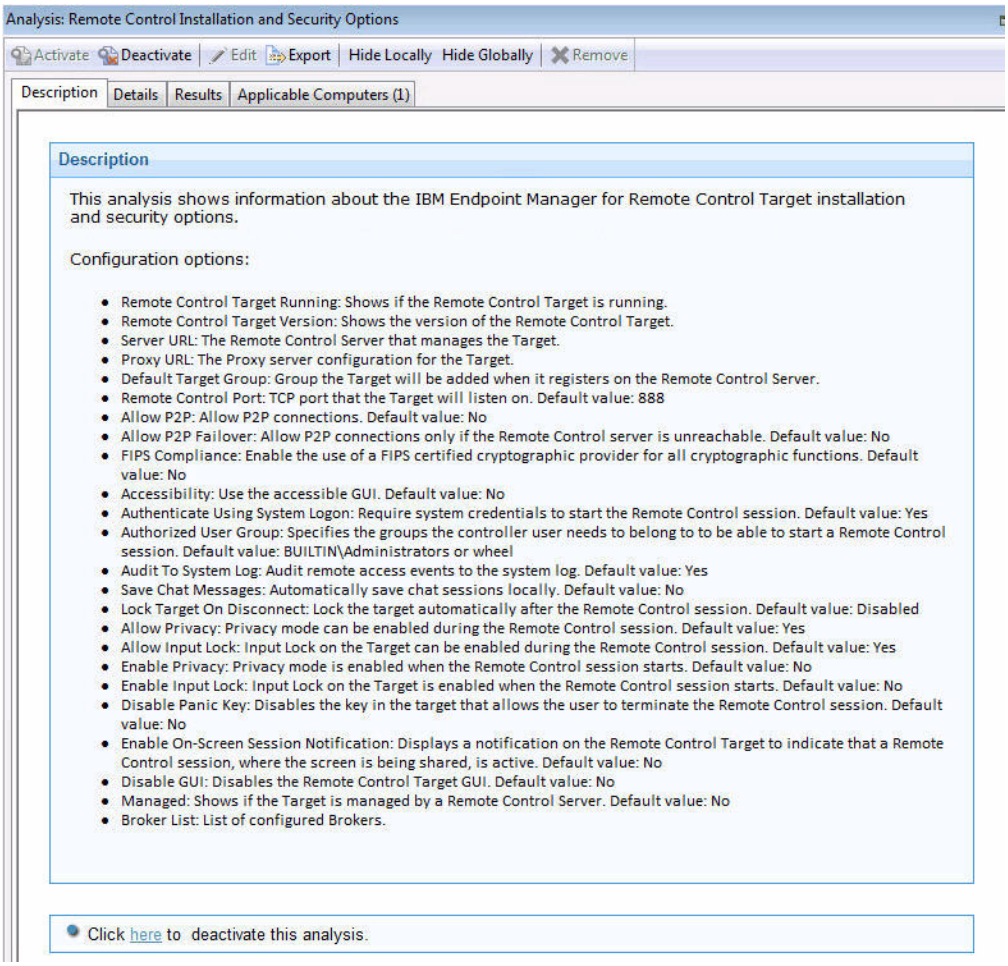


Analyses

The Analyses subnode provides a set of analyses which gather installation, user and audit information. This data provides a history of remote control connection events that have taken place on the computers in your environment that have the controller or target components installed. These analyses are activated globally therefore any computers in your environment, that the analysis is relevant for, report their values.

Retrieving target installation and security data

The **Remote Control Installation and Security Options** analysis is used for gathering information about the installation and security property values from targets in your environment that have the IBM Endpoint Manager for Remote Control target software running. You can use the values returned for these properties to determine various things about the targets, for example if they are allowed to take part in peer to peer sessions and if they can take part in remote control sessions initiated from a IBM Endpoint Manager for Remote Control server. For property value definitions, see step 2 on page 56.

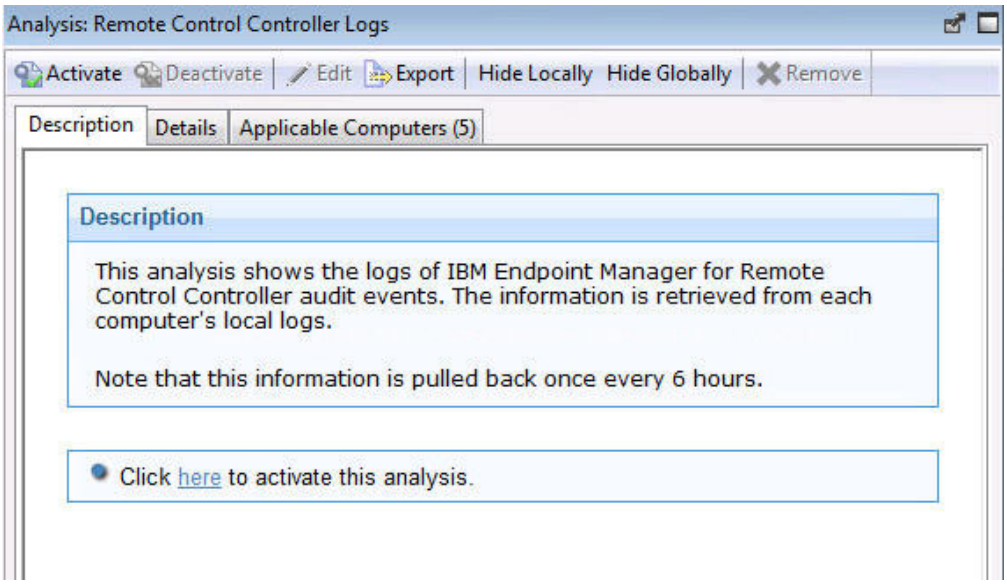


If the analysis is active, the Results tab lists the computers that this analysis was relevant for and the values of the installation and security options are displayed. You can expand the Applicable Computers entry and filter the data further by Retrieved Properties. This can be useful in many ways, for example, for determining which targets can take part in peer to peer remote control sessions or viewing the version of target software installed on the various IBM Endpoint Manager for Remote Control targets.

For example, to determine which targets are running a specific version of IBM Endpoint Manager for Remote Control target, expand **Applicable Computers** > **By Retrieved Properties** > **By Remote Control Target Version** and select a specific version from the list. The list of targets that have the selected version of software installed, is displayed.

Retrieving audit events data

The **Remote Control Controller Logs** analysis is used for gathering the audit events from any computers in your environment that have the IBM Endpoint Manager for Remote Control controller component installed. The information is retrieved and updated every 6 hours. This information can be used for auditing purposes and also for monitoring session activity carried out by the controller user.

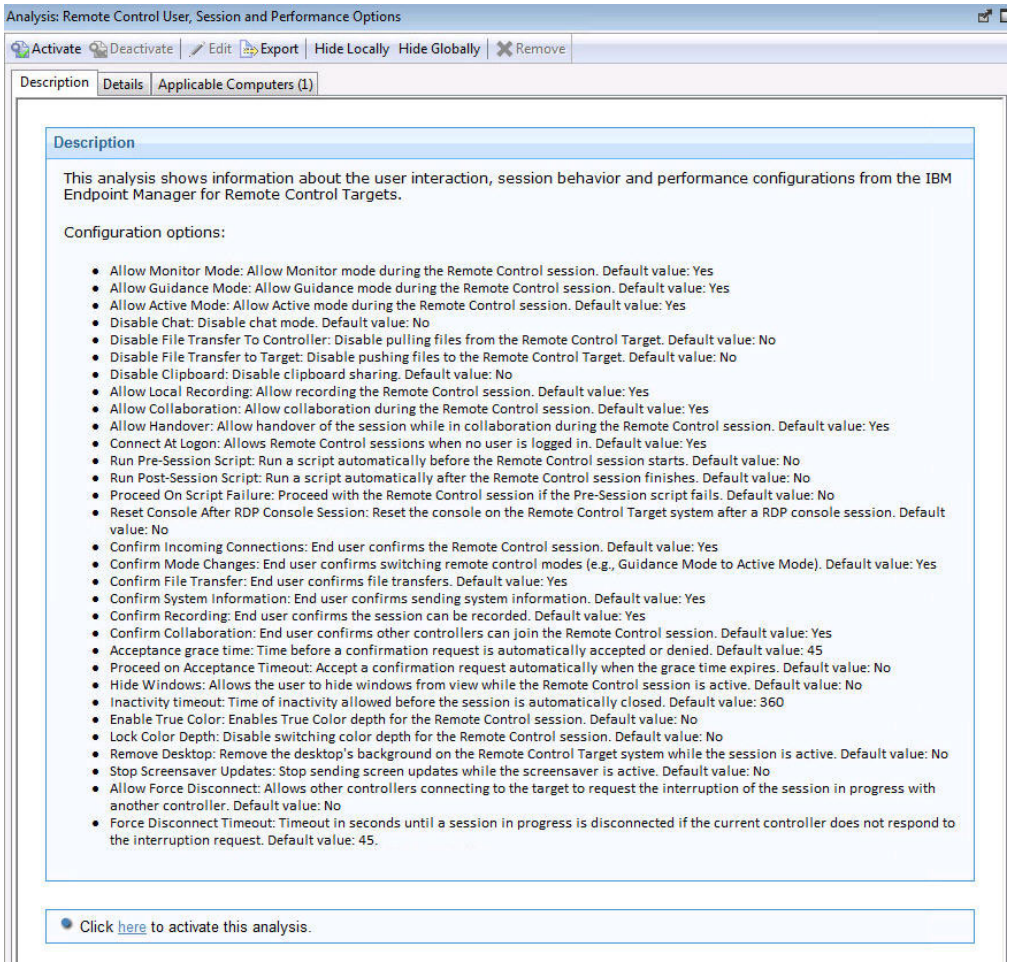


If the analysis is active, the Results tab lists the computers that this analysis was relevant for. Double-click on a computer to see summary data for the selected computer, which includes a section for the controller log entries retrieved by the **Remote Control Controller Logs** analysis. You can also expand the Applicable Computers entry and filter the data further by specific retrieved properties.

Note: If the controller component is actively in a remote control session while the analysis tries to gather data from it, an error stating that the file is in use might be reported in the analysis results.

Retrieving user, session and performance data

The **Remote Control User, Session and Performance Options** analysis is used for gathering user interaction, session behaviour and performance property values from targets in your environment that have the IBM Endpoint Manager for Remote Control target software running. These properties can be used to determine what actions the controller user can carry out during a remote control session with this target. For property value definitions, see step 2 on page 56.

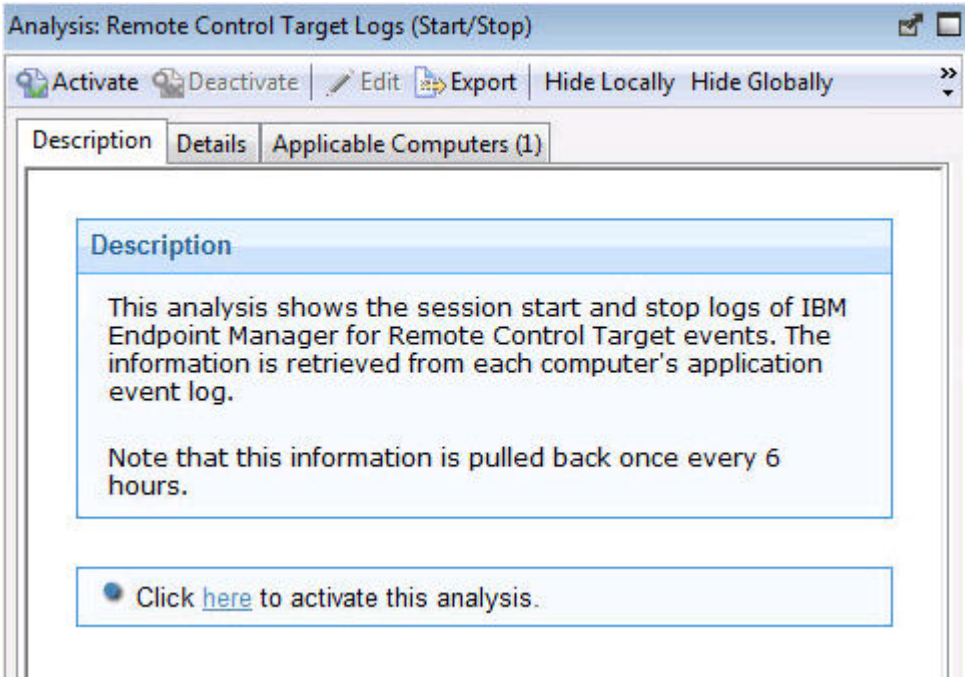


If the analysis is active, the Results tab lists the computers that this analysis was relevant for and the values of the user interaction properties are displayed. You can expand the Applicable Computers entry and filter the data further by specific retrieved properties.

Retrieving session connection data

The **Remote Control Target Log (Start/Stop)** analysis is used for gathering the audit events from any computers in your environment that have the IBM Endpoint Manager for Remote Control target component installed. The information is retrieved and updated every 6 hours. The information returned by this analysis is useful for viewing remote control session usage activity on specific targets as it is only the session connection, start and stop events that are returned for each session. If you require information about the remote control session activity, use the **Remote Control Target Log** analysis.

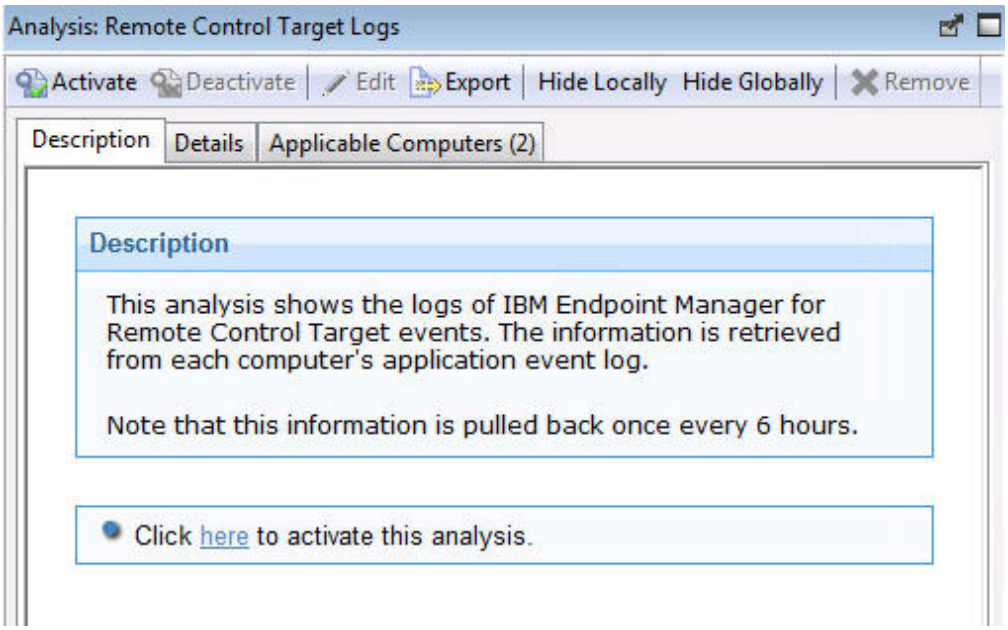
Note: This analysis is only valid for windows targets.



If the analysis is active, the Results tab lists the computers that this analysis was relevant for. Double-click on a computer to see summary data for the selected computer which includes a section for the target log start/stop entries.. You can also expand the Applicable Computers entry and filter the data further by specific retrieved properties.

Retrieving session activity data

The **Remote Control Target Logs** analysis is used for gathering the audit events from any computers in your environment that have the IBM Endpoint Manager for Remote Control target component installed. The information is retrieved and updated every 6 hours. This information is useful for auditing purposes, providing details of actions carried out during a remote control session, for example, a change in session type or a file transfer. The controller user who was carrying out the session is also displayed.



If the analysis is active, the Results tab lists the computers that this analysis was relevant for. Double-click on a computer to see summary data for the selected computer which includes a section for the target log entries retrieved by the **Remote Control Target Logs** analysis. You can also expand the Applicable Computers entry and filter the data further by specific retrieved properties.

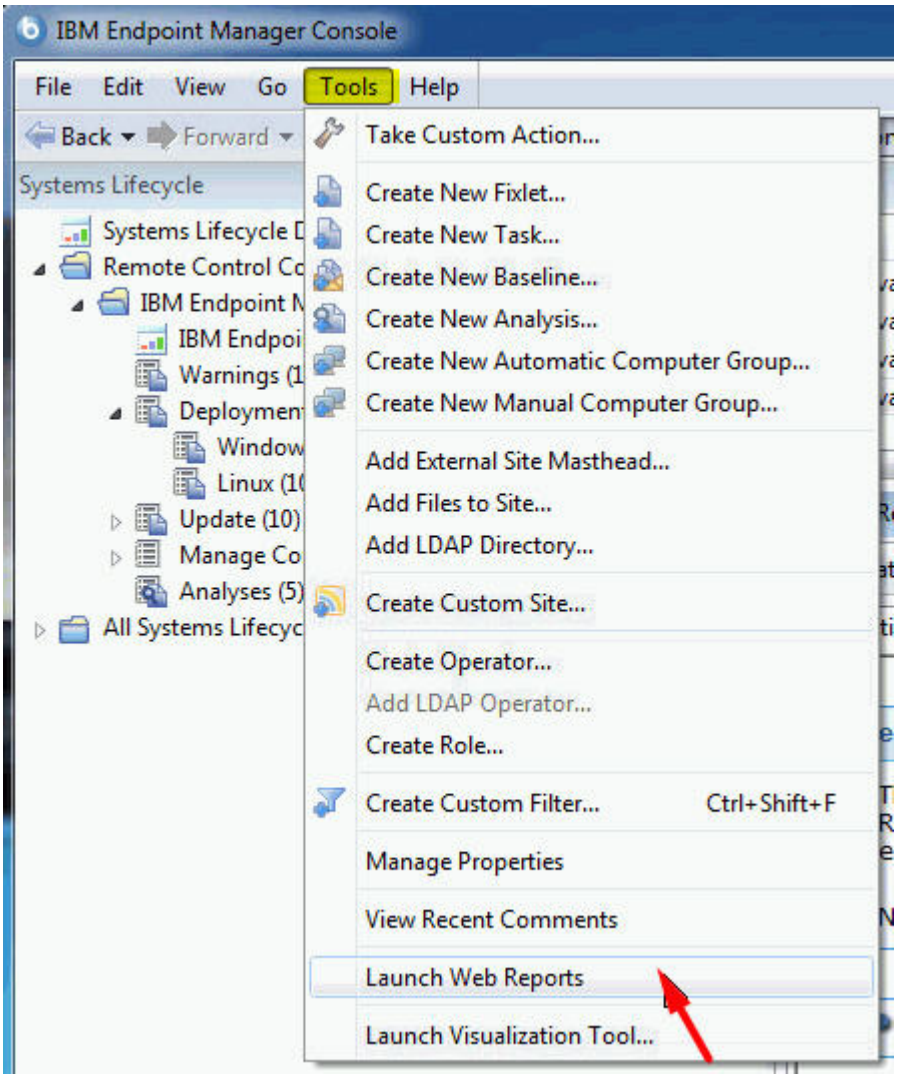
Note: The reason codes returned in this data can be viewed completely by using the web reports to display the output. For more details, see Chapter 6, "Viewing web reports," on page 77.

Chapter 6. Viewing web reports

IBM Endpoint Manager for Remote Control offers a report available in the Web Reports component of the application. This web report was formulated to provide log data gathered from the controller and target logs relevant to specific targets. This data can be used for auditing purposes and for monitoring remote control activity on specific machines in your environment.

To access the IBM Endpoint Manager for Remote Control web report complete the following steps:

1. Click **Tools** > **Launch Web Reports**



2. Enter your Web Reports username and password. If you do not know your username or password, check with your Administrator.

After login, you will see the main Web Reports page open in a new browser.

3. Select **Systems Lifecycle** to see a list of reports including the IBM Endpoint Manager for Remote Control report. You will see the IBM Endpoint Manager for Remote Control Events entry in the reports list displayed under the Report List menu:
4. Click **IBM Endpoint Manager for Remote Control Events**.
5. Enter the computer name of the target whose information you want to view and click **View Events**.

Any log data that has been gathered from the controller and target logs, for the specified target is displayed in the relevant sections, showing the remote control events.

Appendix A. Frequently Asked Questions

1. I have installed the target software on a target in my environment, but I do not have an option to start a remote control session when I right click on the computer in the IBM Endpoint Manager console?

   To start a remote control session using this method make sure that the following conditions are met .

   - The controller component is also installed on the system that the IBM Endpoint Manager console is installed on.
   - The **Remote Control Installation and Security Options** analysis needs to be active for the selected computer and reporting that the IBM Endpoint Manager for Remote Control target is active, for the menu item to be visible.
   - When the controller is deployed it is only the current user who is logged on to the machine that you are deploying to that will have the rights to see the menu item that allows you to start a session. It is not visible to other users. The following registry key can also be created.

     Key name: HKEY_CURRENT_USER\Software\BigFix\Enterprise Console\Settings\ComputerListContextMenuExtensions\TivoliRC

     With the following values

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

     MaxComputerSetSize = 1

     MenuDisplayName= &IBM Endpoint Manager for Remote Control

     ShellCommandRelevance = "%22C:\Program Files\IBM\Tivoli\Remote Control\Controller\jre\bin\javaw.exe%22 -jar %22C:\Program Files\IBM\Tivoli\Remote Control\Controller\TRCConsole.jar%22 --host " & hostname of current computer

2. I have deployed the target software in peer to peer mode but want the target to register with my IBM Endpoint Manager for Remote Control, how can I get it to connect to the server?

   Use the IBM Endpoint Manager for Remote Control Target Wizard to create a configuration task and specify the server URL of the required server. Running this task on the selected target will reconfigure it so that it can contact the server. For more details, see “Creating IBM Endpoint Manager for Remote Control target configuration tasks” on page 55.

3. Where can I find more information on using IBM Endpoint Manager for Remote Control ?

   Information for installing, using and administering IBM Endpoint Manager for Remote Control can be found in the IBM Endpoint Manager for Remote Control infocenter.

4. Additional IBM Endpoint Manager for Remote Control function is available when you have the IBM Endpoint Manager for Remote Control server component installed, where can I obtain the server component from?

   You can create a server installation task using the IBM Endpoint Manager for Remote Control Server Installer Wizard to create a IBM Endpoint Manager for Remote Control server configuration. For more details, see “Creating IBM Endpoint Manager for Remote Control server installation tasks” on page 49.

   You can also install a server which points to an already installed Websphere Application server instance using an already installed DB2, MS SQL or Oracle

database. For more details, see the **Installing the server** section in the IBM Endpoint Manager for Remote Control Installation Guide.

5. How can I determine which type of server installation would be suit my environment?

   See the IBM Endpoint Manager for Remote Control Installation Guide for some guidelines for consideration when planning your installation.

Appendix B. Support

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

- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services offered in the U.S.A.

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

IBM 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:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION 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 states 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. IBM 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-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web

sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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 IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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 the names and addresses used by an actual business enterprise 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 IBM, 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. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the “Web at Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

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

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Index

U

V

W

Printed in USA