Tivoli® Remote Control
5.1.2

Tivoli Endpoint Manager - TRC User's Guide

Tivoli® Remote Control
5.1.2

Tivoli Endpoint Manager - TRC User's Guide

Note

Before using this information and the product it supports, read the information in “Notices,” on page 43

First Edition (January 2011)

This edition applies to version 5, release 1, modification 2 of IBM Tivoli Remote Control (product number 5724-C21) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. Overview

The Tivoli® Remote Control site masthead contains information about Tivoli Remote Control content that performs certain tasks and analyses within your deployment. You must be subscribed to the Tivoli Remote Control "site" in order to collect data from the client. This data will be utilized for reporting and analysis. To add a site, click the Tools menu from within the Tivoli Endpoint Manager (TEM) console and select Add External Site Masthead and follow the prompts.

The TEM Tivoli Remote Control solution allows you to deploy and configure the components required for establishing remote control sessions with workstations and servers across your enterprise . This Users's Guide will describe some of the primary components of Tivoli Remote Control, how to install and configure these from the TEM console and their use in establishing a remote control session. See the **IBM Tivoli Remote Control User's Guide** for details of the functions available within a remote control session.

There are two infrastructure components available in your TEM Tivoli Remote Control solution whose features are listed below.

Note: The availability of some of the features below will depend on whether you have purchased Tivoli Remote Control as a separate product and have the TRC server component installed and running.

Controller

- Participates in a remote control session.
- Records audit information which can be stored in the TRC server, if running.

Target

- Resides on the endpoint (client) to be controlled.
- Presents a Graphical User Interface to the endpoint user.
- Controls the policies set for the session.
- Records audit information locally.
- Additionally if you have the TRC server component
  - Registers and maintains current state information on the TRC server about the endpoint.
  - Receives connection requests and can authenticate them against the infrastructure server if the TRC server is running.
  - Stores audit information on the server.

Chapter 2. System requirements

Controller requirements

The Controller is a Java based application that can run on any platform with the following prerequisites:

- Java Run Time environment: Sun 1.5-1.6 or IBM® 1.4, 1.5, 1.6.

  Note: The Sun Java JRE is not supported in FIPS mode, you should use the IBM Java JRE in this mode.
- Web Browser: either Microsoft Internet Explorer 6, 7, 8 or Mozilla Firefox 1.5, 2.0, 3.0.

Target requirements

The computer on which you install the Tivoli Remote Control target must have the minimum following items or specification:

1. At least a 166MHz Intel or AMD processor.
2. A minimum of 64Mb of memory.
3. A minimum of 50Mb hard disk space.

Platform Support

The following Platforms are supported

1. Windows 2000 Pro, Server, Advanced Server.
2. Windows XP Pro (32 bits), (64 bits).
3. Windows Server 2003 Standard R2 (32 bit), Standard R2 (64 bit), Enterprise R2 (32 bit), Enterprise R2 (64 bit).
4. Windows Server 2003 R2 Datacenter Edition x86-32 , x86-64.
5. Windows Vista (32 bit), (64 bit).
6. Windows Vista Enterprise x86-32 and x86-32 with FDCC
7. Windows 2008 Server (Standard , Enterprise and Datacenter editions).
8. Windows 7 Enterprise x86 (32 and 64 bit) and 32 bit with FDCC.
9. RHEL 4.0 for Intel x86, 5.0 for Intel x86 , 5.0 for AMD/eMT 64bit .
10. SLES 9 / 10 for Intel x86, AMD/eMT 64bit.
11. SLED 10, 11 for Intel x86, AMD/eMT 64bit .
12. SUSE (SLES) 10/11 - x86-32 , x86-64

Chapter 3. Definitions

This section defines some common terms used when using Tivoli Remote Control.

Remote control session

Establishing a connection to a computer in your environment to allow you 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 Tivoli Remote Control 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 launches 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 configurations" on page 26 for more information. For details about using the controller GUI once the session is established see the **IBM Tivoli Remote Control User's Guide**.

Managed remote control session

A remote control session in which the controller users initiates the session from the TRC server. From here the controller component is launched and contacts the target to send the session request. The target then contacts the server to authenticate the request and obtain the policies and permissions that will be set for the session. See the **IBM Tivoli Remote Control Administrators Guide** for more information on policies and permissions for a managed remote control session. If the target cannot reach the server then the session will be refused.

Note: The availability of managed remote control sessions will depend on whether you have purchased Tivoli Remote Control as a separate product and have the TRC server component installed and running.

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. See **The Policy Engine** section in the IBM Tivoli Remote Control Administrators Guide for more information on how policies and permissions are derived for a managed remote control session.

Chapter 4. Using the new Tivoli Endpoint Manager console

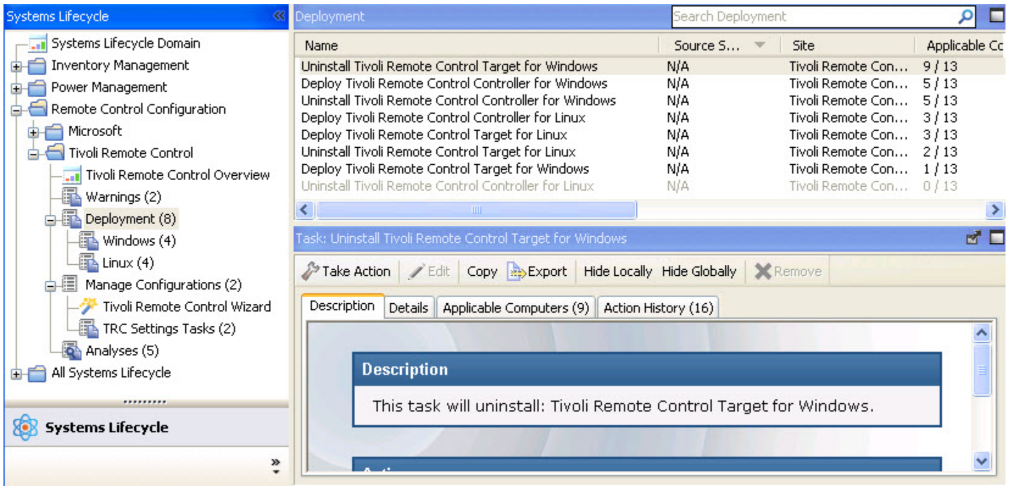
TEM Tivoli Remote Control encompasses a host of new features that provide the components required for remote takeover and monitoring of workstations and servers in your deployment.

In addition, the TEM 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 TEM Console, which is available for all Tivoli Endpoint Manager products, will serve as your central command for all Tivoli 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 TEM 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.

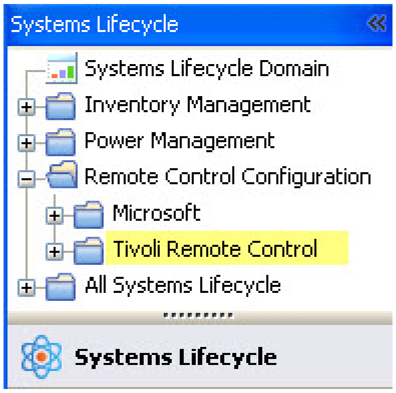


Name	Source S...	Site	Applicable Cc
Uninstall Tivoli Remote Control Target for Windows	N/A	Tivoli Remote Con...	9 / 13
Deploy Tivoli Remote Control Controller for Windows	N/A	Tivoli Remote Con...	5 / 13
Uninstall Tivoli Remote Control Controller for Windows	N/A	Tivoli Remote Con...	5 / 13
Deploy Tivoli Remote Control Controller for Linux	N/A	Tivoli Remote Con...	3 / 13
Deploy Tivoli Remote Control Target for Linux	N/A	Tivoli Remote Con...	3 / 13
Uninstall Tivoli Remote Control Target for Linux	N/A	Tivoli Remote Con...	2 / 13
Deploy Tivoli Remote Control Target for Windows	N/A	Tivoli Remote Con...	1 / 13
Uninstall Tivoli Remote Control Controller for Linux	N/A	Tivoli Remote Con...	0 / 13

Description

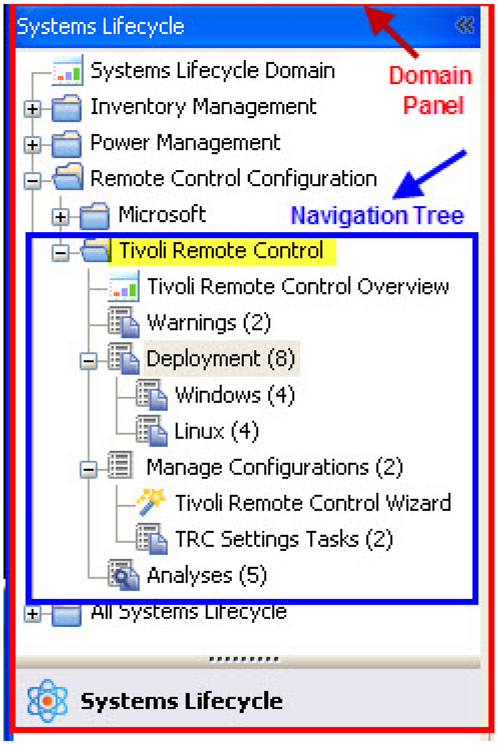
This task will uninstall: Tivoli Remote Control Target for Windows.

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



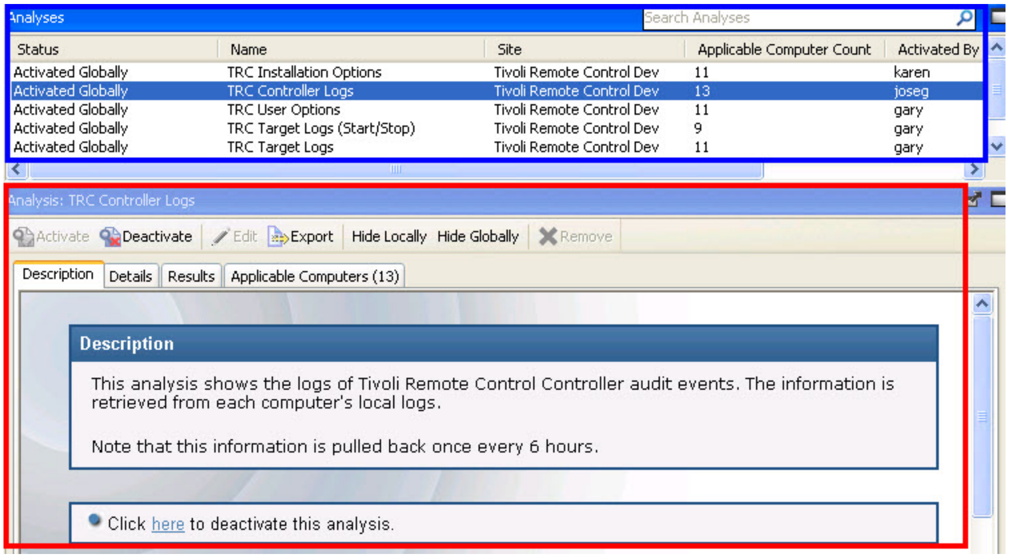
The Domain Panel is the area on the left side of the Console that includes a navigation tree and a list of all domains. The Navigation Tree includes a list of nodes and sub-nodes containing site content.

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 Tivoli Remote Control site.

Tivoli 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 or Wizard from which you will be directed to take specific actions to customise the content in your deployment.



Status	Name	Site	Applicable Computer Count	Activated By
Activated Globally	TRC Installation Options	Tivoli Remote Control Dev	11	karen
Activated Globally	TRC Controller Logs	Tivoli Remote Control Dev	13	joseg
Activated Globally	TRC User Options	Tivoli Remote Control Dev	11	gary
Activated Globally	TRC Target Logs (Start/Stop)	Tivoli Remote Control Dev	9	gary
Activated Globally	TRC Target Logs	Tivoli Remote Control Dev	11	gary

Description

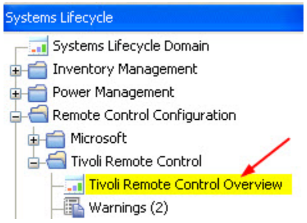
This analysis shows the logs of Tivoli Remote Control Controller audit events. The information is retrieved from each computer's local logs.

Note that this information is pulled back once every 6 hours.

- Click here to deactivate this analysis.

Chapter 5. Dashboards overview

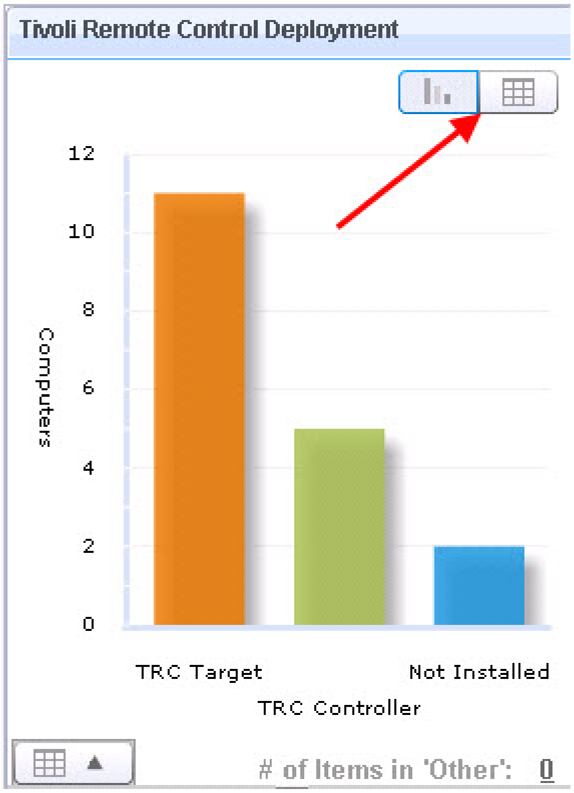
TEM Tivoli Remote Control offers a convenient dashboard for viewing the deployment distribution of the TRC components in your environment and the distribution of the type of target deployment carried out. You can access this dashboard from the top of the Tivoli Remote Control navigation tree by selecting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



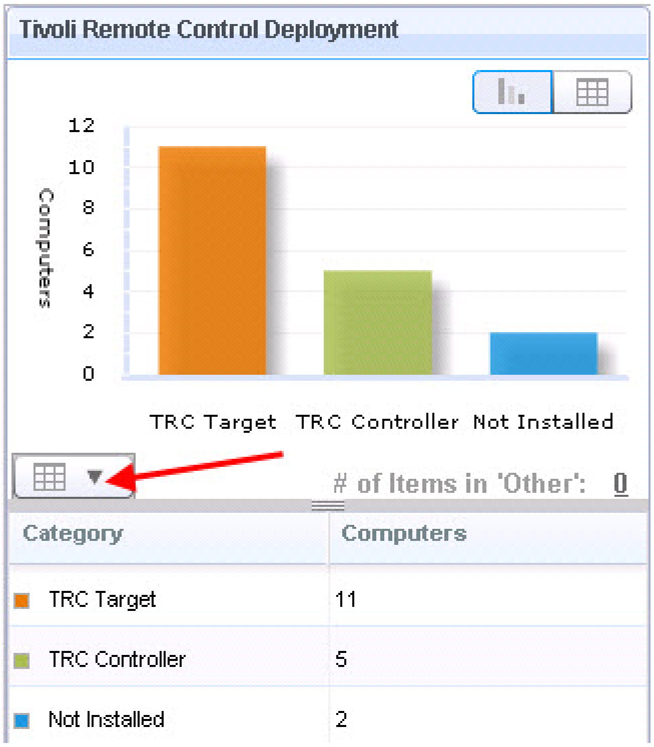
Tivoli Remote Control Overview

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

The **Tivoli Remote Control Deployment** section displays the number of computers in your environment having the various TRC 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.

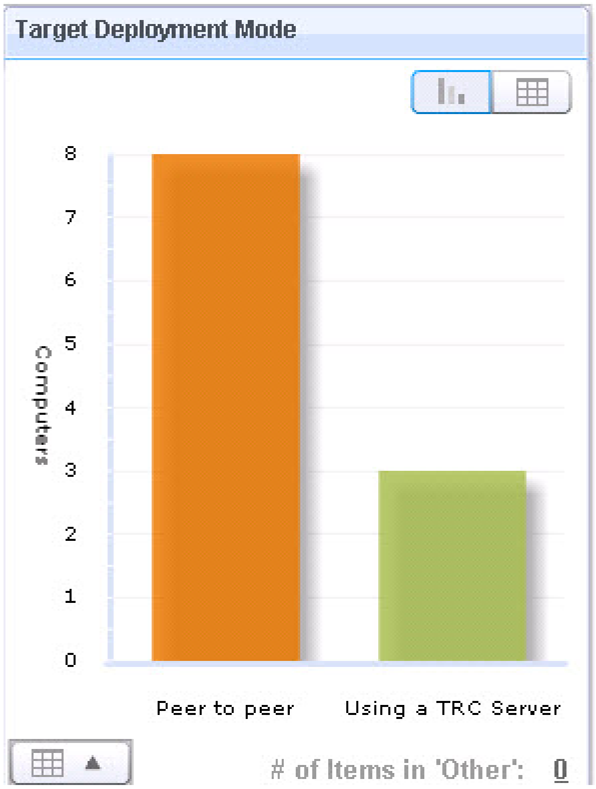


You can also view both representations of the data by clicking the button on the bottom left of the graph.



Category	Computers
🟧 TRC Target	11
🟩 TRC Controller	5
🟦 Not Installed	2

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 TRC agent software running. 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.

Chapter 6. Using Tivoli Remote Control

Tivoli Remote Control provides a suite of fixlets, tasks and wizards for deploying the components required to allow you to configure, monitor and control the computers in your environment.

Deploying TRC

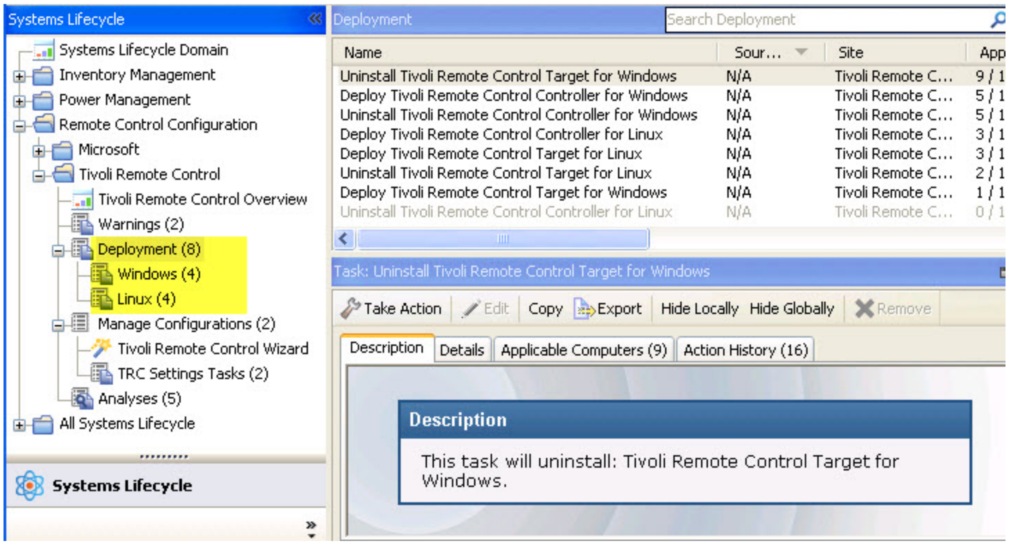
The Deployment node in the TEM Tivoli Remote Control navigation tree provides two subnodes which provide the components you need to establish a remote control session. Select the node which is relevant to the required operating system. Under each node you will find a list of tasks which allow you to deploy or remove the required TRC components.

Controller
The controller component should be deployed on the computer(s) that will initiate the remote control session when you do not have access to a TRC server.

Target The target component should be deployed on the computer(s) that will be controlled during a remote control session.

TEM Tivoli 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 more detail in the **IBM Tivoli Remote Control Users Guide**.

Note: It should be noted that the 'Using the TRC server' method requires a TRC server to have already been installed in your environment.



Name	Sour…	Site	App
Uninstall Tivoli Remote Control Target for Windows	N/A	Tivoli Remote C…	9 / 1
Deploy Tivoli Remote Control Controller for Windows	N/A	Tivoli Remote C…	5 / 1
Uninstall Tivoli Remote Control Controller for Windows	N/A	Tivoli Remote C…	5 / 1
Deploy Tivoli Remote Control Controller for Linux	N/A	Tivoli Remote C…	3 / 1
Deploy Tivoli Remote Control Target for Linux	N/A	Tivoli Remote C…	3 / 1
Uninstall Tivoli Remote Control Target for Linux	N/A	Tivoli Remote C…	2 / 1
Deploy Tivoli Remote Control Target for Windows	N/A	Tivoli Remote C…	1 / 1
Uninstall Tivoli Remote Control Controller for Linux	N/A	Tivoli Remote C…	0 / 1

Task: Uninstall Tivoli Remote Control Target for Windows

Description

This task will uninstall: Tivoli Remote Control Target for Windows.

Windows Deployment

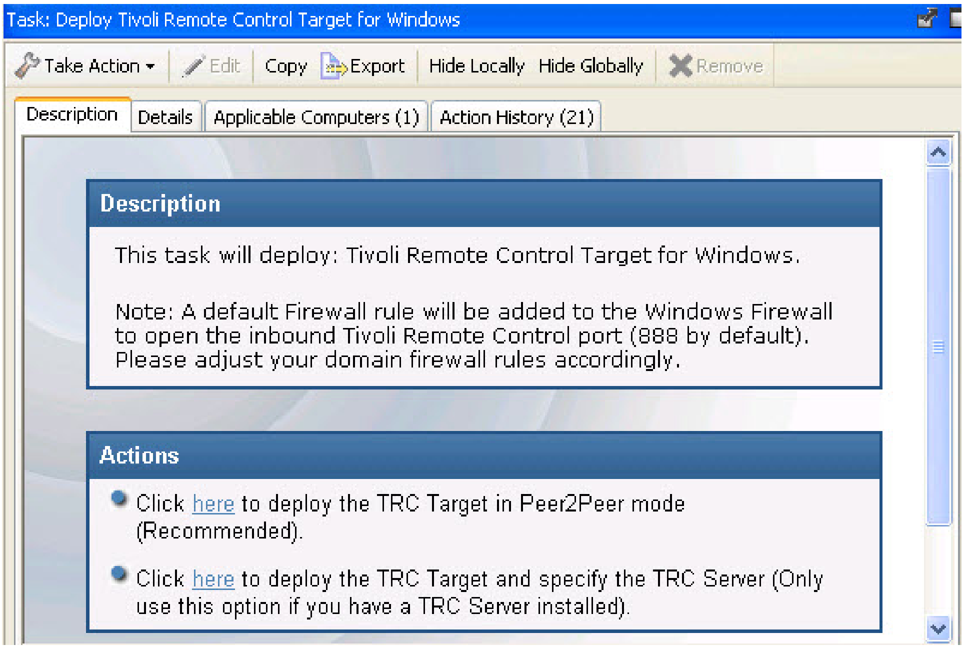
The Windows deployment node provides a set of tasks that you can use to install or remove the target and controller software in a Windows environment.

Deploying the Windows target

The **Deploy Tivoli Remote Control Target for Windows** task allows you to install the target software onto a Windows computer. To initiate this task complete the following steps:

1. Click on **Deployment** > **Windows** in the navigation tree.
2. Click **Deploy 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.



Description

This task will deploy: Tivoli Remote Control Target for Windows.

Note: A default Firewall rule will be added to the Windows Firewall to open the inbound Tivoli Remote Control port (888 by default). Please adjust your domain firewall rules accordingly.

Actions

- Click here to deploy the TRC Target in Peer2Peer mode (Recommended).
- Click here to deploy the TRC Target and specify the TRC Server (Only use this option if you have a TRC Server installed).

Deploy the TRC target in Peer2Peer mode

You can choose this installation option to allow remote control sessions to be established directly between the controller and the target without the need for a TRC server. This deployment method will install the target without requiring a TRC server URL to be specified and the local target policies set by this installation method will be used when a remote control session is established. See "Managing target configurations" on page 26 for details of the target installation properties.

In the Take Action window on the Target tab, select the required option for determining which target(s) to deploy the TRC target on.

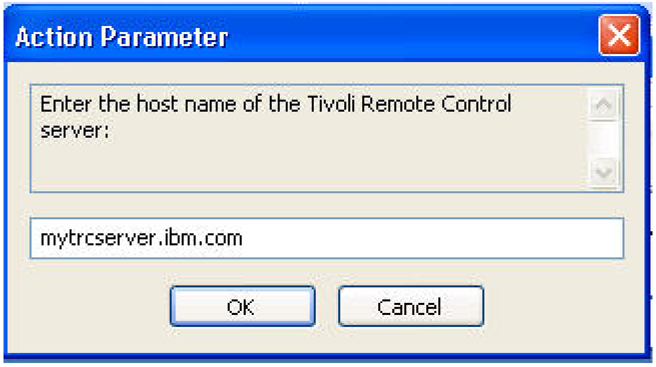
Click OK and enter your Private Key Password.

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

Deploy the TRC target and specify the TRC Server

You can chose this installation option if you would like the target(s) to register with the TRC server and take part in remote control sessions initiated from the TRC server. This deployment method will require a TRC server hostname to be specified. If a remote control session, initiated from the TRC server, is requested with this target the specified TRC server will be contacted to authenticate the request and the policies set for the session will be passed from the TRC server to the target, once authenticated, to allow the session to be established. See “Managing target configurations” on page 26 for details of the target installation properties.

Enter the hostname of your TRC server and click OK.



Enter the host name of the Tivoli Remote Control server:

mytrcserver.ibm.com

In the Take Action window on the Target tab, select the required option for determining which target(s) to deploy the TRC target on.

Click OK and enter your Private Key Password.

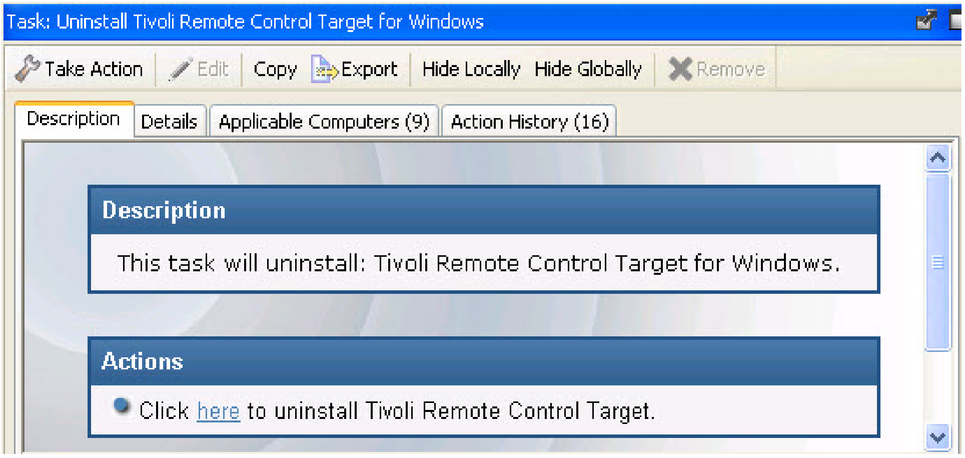
The summary screen will show the progress of the task and will show status complete when it is finished.

Note: This installation option should only be chosen if you have purchased Tivoli Remote Control 5.1.2 as a separate product and have the TRC server component installed and running.

Removing the Windows target

The **Uninstall Tivoli Remote Control Target for Windows** task allows you 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 on **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall 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.



This task will uninstall: Tivoli Remote Control Target for Windows.

Click here to uninstall Tivoli Remote Control Target.

In the Take Action window, on the Target tab, select the required option for determining which target(s) to remove the TRC target from.

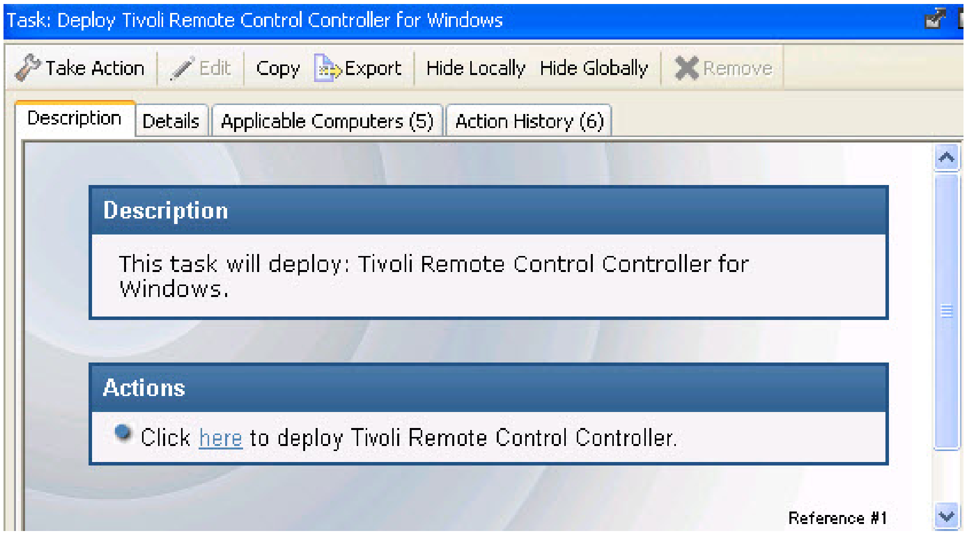
Click OK and enter your Private Key Password.

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

Deploying the Windows controller

The **Deploy Tivoli Remote Control Controller for Windows** task allows you to install the controller software onto a Windows computer. To initiate this task complete the following steps:

1. Click on **Deployment** > **Windows** in the navigation tree.
2. Click **Deploy Tivoli 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.



Description

This task will deploy: Tivoli Remote Control Controller for Windows.

Actions

Click here to deploy Tivoli Remote Control Controller.

In the Take Action window on the Target tab, select the required option for determining which target(s) to deploy the controller on.

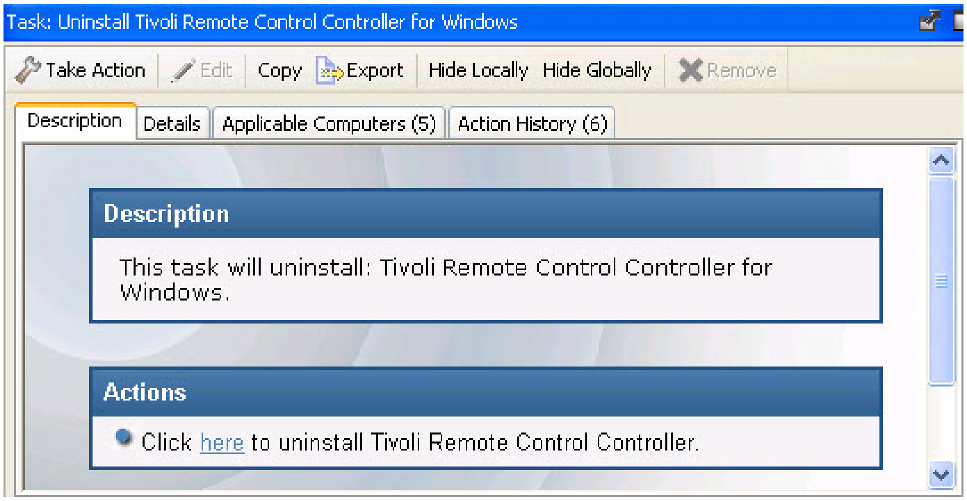
Click OK and enter your Private Key Password.

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

Removing the Windows controller

The **Uninstall Tivoli Remote Control Controller for Windows** task allows you 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 on **Deployment** > **Windows** in the navigation tree.
2. Click **Uninstall Tivoli 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.



Task: Uninstall Tivoli Remote Control Controller for Windows

Description

This task will uninstall: Tivoli Remote Control Controller for Windows.

Actions

- Click here to uninstall Tivoli Remote Control Controller.

In the Take Action window, in the Target tab , select the required option for determining which target(s) to remove the TRC controller from.

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.

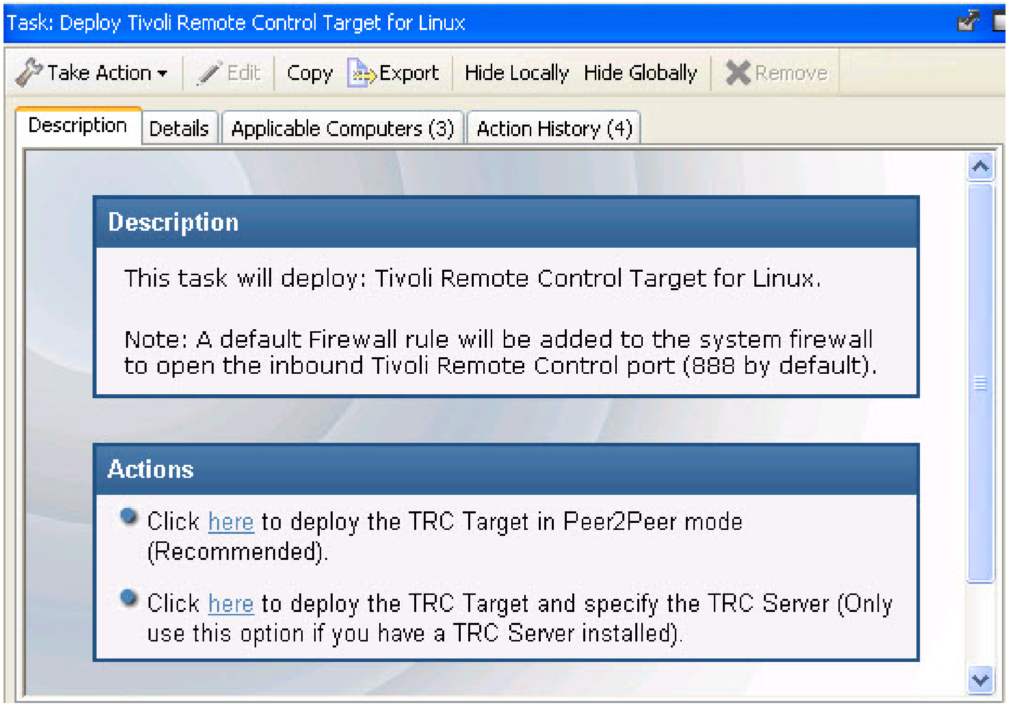
Linux Deployment

Deploying the Linux target

The **Deploy Tivoli Remote Control Target for Linux** task allows you to install the target software onto a Linux computer. To initiate this task complete the following steps:

1. Click on **Deployment** > **Linux** in the navigation tree.
2. Click **Deploy 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.



Description

This task will deploy: Tivoli Remote Control Target for Linux.

Note: A default Firewall rule will be added to the system firewall to open the inbound Tivoli Remote Control port (888 by default).

Actions

- Click here to deploy the TRC Target in Peer2Peer mode (Recommended).
- Click here to deploy the TRC Target and specify the TRC Server (Only use this option if you have a TRC Server installed).

Deploy the TRC target in Peer2Peer mode

You can chose this installation option to allow remote control sessions to be established directly between the controller and the target without the need for a TRC server. This deployment method will install the target without requiring a TRC server URL to be specified and the local target policies set by this installation method will be used when a remote control session is established. See “Managing target configurations” on page 26 for details of the target installation properties.

In the Take Action window on the Target tab, select the required option for determining which target(s) to deploy the TRC target on.

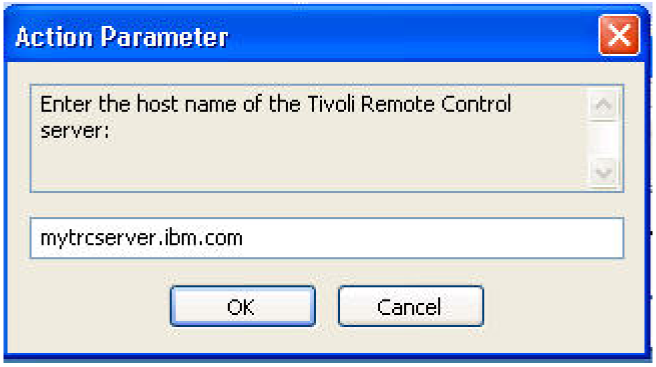
Click OK and enter your Private Key Password.

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

Deploy the TRC target and specify the TRC Server

You can choose this installation option if you would like the target(s) to register with the TRC server and take part in remote control sessions initiated from the TRC server. This deployment method will require a TRC server hostname to be specified. If a remote control session, initiated from the TRC server, is requested with this target the specified TRC server will be contacted to authenticate the request and the policies set for the session will be passed from the TRC server to the target, once authenticated, to allow the session to be established. See “Managing target configurations” on page 26 for details of the target installation properties.

Enter the hostname of your TRC server and click OK.



Enter the host name of the Tivoli Remote Control server:

mytrcserver.ibm.com

In the Take Action window on the Target tab, select the required option for determining which target(s) to deploy the TRC target on.

Click OK and enter your Private Key Password.

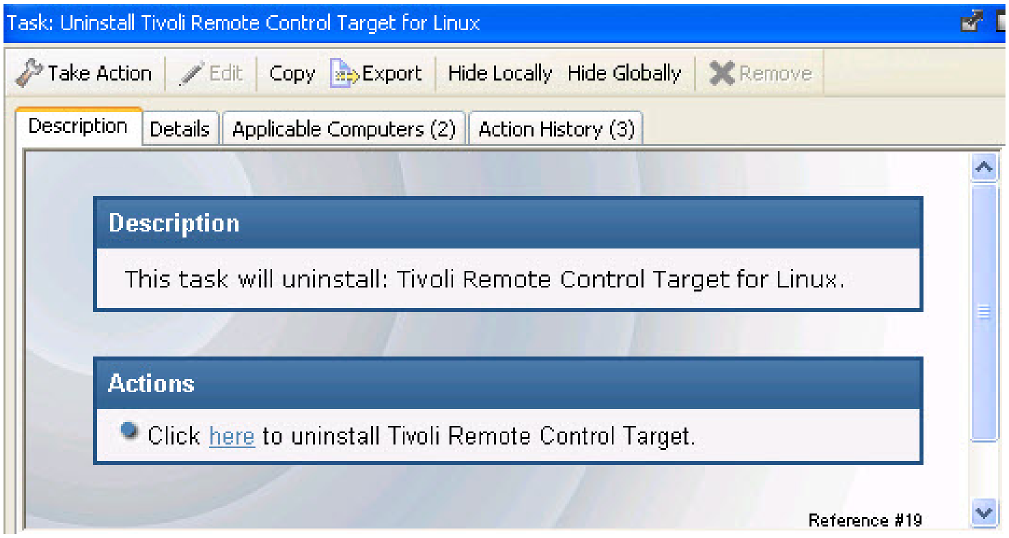
The summary screen will show the progress of the task and will show status complete when it is finished.

Note: This installation option should only be chosen if you have purchased Tivoli Remote Control 5.1.2 as a separate product and have the TRC server component installed and running.

Removing the Linux target

The **Uninstall Tivoli Remote Control Target for Linux** task allows you 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 on **Deployment** > **Linux** in the navigation tree.
2. Click **Uninstall 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.



This task will uninstall: Tivoli Remote Control Target for Linux.

Click here to uninstall Tivoli Remote Control Target.

In the Take Action window, on the Target tab, select the required option for determining which target(s) to remove the TRC target from.

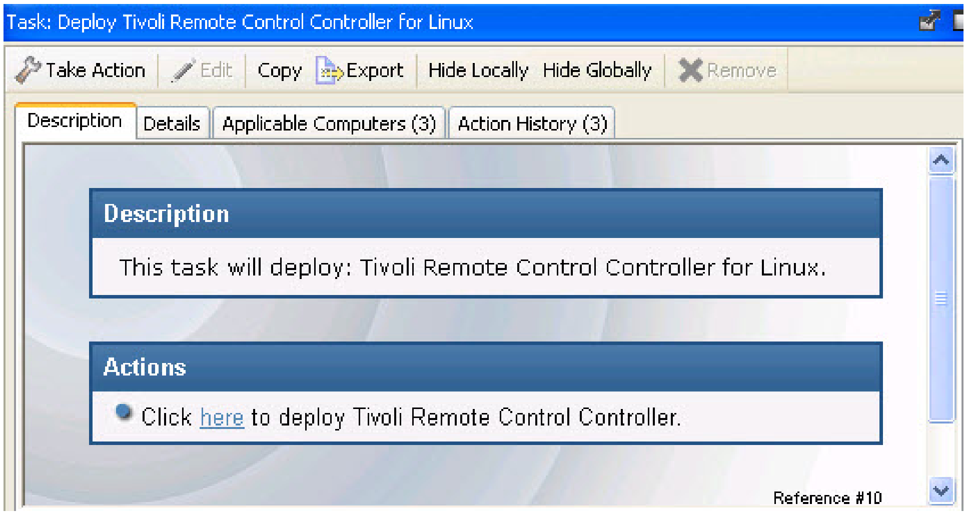
Click OK and enter your Private Key Password.

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

Deploying the Linux controller

The **Deploy Tivoli Remote Control Controller for Linux** task allows you to install the controller software onto a Linux computer. To initiate this task complete the following steps:

1. Click on **Deployment** > **Linux** in the navigation tree.
2. Click **Deploy Tivoli 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.



Description

This task will deploy: Tivoli Remote Control Controller for Linux.

Actions

- Click here to deploy Tivoli Remote Control Controller.

In the Take Action window on the Target tab, select the required option for determining which target(s) to deploy the controller on.

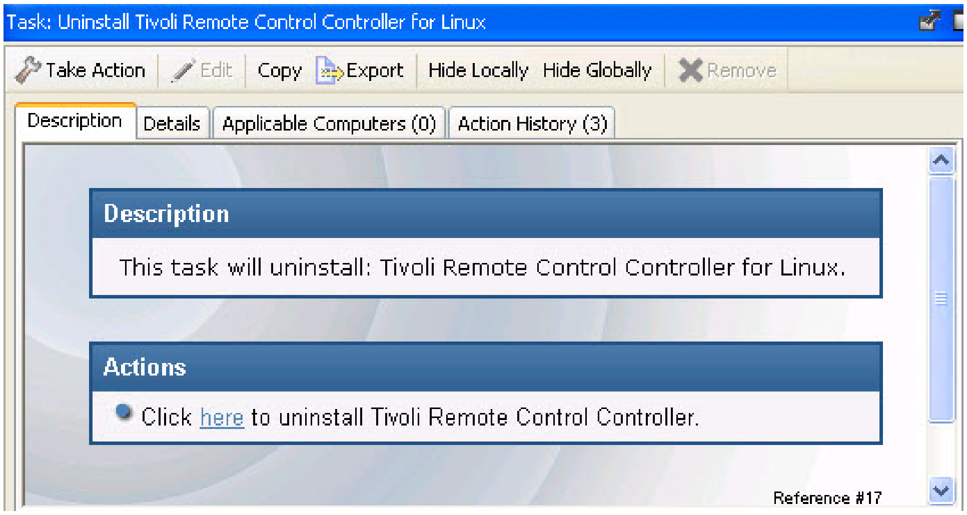
Click OK and enter your Private Key Password.

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

Removing the Linux controller

The **Uninstall Tivoli Remote Control Controller for Linux** task allows you 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 Tivoli 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.



This task will uninstall: Tivoli Remote Control Controller for Linux.

Click here to uninstall Tivoli Remote Control Controller.

In the Take Action window, in the Target tab, select the required option for determining which target(s) to remove the TRC controller from.

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.

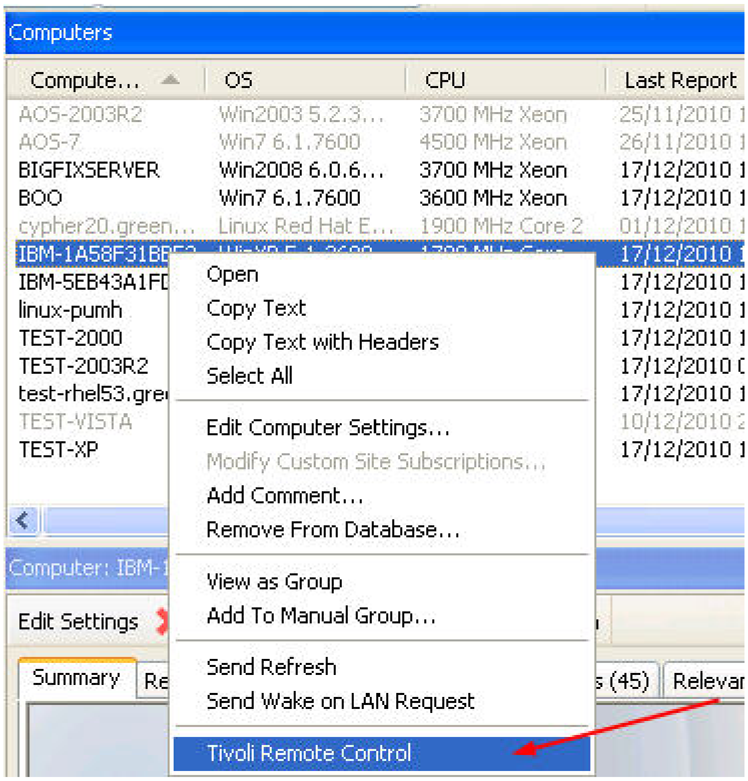
Establishing a remote control session

The TRC controller and target components can be used to establish remote connections between each other to allow you 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 TRC server, as explained in Chapter 3, “Definitions,” on page 5. The TEM console provides a method for establishing a peer to peer session directly from the console.

Note: This method is only available when you have the controller component installed on the same system as the TEM console.

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

1. From the list of computers **Right Click** on the computer that you want to establish a remote control session with.
2. Select **Tivoli Remote Control**.

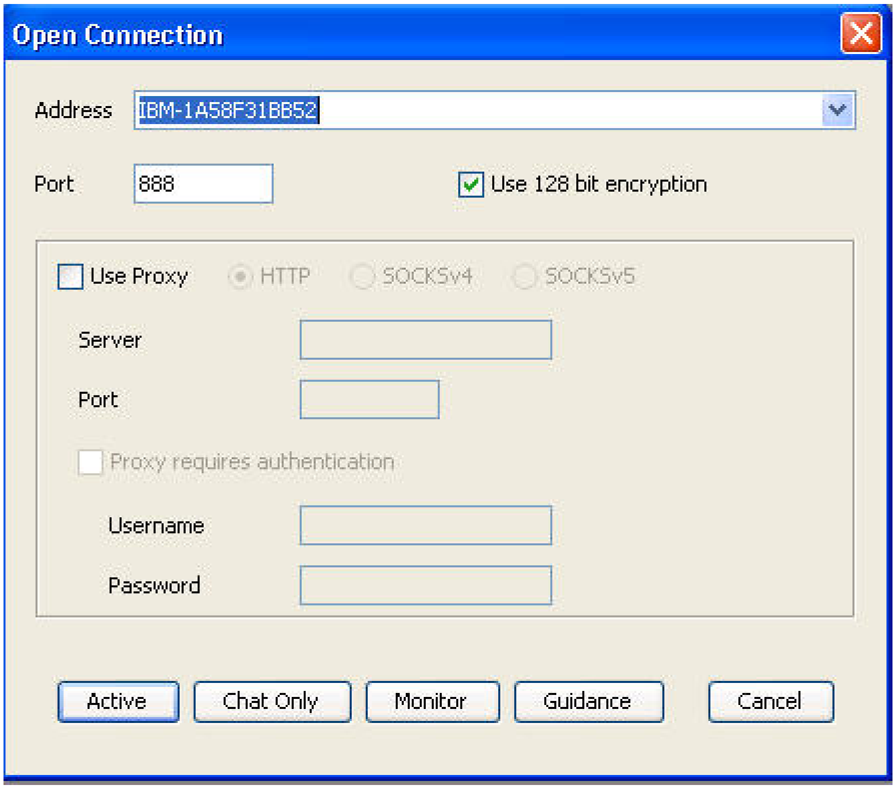


Computers

Compute...	OS	CPU	Last Report
AOS-2003R2	Win2003 5.2.3...	3700 MHz Xeon	25/11/2010 1
AOS-7	Win7 6.1.7600	4500 MHz Xeon	26/11/2010 1
BIGFIXSERVER	Win2008 6.0.6...	3700 MHz Xeon	17/12/2010 1
BOO	Win7 6.1.7600	3600 MHz Xeon	17/12/2010 1
cypher20.green...	Linux Red Hat E...	1900 MHz Core 2	01/12/2010 1
IBM-1A58F31BB			17/12/2010 1
IBM-5EB43A1FD			17/12/2010 1
linux-pumh			17/12/2010 1
TEST-2000			17/12/2010 1
TEST-2003R2			17/12/2010 0
test-rhel53.gre			17/12/2010 1
TEST-VISTA			10/12/2010 2
TEST-XP			17/12/2010 1

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

3. On the Open connection dialog if you require to use a proxy select **use proxy** and enter the relevant details. Select the session type required. See the **IBM Tivoli Remote Control User's Guide** for more information on the session types which can be established.



Open Connection

Address IBM-1A58F31BB52

Port 888

☑ Use 128 bit encryption

□ Use Proxy ● HTTP ○ SOCKSv4 ○ SOCKSv5

Server

Port

□ Proxy requires authentication

Username

Password

Notes:

a. If the target has Windows installed, a login window may appear. You must enter a valid windows id and password to continue.

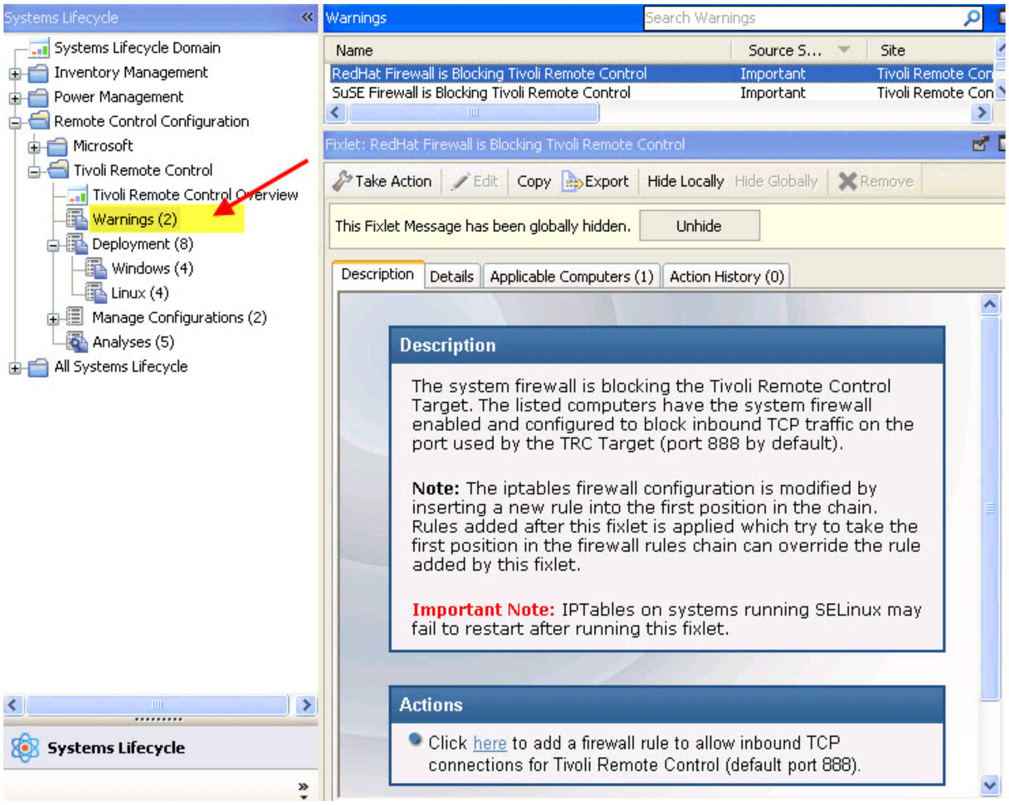
b. A user acceptance dialog may be presented to the target user to allow them to accept or reject the session, depending on the policies set on the target.

When the session is accepted, it will be established and the policies set locally on the target will determine what actions can be carried out during the session. See the **IBM Tivoli Remote Control User's Guide** for more information on peer to peer sessions and the functionality available in the controller GUI.

For details of how to end a remote control session see **Ending a session** in the Tivoli Remote Control Users's Guide.

Responding to warnings

During the discovery process if there are any issues found which interfere with the normal operation of the TRC components, a set of fixlets will be displayed in the Warnings section to allow you to take action and resolve these issues on any applicable computers. When the TRC target software is installed a default firewall rule is created to open the inbound Tivoli 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 allow inbound TCP connections for Tivoli Remote Control.



Name	Source S...	Site
RedHat Firewall is Blocking Tivoli Remote Control	Important	Tivoli Remote Con
SuSE Firewall is Blocking Tivoli Remote Control	Important	Tivoli Remote Con

This Fixlet Message has been globally hidden.

Description

The system firewall is blocking the Tivoli Remote Control Target. The listed computers have the system firewall enabled and configured to block inbound TCP traffic on the port used by the TRC Target (port 888 by default).

Note: The iptables firewall configuration is modified by inserting a new rule into the first position in the chain. Rules added after this fixlet is applied which try to take the first position in the firewall rules chain can override the rule added by this fixlet.

Important Note: IPTables on systems running SELinux may fail to restart after running this fixlet.

Actions

- Click here to add a firewall rule to allow inbound TCP connections for Tivoli Remote Control (default port 888).

Managing target configurations

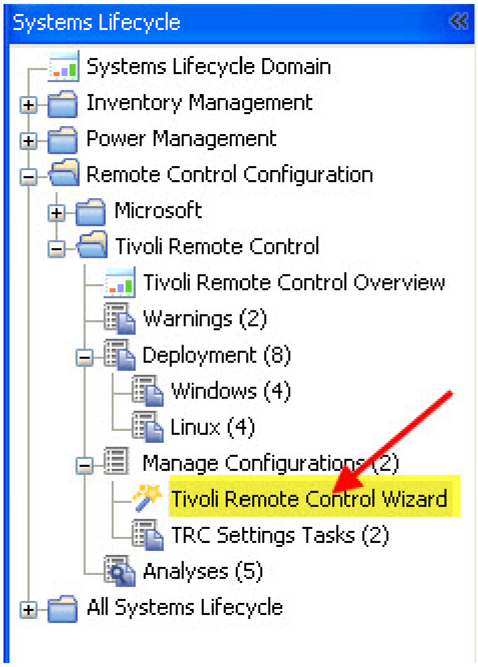
Tivoli Remote Control provides a wizard that allows you to create TRC target configuration tasks which can be performed on all, or specific, targets to alter their current configuration settings. The purpose of these tasks is to create a set of configuration parameters which will determine what types of session the target(s) can take part in, that is, peer to peer or initiated from the server and will also determine what actions can be carried out by the controller user during a remote control session. Installation and User Options can both be configured. For more details about these options see the **IBM Tivoli Remote Control Installation Guide**.

Tivoli Remote Control Wizard

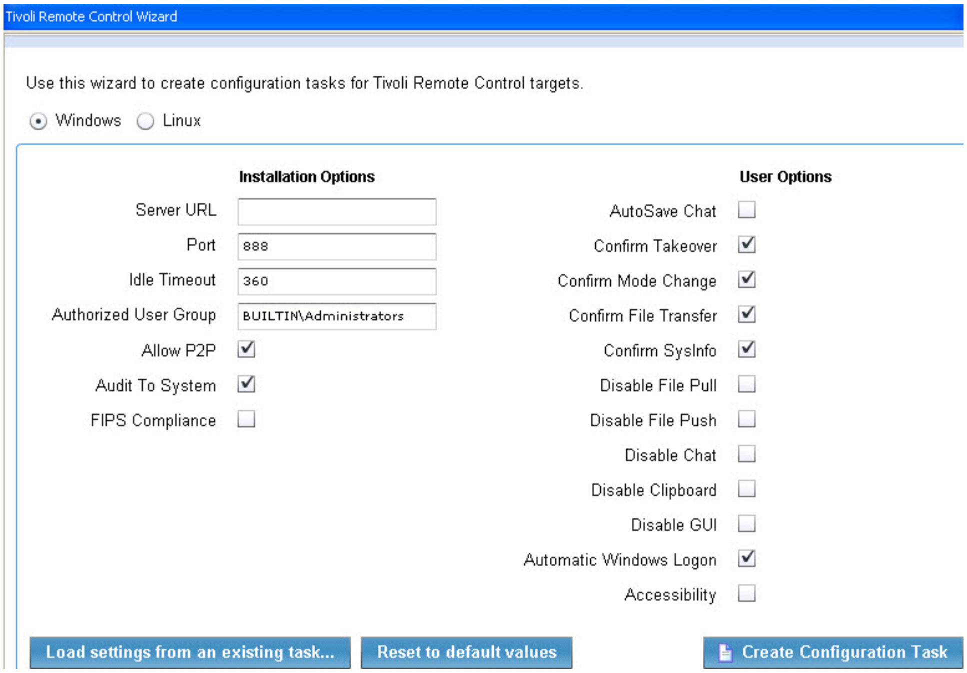
To create a configuration task complete the following steps:

Note: It should be noted that the configuration values set here will only be in effect when a peer to peer session is requested with a target. If a remote control session is initiated from the TRC server, the session policies will be passed to the target from the server.

1. In the Tivoli Remote Control navigation tree select **Tivoli Remote Control Wizard**.



2. In the **Tivoli Remote Control Wizard** select the required operating system.


Tivoli Remote Control Wizard
Load settings from an existing task...
Reset to default values
Create Configuration Task

Use this wizard to create configuration tasks for Tivoli Remote Control targets.

● Windows ○ Linux

Installation Options		User Options	
Server URL		AutoSave Chat	□
Port	888	Confirm Takeover	☑
Idle Timeout	360	Confirm Mode Change	☑
Authorized User Group	BUILTIN\Administrators	Confirm File Transfer	☑
Allow P2P	☑	Confirm SysInfo	☑
Audit To System	☑	Disable File Pull	□
FIPS Compliance	□	Disable File Push	□
		Disable Chat	□
		Disable Clipboard	□
		Disable GUI	□
		Automatic Windows Logon	☑
		Accessibility	□

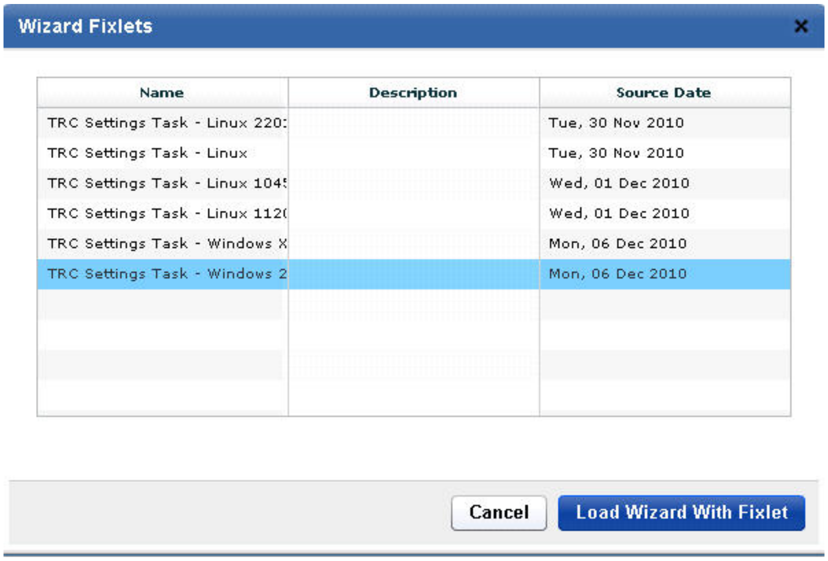
3. Set your configuration values.

   Load settings from an existing task

   You can use this feature to load configuration settings which have been previously saved.

   a. Click **Load settings from an existing task**.

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



Name	Description	Source Date
TRC Settings Task - Linux 220		Tue, 30 Nov 2010
TRC Settings Task - Linux		Tue, 30 Nov 2010
TRC Settings Task - Linux 104		Wed, 01 Dec 2010
TRC Settings Task - Linux 112		Wed, 01 Dec 2010
TRC Settings Task - Windows X		Mon, 06 Dec 2010
TRC Settings Task - Windows 2		Mon, 06 Dec 2010

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.

Selecting configuration values

The wizard is loaded with default configuration values which you can change to your own requirements by selecting or deselecting the relevant installation and user options.

Installation Options

Table 1. Installation option descriptions

Installation option	Default Value	Description
Server URL	blank	If you have a TRC server running and you want the target to register with the TRC server and take part in remote control sessions initiated from the server, provide the TRC server url. **Note:** If you provide a server url and want the target(s) that this task is performed on to only take part in remote control sessions initiated from the server you should deselect the AllowP2P option.
Port	888	Specify the TCP port that you want the target to listen on.
AllowP2P	Selected	Used to enable peer to peer mode. **Selected** 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 has also been provided the target(s) can take part in both peer to peer sessions and those initiated from the server. **Not selected** A peer to peer session cannot be established between a controller and this target. If a serverURL has been provided the target(s) can only take part in remote control sessions initiated from the server.
Idle timeout	360	Specify the number of seconds to wait before stopping the connection automatically if there is no remote control session activity. Setting this value to 0 effectively disables the timer and the session will not timeout . The minimum timeout value is 60 seconds so a value >0 and <60 will timeout about 60 seconds and values >60 will timeout when value is reached . The default value is 360. **Note:** This value should be set to 0 for sessions which don't involve sending or receiving information from the controller to the target. For example in Monitor sessions.

Table 1. Installation option descriptions (continued)

Installation option	Default Value	Description

Authorized User Group	See description.	Default value is
		Windows `BUILTIN\Administrators`
		Linux `wheel`
		When Authorized User Group has a value set, the username used for authentication must be a member of one of the groups listed, otherwise, the session will be refused. Multiple groups should be separated with a semicolon,
		`for example:Authorized User Group 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. If the user(s) you want to grant access to should also be granted administrator rights, add them as members of the Administrators group on Windows or the wheel group on Linux.
		2. If the user(s) you want to grant access to should not have administrator rights you can complete the following steps
		a. Create a new group or use an existing group.
		`For example, the following command could be executed as root`
		`groupadd trcusers`
		b. Add the user(s) to this group.
		`For example, the following command could be executed 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.

AuditToSystem	Selected	Determines the ability to log the actions that are carried out during remote control sessions to the application event log on the target, which can then be used for audit purposes **Selected** Entries will appear in the application event log of the target corresponding to the each action carried out during the session. **Not selected** No entries will be logged to the application event log.
FIPS Compliance	Not selected	Select this option to enable the use of a FIPS certified cryptographic provider for all cryptographic functions. See the **IBM Tivoli Remote Control Installation Guide** for more information on enabling FIPS compliancy. **Note:** If you enable FIPS compliance on the target you will also have to enable FIPS compliance on the controller components that you have installed. Only the IBM Java Run-time Environment (JRE) is supported in FIPS compliant mode and this 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 install dir]***\trc_controller.properties where ***[controller install dir]*** is the installation directory chosen when installing the controller. **Linux** opt/ibm/trc/controller/trc_controller.properties 2. Set the **fips.compliance** property to true and save the file.

User Options

User options determine the policies that will be set for a controller user when they establish a direct remote control session with the target(s).

Note: If a server url is supplied and the remote control session is initiated from the TRC server these policies will be overridden by policies passed from the server.

Table 2. User option descriptions

User options	Default Value	Description

AutoSaveChat	Not selected	Determines the ability to save the chat dialog entered during a chat session.
		Selected The chat dialog is saved as an html file with name starting 'chat', in the working directory of the target whose location is defined by the target property WorkingDir.
		`for example in Windows: chat-m15.html`
		`saved to the following location`
		`c:\Documents and Settings\All Users`
		`\Application Data\IBM\Tivoli\Remote Control`
		Not selected
		The chat dialog will not be saved to a file.

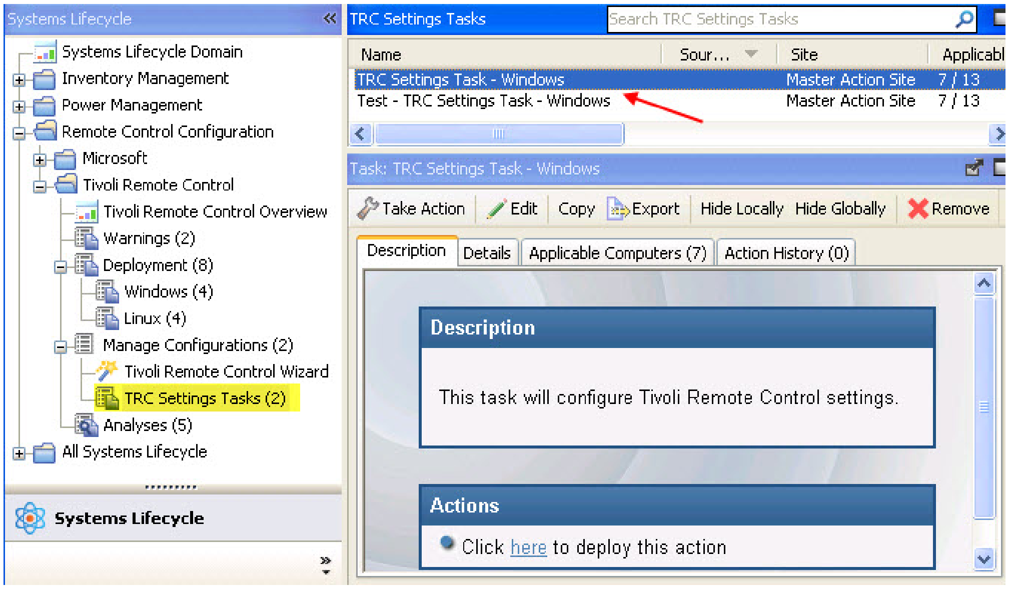
ConfirmTakeover	Selected	Determines the appearance of the user acceptance dialog when a remote control session is requested **Selected** The user acceptance dialog will appear to the target user who can accept or refuse the session. **Not selected** The user acceptance dialog does not appear and the session is established.
ConfirmModeChange	Selected	Determines the appearance of the user acceptance dialog when the controller user selects a different session mode from the session mode list on the controller window. **Selected** The user acceptance dialog 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 dialog is not displayed and the session mode is changed automatically.
ConfirmFileTransfer	Selected	Determines the appearance of the user acceptance dialog when the controller user wants to transfer files from the target to the controller. **Selected** The acceptance dialog is displayed in the following two cases forcing the target user to accept or refuse the file transfer. • If the controller user selects **pull file** from the file transfer menu on the controller window **Note:** The target user must select the file, that is to be transferred, after they have accepted the request. • If the controller user selects **send file to controller** from the Actions menu in the target window **Not selected** The acceptance dialog is not displayed and files are transferred automatically from the target to the controller system when requested.
ConfirmSysInfo	Selected	Determines the appearance of the user acceptance dialog when the controller user requests to view the target system information **Selected** When the controller user clicks on the system information icon in the controller window, the user acceptance dialog is displayed. The **target user** must now accept or refuse the request to view the target system information. 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 on the system information icon.
DisableFilePull	Not selected	Determines the ability to transfer files during the session from the target to the controller. **Selected** Files can be transferred from the target to the controller **Not selected** Files cannot be transferred from the target to the controller
DisableFilePush	Not selected	Determines the ability to transfer files during the session from the controller to the target. **Selected** Files can be transferred from the controller to the target. **Not selected** Files cannot be transferred from the controller to the target

Table 2. User option descriptions (continued)

User options	Default Value	Description
DisableChat	Not selected	Determines the ability to start a chat session with the target and also chat to the controller user during the peer to peer session. **Selected** If ChatOnly is chosen as the connection type on the open connection screen the session will be refused. The chat icon is not available during the session. **Not selected** A Chat Only session can be initiated from the open connection window. The chat icon is available during the session.
DisableClipboard	Not selected	Determines the availability of the clipboard transfer menu which gives you the ability 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 allow you to transfer the clipboard content to and from the target. **Not selected** The clipboard transfer menu is not available during the session.
Disable GUI	Not selected	Determines the appearance of the target GUI when the remote control session is starting and during the session. **Note:** This option only works when the target(s) that it will be applied to has been installed in peer to peer mode. This option will be ignored when applied to any target(s) that were installed using the TRC server mode when a server URL was supplied. **Selected** The GUI will not appear on the target and the session will be established without the target user being aware of the action. The TRC target icon will not be visible in the Windows system tray. **Not selected** The GUI will appear on the target as the session is starting and will be available to the target user during the remote control session.
Automatic Windows Login	Selected	Determines the appearance of the user acceptance dialog on a target where the user is not logged on. **Selected** The acceptance dialog will not appear on the target and the session will be established. **Not selected** The session will be refused as there is no user logged on at the target to accept the session.
Accessibility	Not selected	Select this option to enable the accessibility GUI. Available when Windows is selected as the operating system.

4. Click **Create Configuration Task**. Fill in the required information for your task and click **OK**.
5. Enter your private key password and click OK.

Your task will now be displayed in the list panel of the TRC Settings Tasks sub node.



Name	Sour...	Site	Applicabl
TRC Settings Task - Windows		Master Action Site	7 / 13
Test - TRC Settings Task - Windows		Master Action Site	7 / 13

Description

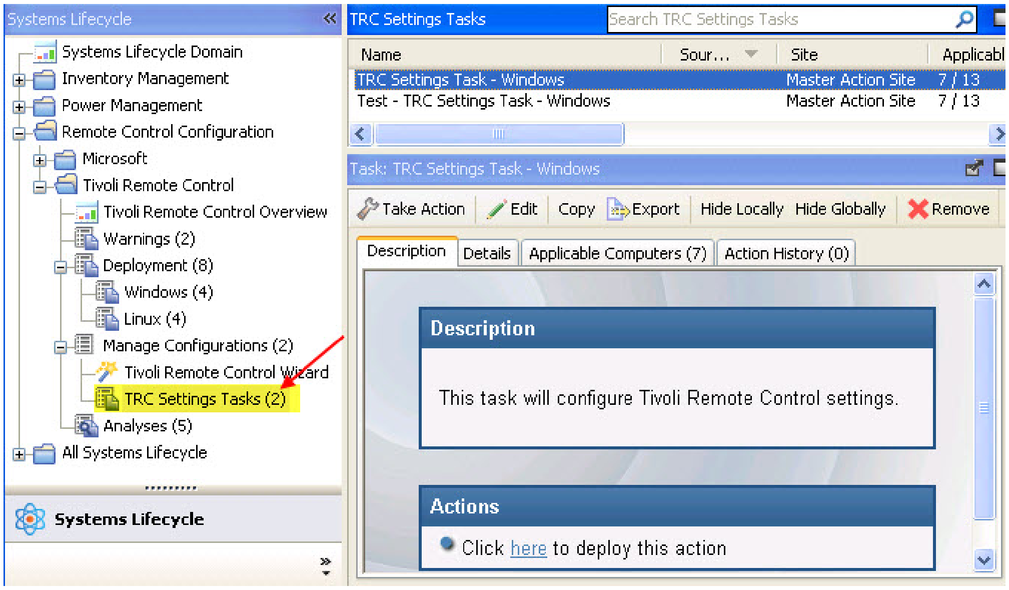
This task will configure Tivoli Remote Control settings.

Actions

- Click here to deploy this action

TRC Settings Tasks

You can use the TRC Settings Tasks section to execute the configuration tasks that you created using the Tivoli Remote Control 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.



Name	Sour...	Site	Applicabl
TRC Settings Task - Windows		Master Action Site	7 / 13
Test - TRC Settings Task - Windows		Master Action Site	7 / 13

Description

This task will configure Tivoli Remote Control settings.

Actions

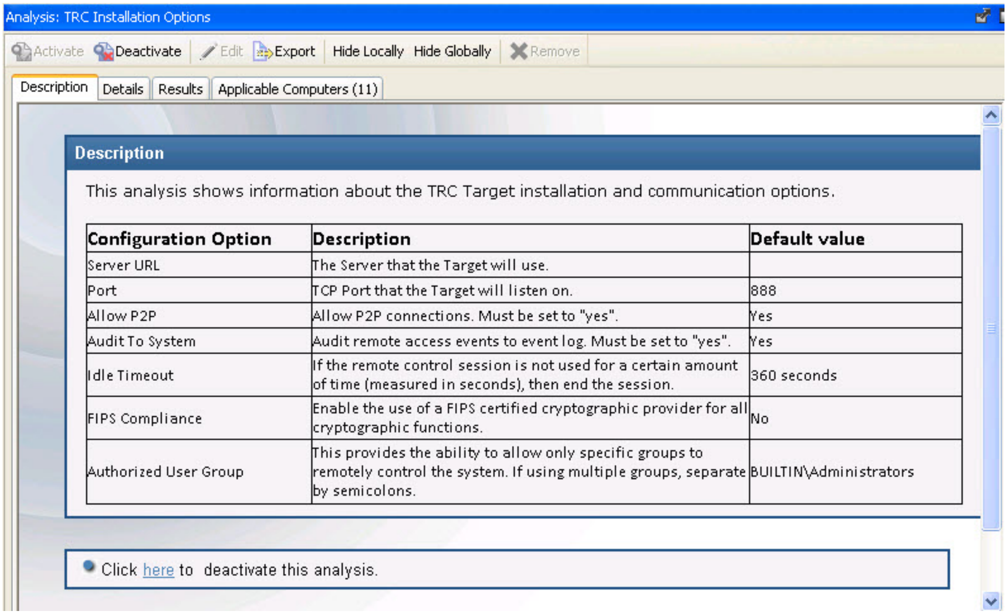
- Click here to deploy this action

Analyses

The Analyses sub-node provides a set of analyses which gather installation, user and audit information. This data will provide you with a history of remote control connection events which have taken place on the computers in your environment that have the controller or target components installed. These analyses are activated globally therefore any computer(s) in your environment, for whom the analysis is relevant, will report their values.

TRC Installation Options

The TRC Installations Options analysis is used for gathering installation property values from targets in your environment that have the TRC target software running. The values returned for these properties will allow you to determine which type of remote control session(s) that a target can take part in. See step 3c on page 28 for installation option definitions.



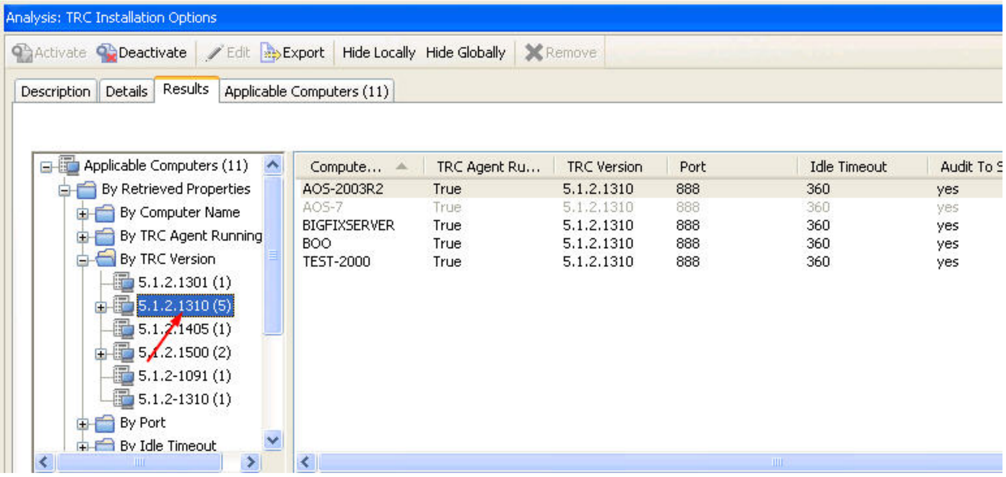
Description

This analysis shows information about the TRC Target installation and communication options.

Configuration Option	Description	Default value
Server URL	The Server that the Target will use.	
Port	TCP Port that the Target will listen on.	888
Allow P2P	Allow P2P connections. Must be set to "yes".	Yes
Audit To System	Audit remote access events to event log. Must be set to "yes".	Yes
Idle Timeout	If the remote control session is not used for a certain amount of time (measured in seconds), then end the session.	360 seconds
FIPS Compliance	Enable the use of a FIPS certified cryptographic provider for all cryptographic functions.	No
Authorized User Group	This provides the ability to allow only specific groups to remotely control the system. If using multiple groups, separate by semicolons.	BUILTIN\Administrators

● Click here to deactivate this analysis.

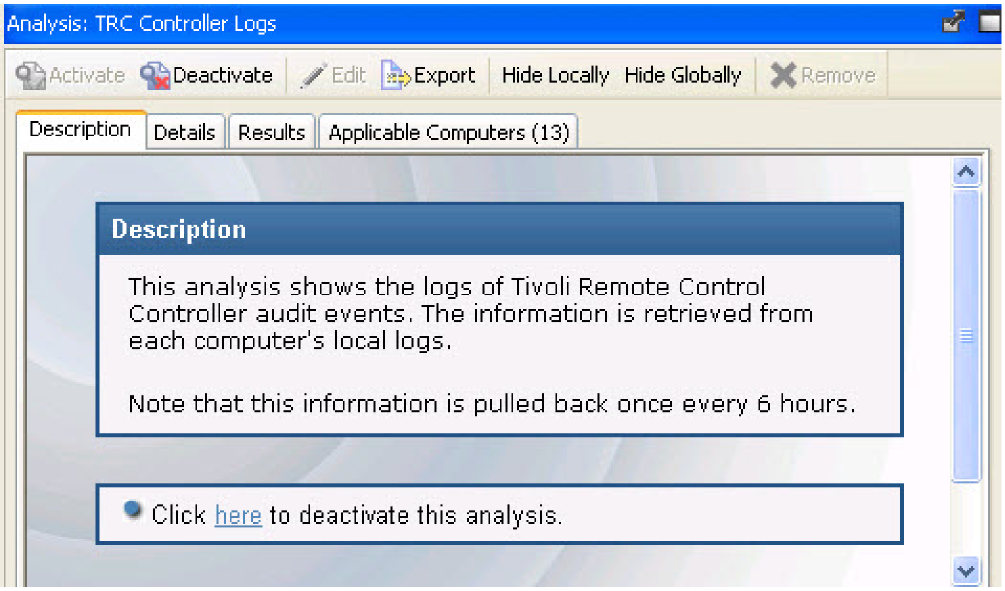
If the analysis is active, the Results tab will list the computers that this analysis was relevant for and the values of the installation options will be displayed. You can expand the Applicable Computers entry and filter the data further by specific retrieved properties. This can be useful in many ways, 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 TRC targets. For example, to determine which targets are running TRC target version 1310, expand **By TRC Version** and select 5.1.2.1310. The list of targets having this version of software installed is listed on the right.



Compute...	TRC Agent Ru...	TRC Version	Port	Idle Timeout	Audit To S
AOS-2003R2	True	5.1.2.1310	888	360	yes
AOS-7	True	5.1.2.1310	888	360	yes
BIGFIXSERVER	True	5.1.2.1310	888	360	yes
BOO	True	5.1.2.1310	888	360	yes
TEST-2000	True	5.1.2.1310	888	360	yes

TRC Controller Logs

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



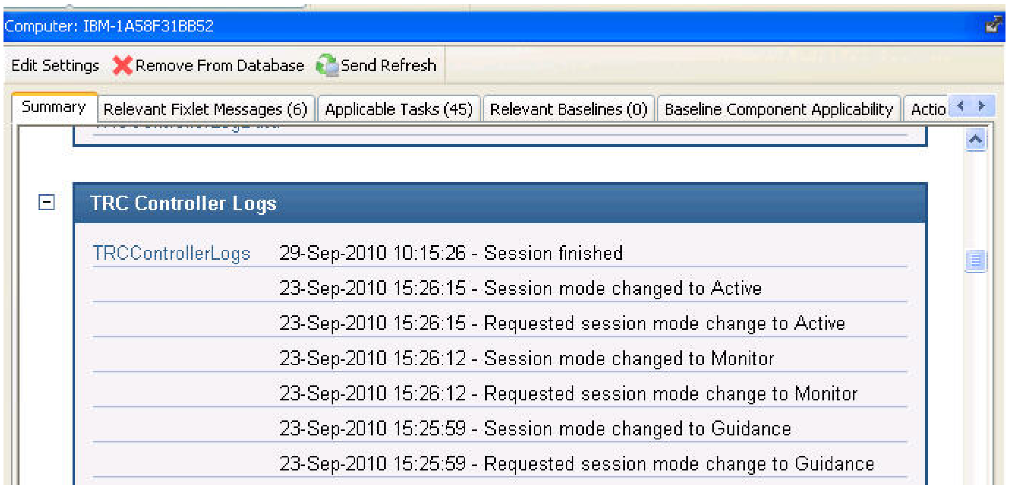
Description

This analysis shows the logs of Tivoli Remote Control Controller audit events. The information is retrieved from each computer's local logs.

Note that this information is pulled back once every 6 hours.

Click here to deactivate this analysis.

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

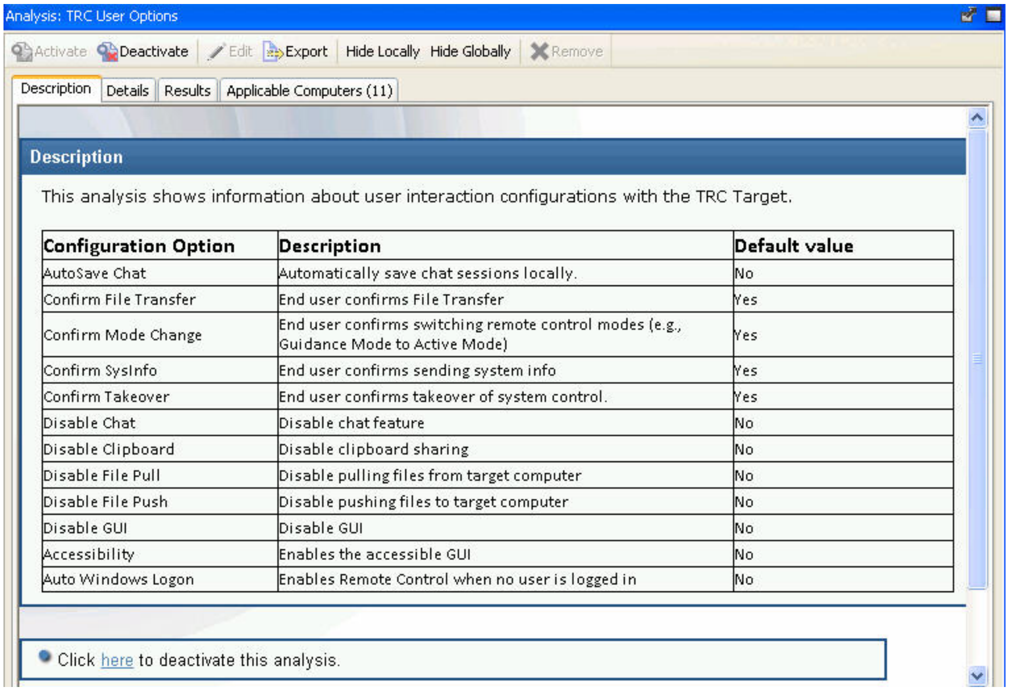


TRC Controller Logs

TRCControllerLogs	29-Sep-2010 10:15:26 - Session finished
	23-Sep-2010 15:26:15 - Session mode changed to Active
	23-Sep-2010 15:26:15 - Requested session mode change to Active
	23-Sep-2010 15:26:12 - Session mode changed to Monitor
	23-Sep-2010 15:26:12 - Requested session mode change to Monitor
	23-Sep-2010 15:25:59 - Session mode changed to Guidance
	23-Sep-2010 15:25:59 - Requested session mode change to Guidance

TRC User Options

The **TRC User Options** analysis is used for gathering user options property values from targets in your environment that have the TRC target software running. These properties are used to determine what actions the controller user can carry out during a remote control session with this target. See step 3c on page 28 for user option definitions.



Description

This analysis shows information about user interaction configurations with the TRC Target.

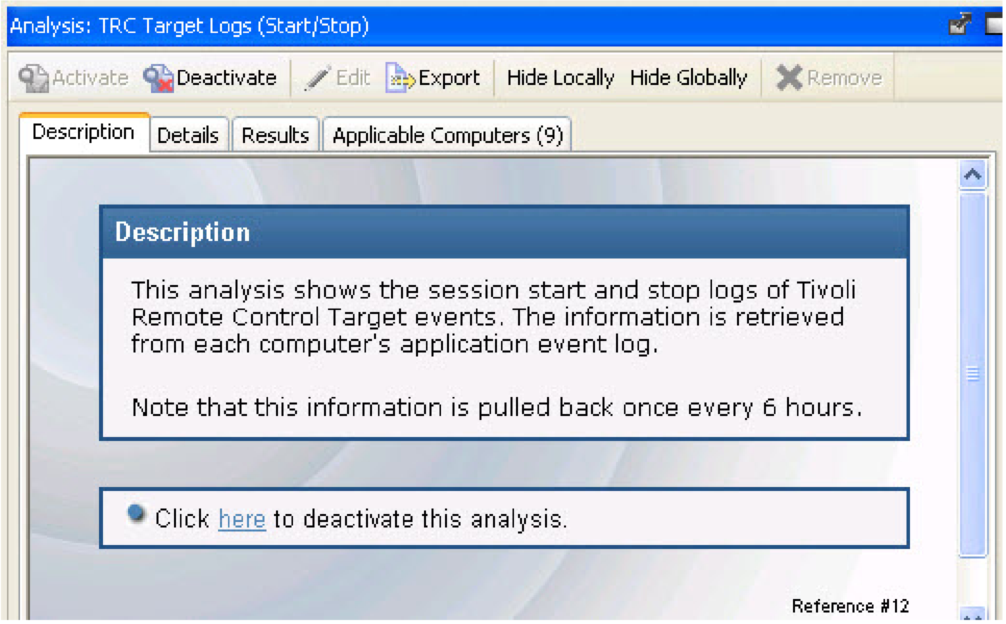
Configuration Option	Description	Default value
AutoSave Chat	Automatically save chat sessions locally.	No
Confirm File Transfer	End user confirms File Transfer	Yes
Confirm Mode Change	End user confirms switching remote control modes (e.g., Guidance Mode to Active Mode)	Yes
Confirm SysInfo	End user confirms sending system info	Yes
Confirm Takeover	End user confirms takeover of system control.	Yes
Disable Chat	Disable chat feature	No
Disable Clipboard	Disable clipboard sharing	No
Disable File Pull	Disable pulling files from target computer	No
Disable File Push	Disable pushing files to target computer	No
Disable GUI	Disable GUI	No
Accessibility	Enables the accessible GUI	No
Auto Windows Logon	Enables Remote Control when no user is logged in	No

● Click here to deactivate this analysis.

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

TRC Target Log (Start/Stop)

The TRC Target Log (Start/Stop) analysis is used for gathering the audit events from any computers in your environment that have the TRC target component installed. The information is retrieved and updated once 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 TRC Target Log analysis.



Description

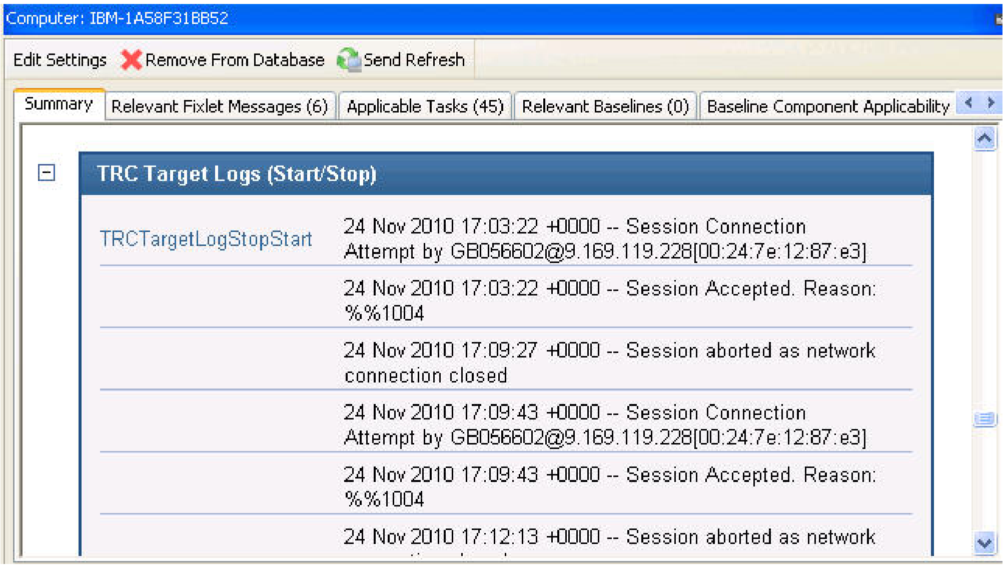
This analysis shows the session start and stop logs of Tivoli Remote Control Target events. The information is retrieved from each computer's application event log.

Note that this information is pulled back once every 6 hours.

Click here to deactivate this analysis.

Reference #12

If the analysis is active, the Results tab will list the computers that this analysis was relevant for. If you double click on a computer you will see summary data for the selected computer which includes a section for the target log start/stop entries retrieved by the **TRC Target Logs** analysis. You can also expand the Applicable Computers entry and filter the data further by specific retrieved properties.

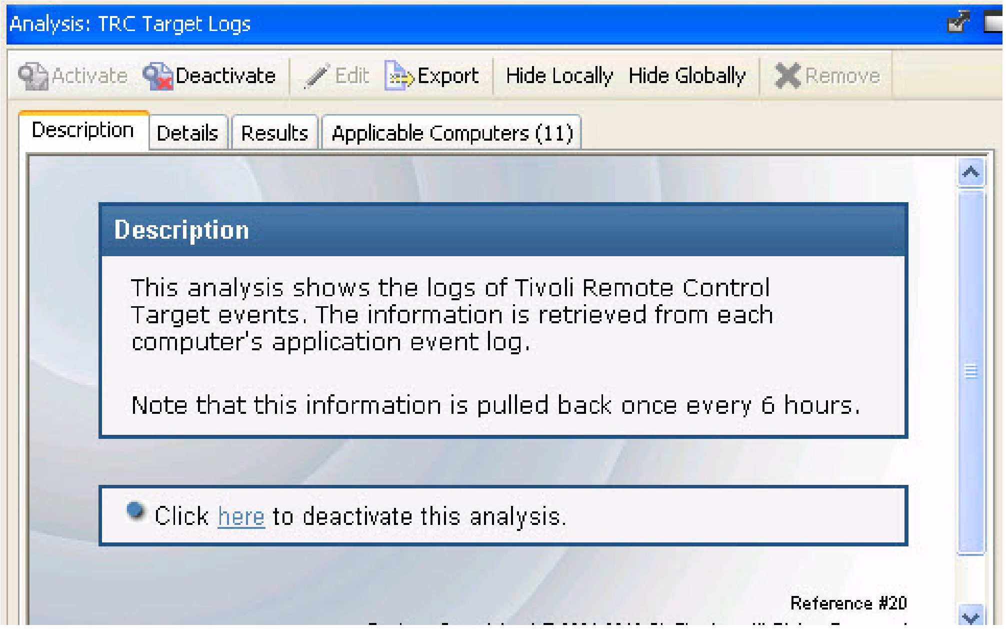


TRC Target Logs (Start/Stop)

TRCTargetLogStopStart	24 Nov 2010 17:03:22 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
	24 Nov 2010 17:03:22 +0000 -- Session Accepted. Reason: %%1004
	24 Nov 2010 17:09:27 +0000 -- Session aborted as network connection closed
	24 Nov 2010 17:09:43 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
	24 Nov 2010 17:09:43 +0000 -- Session Accepted. Reason: %%1004
	24 Nov 2010 17:12:13 +0000 -- Session aborted as network

TRC Target Log

The **TRC Target Logs** analysis is used for gathering the audit events from any computers in your environment that have the TRC target component installed. The information is retrieved and updated once 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.



Description

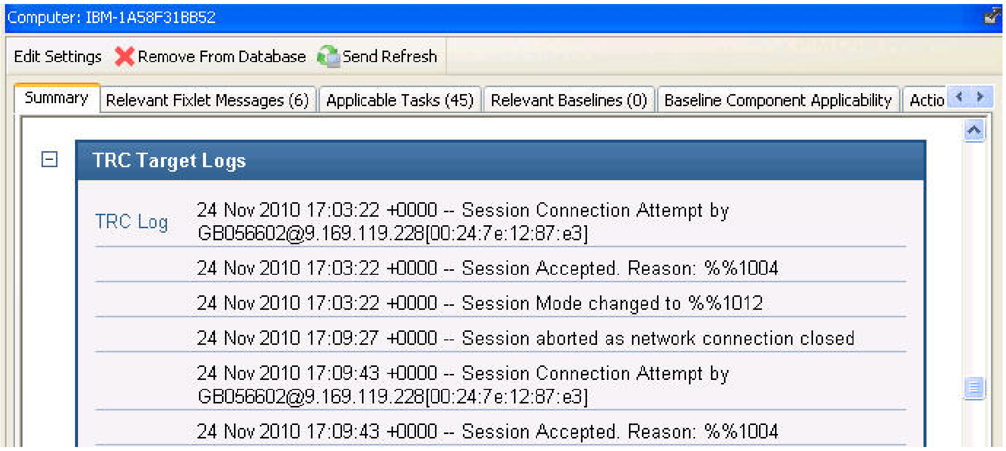
This analysis shows the logs of Tivoli Remote Control Target events. The information is retrieved from each computer's application event log.

Note that this information is pulled back once every 6 hours.

Click here to deactivate this analysis.

Reference #20

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



TRC Target Logs

TRC Log	24 Nov 2010 17:03:22 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
	24 Nov 2010 17:03:22 +0000 -- Session Accepted. Reason: %%1004
	24 Nov 2010 17:03:22 +0000 -- Session Mode changed to %%1012
	24 Nov 2010 17:09:27 +0000 -- Session aborted as network connection closed
	24 Nov 2010 17:09:43 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
	24 Nov 2010 17:09:43 +0000 -- Session Accepted. Reason: %%1004

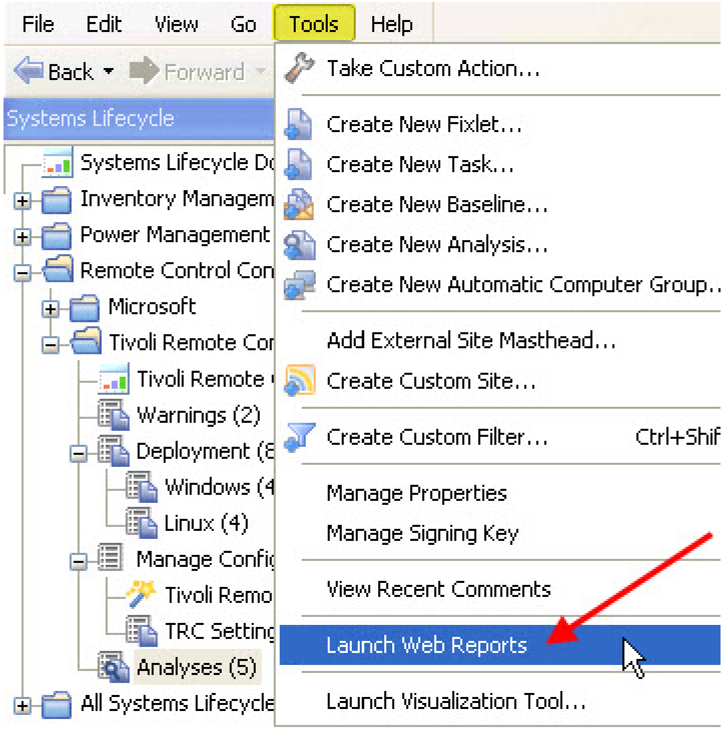
Note: The reason codes returned in this data can be viewed completely by using the web reports to display the output. See Chapter 7, "Viewing Web Reports," on page 39 for more details.

Chapter 7. Viewing Web Reports

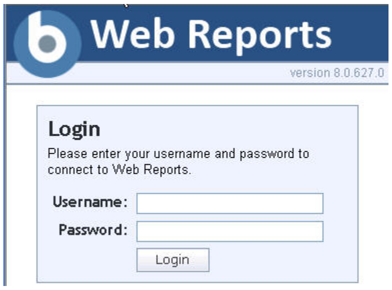
TEM Tivoli Remote Control offers a report available in the Web Reports component of the application. This Web Report was formulated to provide log data gathered from the controller and target logs relevant to specific targets. This data can be used for auditing purposes and for monitoring remote control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

To access the Tivoli 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.

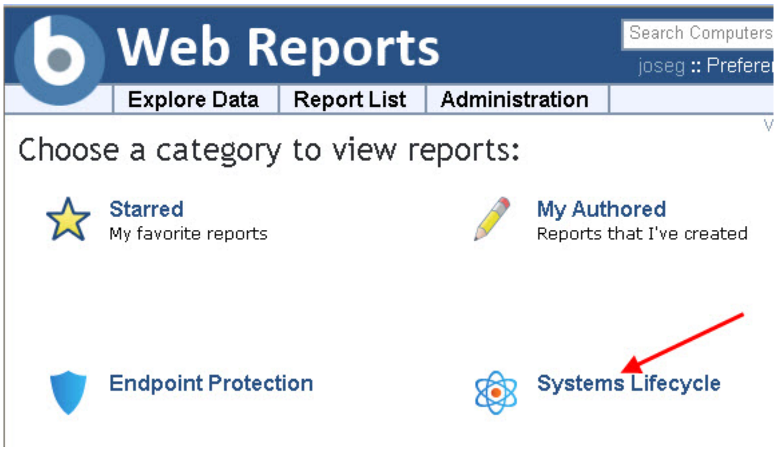


Please enter your username and password to connect to Web Reports.

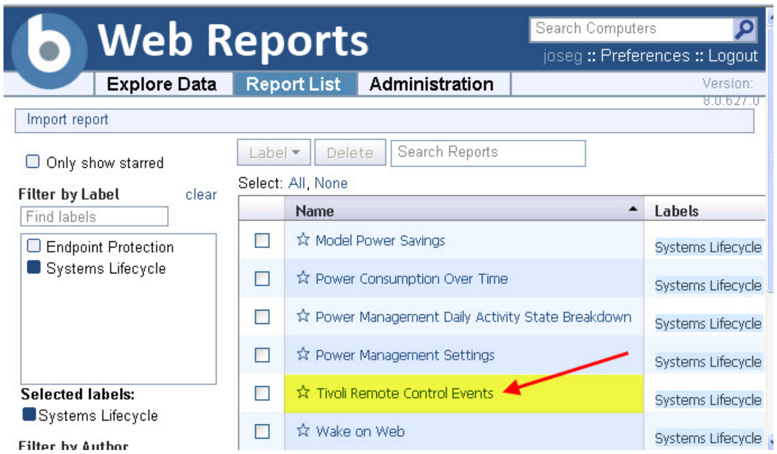
Username:

Password:

3. After login, you will see the main Web Reports page open in a new browser. Select **Systems Lifecycle** to see a list of reports including the Tivoli Remote Control report.



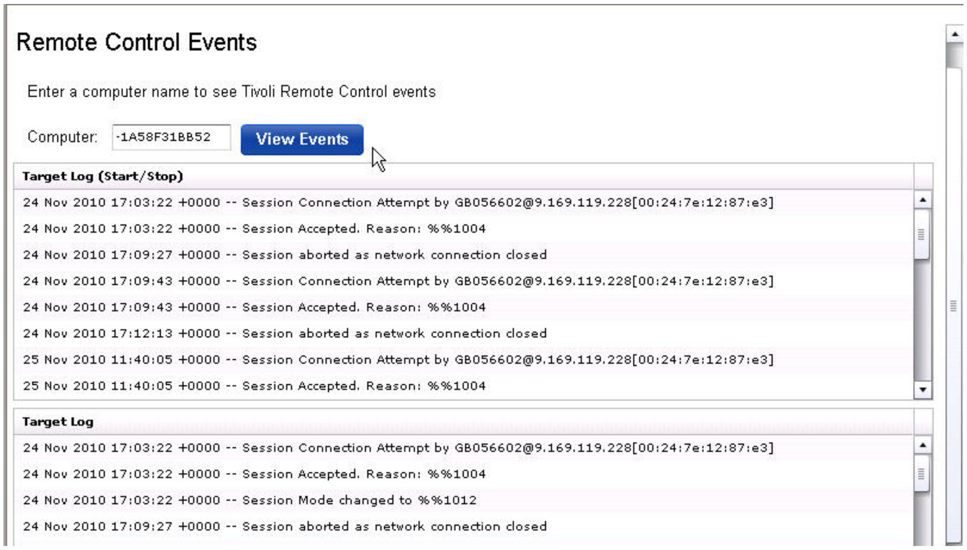
4. You will see the Tivoli Remote Control Events entry in the reports list displayed under the Report List menu:



	Name	Labels
□	☆ Model Power Savings	Systems Lifecycle
□	☆ Power Consumption Over Time	Systems Lifecycle
□	☆ Power Management Daily Activity State Breakdown	Systems Lifecycle
□	☆ Power Management Settings	Systems Lifecycle
□	☆ Tivoli Remote Control Events	Systems Lifecycle
□	☆ Wake on Web	Systems Lifecycle

Click on **Tivoli Remote Control Events**.

5. Enter the computername 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 will be displayed in the relevant sections, showing the remote control events.



Enter a computer name to see Tivoli Remote Control events

Computer: -1A58F31BB52

Target Log (Start/Stop)

```
24 Nov 2010 17:03:22 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
24 Nov 2010 17:03:22 +0000 -- Session Accepted. Reason: %%1004
24 Nov 2010 17:09:27 +0000 -- Session aborted as network connection closed
24 Nov 2010 17:09:43 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
24 Nov 2010 17:09:43 +0000 -- Session Accepted. Reason: %%1004
24 Nov 2010 17:12:13 +0000 -- Session aborted as network connection closed
25 Nov 2010 11:40:05 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
25 Nov 2010 11:40:05 +0000 -- Session Accepted. Reason: %%1004
```

Target Log

```
24 Nov 2010 17:03:22 +0000 -- Session Connection Attempt by GB056602@9.169.119.228[00:24:7e:12:87:e3]
24 Nov 2010 17:03:22 +0000 -- Session Accepted. Reason: %%1004
24 Nov 2010 17:03:22 +0000 -- Session Mode changed to %%1012
24 Nov 2010 17:09:27 +0000 -- Session aborted as network connection closed
```

Chapter 8. Support

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 TEM console?

   To start a remote control session using this method you need to have the controller component also installed on the system that the TEM console is installed on.
2. Where can I find more information on using TRC ?

   Information on installing, using and administering Tivoli Remote Control can be found in the **Tivoli Remote Control information center.**

Technical Support

TEM technical support site offers a number of specialized support options to help you learn, understand, and optimize your use of this product:

- **TEM Support Site**
- **Documentation**
- **Knowledge Base**
- **Forums and Communities**

Appendix. 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 users 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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A

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

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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
USA

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 information 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.

Customers are responsible for ensuring their own compliance with various laws such as the Graham-Leach-Bliley Act, the Sarbanes-Oxley Act, and the Health Insurance Portability and Accountability Act. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal, accounting or auditing advice, or represent or warrant that its products or services will ensure that customer is in compliance with any law.

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 measurement 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.

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.

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

Trademarks

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

AIX
DB2
DB2 Universal Database
IBM
IBM logo
Lotus
SmartSuite
Tivoli
Tivoli logo

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

Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

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

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

Other company, product, and service names may be trademarks or service marks of others.

Index

Printed in USA