IBM Endpoint Manager for Remote Control Installation Guide

Version 9.1.0

IBM Endpoint Manager for Remote Control Installation Guide

Version 9.1.0

Note

Before using this information and the product it supports, read the information in "Notices" on page 131.

This edition applies to version 9, release 1, modification level 0 of IBM Endpoint Manager and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

##

##

##

##

##

##

##

##

Chapter 1. IBM Endpoint Manager for Remote Control Installation Guide

Using IBM® Endpoint Manager for Remote Control you can remotely support and control thousands of PCs and servers, on an enterprise scale, from a central location or directly, in peer to peer mode.

Using the IBM Endpoint Manager for Remote Control administration Web interface, you can view and control a remote desktop, including its keyboard and mouse, anywhere on your network. You can also chat, transfer files, remotely guide the users, administer the policies to be applied to different users and target groups, and much more. These features can help provide more efficient and effective analysis of user problems from the administrators desktop, without the added cost of dispatching a technician or relying on user descriptions over the phone. Use IBM Endpoint Manager for Remote Control to deliver better support, more flexibility, and richer security, using robust features that include enhanced central logging and video capture of the sessions and full data stream encryption.

Audience

This guide is for administrators and IT managers who want to install and administer IBM Endpoint Manager for Remote Control. It details the system requirements for each of the components and provides installation instructions that allow you to deploy the program in your environment. It also includes information about configuring and maintaining IBM Endpoint Manager for Remote Control.

Versions

The guide includes the functions introduced in IBM Endpoint Manager for Remote Control, Version 9.1.0 © Copyright IBM Corp. 2014.

Terms used in this guide

The following terms are all IBM Endpoint Manager for Remote Control terms, but are used throughout the guide without being labeled every time with IBM Endpoint Manager for Remote Control:

- • Controller always means IBM Endpoint Manager for Remote Control Controller application
- • Target always means IBM Endpoint Manager for Remote Control Target
- • Server always means IBM Endpoint Manager for Remote Control Server
- • Broker always means IBM Endpoint Manager for Remote Control Broker
- • Managed mode refers to installations where a server has been deployed and the targets are configured to register and report status to the server.

Chapter 2. 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. 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.

Using this guide

The process of getting IBM Endpoint Manager for Remote Control up and running varies, depending on your network environment and the management granularity you want to achieve. This guide will focus on three types of deployments:

Peer to peer
is the simplest scenario and therefore ideal for small deployments where all targets are in network sight of the controllers and there is no requirement to centrally manage the controller policies.

Intranet managed
are most appropriate when there is a complex network infrastructure that requires the deployment of gateways to traverse firewalls or there is a requirement for strict policy control and centralized auditing.

Managed
with support for internet sessions where at least one broker must be installed in an internet facing machine so that it is visible to targets outside the controllers network sight.

For the sake of readability and generality, this guide assumes the following restrictions:

- Each IBM Endpoint Manager for Remote Control server must have access to one of the supported database servers, located locally on the server machine or remotely on a separate server. The supported database systems are DB2, Oracle and MS SQL. It is also possible to install the server using the embedded Derby database provided by the installer but this configuration is not supported for production deployments.
- In managed environments, each controller can make an HTTP or HTTPS connection to the IBM Endpoint Manager for Remote Control server.
- In managed environments, each IBM Endpoint Manager for Remote Control target computer in the network must be able to make an HTTP or HTTPS connection to a server, a gateway or a broker on the specified ports.

If your network configuration does not match any of the scenarios in that chapter, contact a support technician for more options.

The initial deployment of a minimal managed IBM Endpoint Manager for Remote Control system (server and a few targets) should take about an hour to complete.

Several steps in the IBM Endpoint Manager for Remote Control installation depend on the completion of prior steps. For this reason, it is recommended that you follow this guide in the order presented.

IBM Endpoint Manager for Remote Control operating requirements

IBM Endpoint Manager for Remote Control runs efficiently using minimal server, network, and client resources. The requirements for the client programs are not stringent. The hardware required by the server and the target depends on the number of computers that are administered and the frequency defined for their status updates.

A Basic installation

The most basic installation requires the IBM Endpoint Manager for Remote Control target and controller components. Use the two components to start a peer to peer remote control session, for which the policies are defined only at target level.

The port to be used for target to controller communication is configurable at installation time. The default is port 888.

Such an installation provides basic audit information. This information is accessible from the IBM Endpoint Manager console. It is also stored in the application event log, in a Windows operating system, or system log, in a Linux operating system. However, if centralized auditing and management of users and computers is required, install the server component.

The server component provides a single interface where controller users can easily search for targets. They can also organize the targets that are most frequently accessed and view their session history. For an administrator, a managed environment provides the following extra capability.

- Centralized management of users and targets: Users can be organized into groups with similar profiles. They can be organized manually, by using the IBM Endpoint Manager for Remote Control server interface, or by importing users and groups from LDAP. Similarly, targets can be organized into groups manually or by setting target membership rules to automatically assign a target to a specific group. For more details of target membership rules, see the IBM Endpoint Manager for Remote Control Administrator's Guide.
- Centralized policy management: When a session is started from the server interface, the permissions that are set for the session are derived from the target and controller properties. Provides more flexibility to define different levels of access, against a single target, for different users in your organization.
- Centralized auditing and recording repository: Administrators can use the IBM Endpoint Manager for Remote Control server interface to browse and examine audit information. They can also view recordings that are associated with a specific remote control session. Administrators can search the existing session history. For example, by user ID or computer name.
- Access request management: Administrators can grant temporary access, or increase the level of access, to a target or group of targets. Temporary access can be granted to IBM Endpoint Manager for Remote Control registered and unregistered users.
- Reporting capabilities

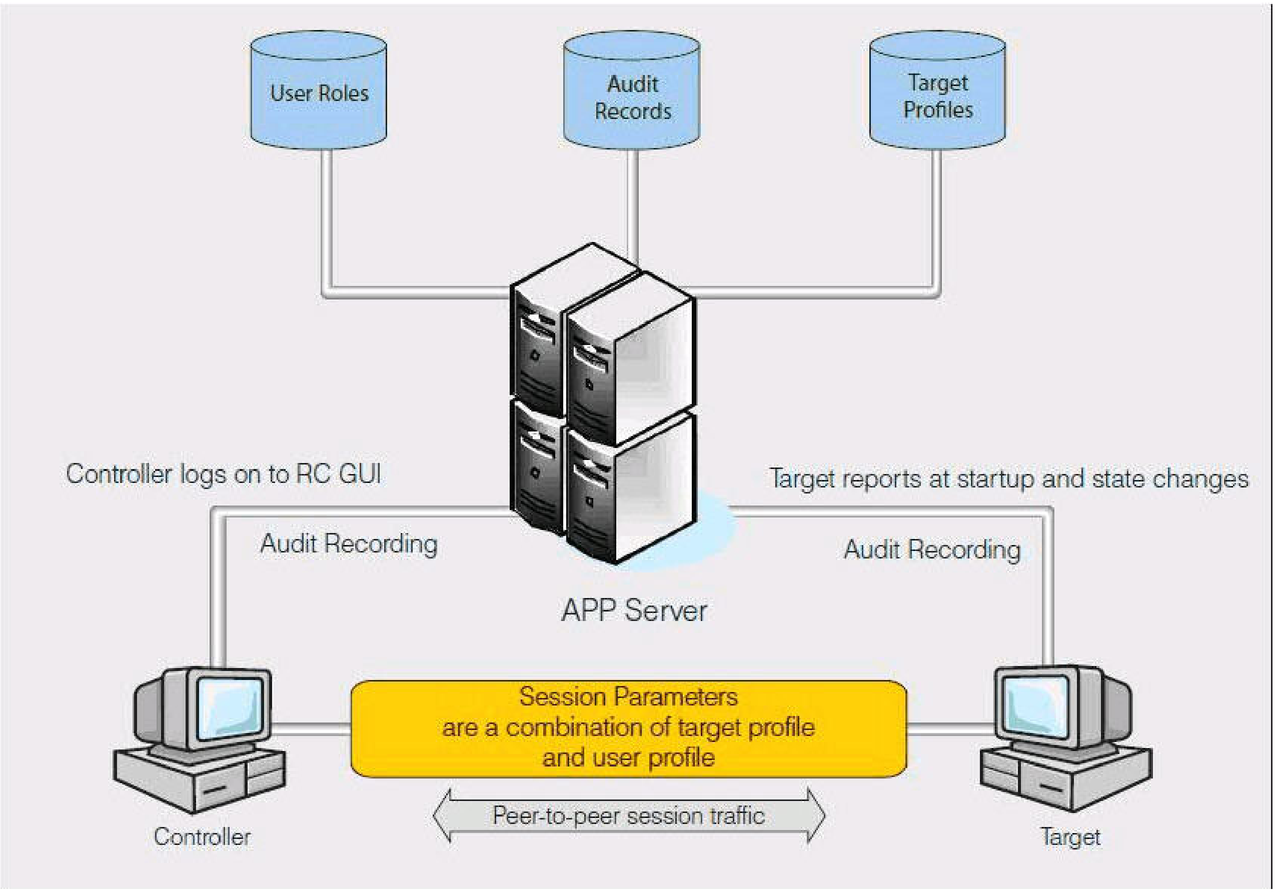

User Roles
Audit Records
Target Profiles
Controller logs on to RC GUI
Target reports at startup and state changes
Audit Recording
Audit Recording
APP Server
Session Parameters are a combination of target profile and user profile
Peer-to-peer session traffic
Controller
Target

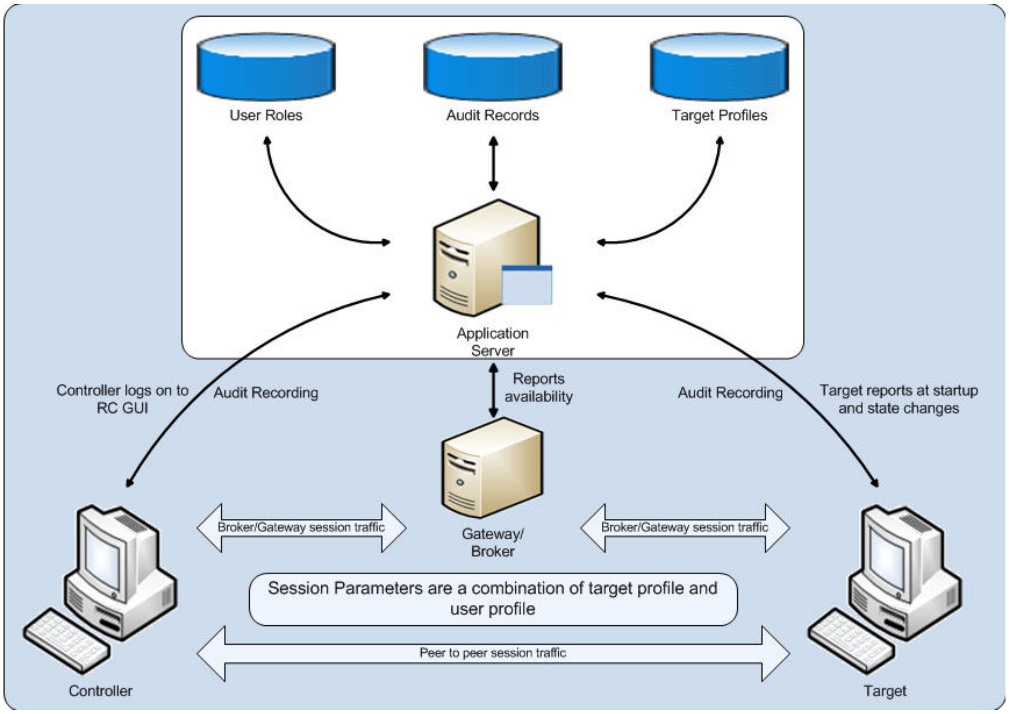
Figure 1. Basic installation environment

Note: It is not necessary to install the controller component in a managed environment, Remote control sessions are launched in-context from the IBM Endpoint Manager for Remote Control server interface. You can also configure the target components, in a managed environment, to accept peer to peer remote control requests from a stand-alone controller component. For more information about installing the target, see "Installing the target" on page 40.

Installation with support for firewall and NAT traversal

In some environments, it is not possible to open a port in a firewall to enable controller to target, or target to server communication for all endpoints. It is more appropriate to enable traffic from, or traffic to a single computer that acts as a gateway to traverse the firewall.

The gateway component can be strategically installed in your network to enable traffic between targets and controllers, or targets and servers that are located in different networks. This component can also be used as a proxy server to forward the target's status update to the remote control server.


User Roles
Audit Records
Target Profiles
Application Server
Controller logs on to RC GUI
Audit Recording
Reports availability
Audit Recording
Target reports at startup and state changes
Broker/Gateway session traffic
Gateway/ Broker
Broker/Gateway session traffic
Session Parameters are a combination of target profile and user profile
Peer to peer session traffic
Controller
Target

Installation with support for remote control sessions over the internet

There can be occasions when the target that requires support is out of network sight in some internet location. For example, in a hotel or an airport lounge.

Use the broker component to enable remote control sessions to these computers by bridging the target and controller communication. The broker must be placed in the DMZ and a gateway is required to provide secure communication to the server in the intranet.

In this scenario, the controller user can start a broker connection and obtain a connection code from the server. The user who requires assistance enters the connection code by using the appropriate menu option in the target UI. When the session details are validated by the server, the session is connected.

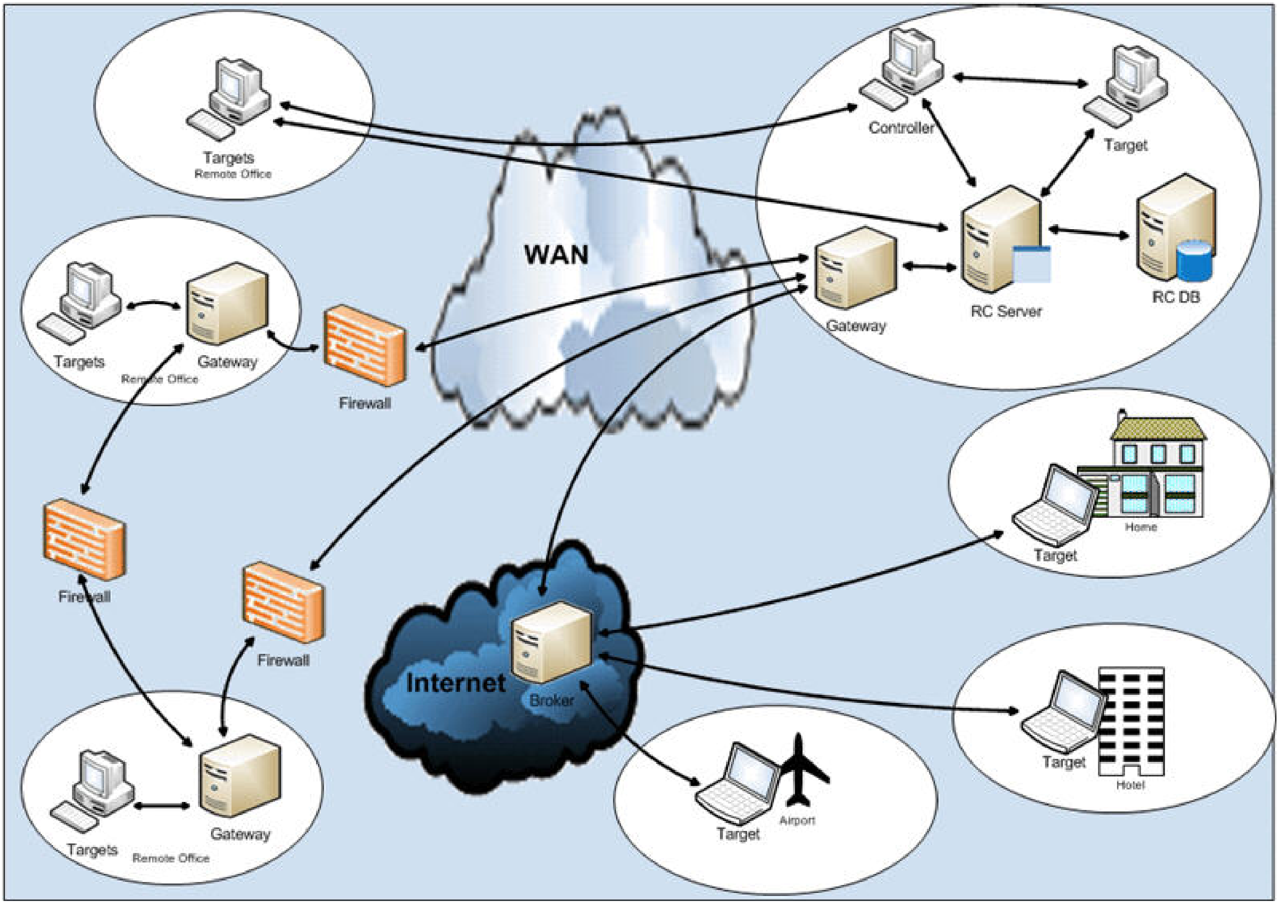


Figure 2. Sample deployment environment

Server requirements

The hardware that is required by the server component depends on the number of computers that are administered and the frequency that is defined for their status updates.

The distributed architecture of IBM Endpoint Manager for Remote Control allows a single server to support hundreds of thousands of computers.

Note: IBM Endpoint Management for Remote Control includes entitlement for DB2 v10.5 and WebSphere v8.5.

The computer on which you install the IBM Endpoint Manager for Remote Control server must have the **minimum** following items or capability:

1. 1 Quad core or two dual core processors. 2.40 GHz with supported OS.
2. A minimum of 4 GB of memory.
3. A minimum of 2 GB of storage or hard disk space to install, and an average of 2 MB per client in the database.
4. A minimum screen resolution of 800 by 600 pixels is required when you perform an automated server installation.
5. Adequate space for storing session video recordings. Recordings are stored on the hard disk and their size can vary depending on the duration and screen

activity of the session. On average a 5-minutes session, 8-bits mode, can use about 2 MB of space. In true color 24-bit mode, recordings can take more space.

6. A network card that supports TCP/IP.
7. A supported browser.
8. When you use an Oracle database you must use the **10.2 g JDBC 4** drivers for Oracle. Alternatively, if you are using the Oracle 11g drivers, **`oracle.increment.keys.off=1`** must be set in the `trc.properties` file. Restart the server service.

Platform Support

The following platforms are supported when you use the installation tasks

Note: Derby 10.10 provides support only up to Windows Server version 2008.

- Windows Server 2003.
- Windows Server 2003 R2.
- Windows Server 2008.
- Windows Server 2008 R2.
- Windows Server 2012.
- Windows Server 2012 R2.
- Red Hat Enterprise Linux 5.0.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 7.0.
- SuSE Enterprise Linux Server 10.
- SuSE Enterprise Linux Server 11.
- CentOS 5.0.
- CentOS 6.0.

Supported Architectures

- Intel IA-32 (also known as x86, x86-32)
- Intel 64 or AMD64 (also known as x64, x86-64, EM64T)

Note: IA-64 (also known as Itanium) processors are not supported.

Server environment guidelines

As well as determining the system requirements for installing the IBM Endpoint Manager for Remote Control components you must also determine which type of server installation is best for your environment. Use the following information as a guide when you make this decision.

Table 1. IBM Endpoint Manager for Remote Control server installation types

Server installation type	Components installed	Install using the IBM Endpoint Manager console	Install using the installation files
1	embedded Liberty profile, embedded Derby database	Yes	Yes
2	embedded Liberty profile, using an already installed DB2, MS SQL or Oracle database	Yes	Yes

Table 1. IBM Endpoint Manager for Remote Control server installation types (continued)

Server installation type	Components installed	Install using the IBM Endpoint Manager console	Install using the installation files
3	stand-alone IBM Endpoint Manager for Remote Control server accessing Websphere Application Server, using an already installed DB2, MS SQL or Oracle database	No	Yes

Note: Server installation types 1 and 2 are only available when using Windows or Linux operating systems.

Note: Server installation type 1 should only be used in Proof of Concept or test deployments.

The following sections provide guidance and recommendations based on environment size.

Small environment guidelines

For environments containing up to 5K targets you can use server installation types 1, proof of concept only, or 2 in "Server environment guidelines" on page 10.

Also consider the following extra requirements.

- Processors: 1 Quad core or 2 dual core processors, 2.40 GHz, with supported OS.
- Memory: 4 GB RAM.
- Storage. For more details, see "Server requirements" on page 9.
- Heartbeat configuration

Table 2. heartbeat configuration properties: suggested values for a small environment

property in trc.properties	value
heartbeat.timeout	60 **Note:** If there are performance issues, set to 1440, which is 24 hours. For example: when there is heavy usage of reports, especially with derby. Default is 60, which is 1 hour.
heartbeat.retry	10
heartbeat.delay	20
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

Note: Installation type 1 is suitable for demos or pilot projects. Installation type 2 can give better performance, which might be preferred for production systems in these environments.

Medium environment guidelines

For environments containing from 5K to 75K targets you can use server installation types 2 or 3 in "Server environment guidelines" on page 10. In terms of performance, installation type 2 is suitable. However with installation type 3 you can also use the admin functions of the installed WAS.

Also consider the following extra requirements.

- Processors: 1 Quad core or 2 dual core processors, 2.40 GHz.
- Memory: 8 GB RAM.
- Storage: RAID 5 - 6 HDD. DB2, Oracle or MS SQL 64 bit or 32 bit.
- Heartbeat configuration -

Table 3. heartbeat configuration properties: suggested values for a medium environment

property in trc.properties	**value**
heartbeat.timeout	1440 **Note:** If there are specific group of machines where more regular updates are needed, a smaller heartbeat timeout setting can be applied as a group attribute for those specific groups of targets. For details of setting this attribute at group level, see the chapter that explains how to create a target group in the IBM Endpoint Manager for Remote Control Administrator's Guide.
heartbeat.retry	10 **Note:** In an environment containing target numbers nearer to 75K, set this value to 20 to help with performance.
heartbeat.delay	20 **Note:** In an environment containing target numbers nearer to 75K, set this value to 40 to help with performance.
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

Note: In this type of environment ensure that the target deployment is performed in stages. A staged deployment can avoid overload in the server when the targets try to register with the server. Give the **RegistrationDelay** target property a value that will distribute the target machine registration evenly through the staged deployment. Distribute the target registration to avoid too many machines trying to register at the one time.

Large environment guidelines

For environments containing from 75K to 225K targets you can use server installation type 3 in “Server environment guidelines” on page 10.

Also consider the following extra requirements.

To host Websphere Application Server

- Processors: 2 Quad core processors. 2.40 GHz with supported OS.
- Memory: 16 GB RAM.
- Storage: RAID 5 - 6 HDD.
- Heartbeat configuration -

Table 4. heartbeat configuration properties: suggested values for a large environment

property in trc.properties	**value**
heartbeat.timeout	1440 **Note:** If there are specific group of machines where more regular updates are needed, a smaller heartbeat timeout setting can be applied as a group attribute for those specific groups of targets. For details of setting this attribute at group level, see the chapter that explains how to create a target group in the IBM Endpoint Manager for Remote Control Administrator's Guide.
heartbeat.retry	60 **Note:** In an environment containing target numbers nearer to 75K, set this to a higher value to help with performance.
heartbeat.delay	60 **Note:** In an environment containing target numbers nearer to 75K, set this to a higher value to help with performance.
heartbeat.on.wake	0
heartbeat.on.user.change	1
heartbeat.on.change	0
heartbeat.on.stop	0

- Optional: 2 network cards, one for target communications and one for database communications which could aid in performance tuning.

To host the database, DB2, Oracle or MS SQL supported.

- Processors: 4 Quad core processors, 2.40 GHz.
- Memory: As recommended by DB supplier.
- Storage: RAID 5 to 6 HDD 146 GB

Note: The database administrator should tune the database for performance as is appropriate.

The following guidelines should also be taken into consideration when using large reports as some performance degradation can be experienced.

- Ensure that the **All targets** report is not the default home page report.
- Ensure staged deployment of the targets to avoid overload in the server when they try to register.

  Note: Give the **RegistrationDelay** target property a value that will distribute the target machine registration evenly through the staged deployment. Distribute the target registration to avoid too many machines trying to register at the one time.

Note: If you have configured LDAP and LDAP synchronization is enabled, set a reasonable frequency for the synchronization. If your LDAP configuration is set up to import a large number of users and groups, set the frequency to 24 hours. For more details about configuring LDAP, see "Configuring LDAP" on page 73.

Controller requirements

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

- Java Run Time environment: Sun 1.6, Oracle 1.6, 1.7 or IBM® 1.5, 1.6, 1.7

Note: Sun Java and Oracle Java are not supported in FIPS or NIST SP800-131a mode. You must use the IBM Java in this mode.

- Web Browser: either Microsoft Internet Explorer 9, 10, 11 or Mozilla Firefox ESR 24, 31.

Target requirements

The computer on which you install the IBM Endpoint Manager for Remote Control target must have the minimum following items or specification:

1. At least a 1 GHz Intel® or AMD processor.
2. A minimum of 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit).
3. A minimum of 50 MB hard disk space.
4. Adequate space for storing session video recordings. Recordings are stored on the hard disk and their size can vary depending on the duration and screen activity of the session. On average a 5-minutes session, 8-bits mode, can use about 2 MB of space. In true color 24-bit mode, recordings can take more space.

Platform Support

The following operating systems are supported

- Windows 7
- Windows 8 and 8.1.
- Windows Server 2003.
- Windows Server 2003 R2.
- Windows Server 2008.
- Windows Server 2008 R2.
- Windows Server 2012.
- Windows Server 2012 R2.
- Windows XP Pro (32 bits), (64 bits).
- Red Hat Enterprise Linux 5.0.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 7.0.
- SuSE Enterprise Linux Server 10.
- SuSE Enterprise Linux Server 11.
- SuSE Linux Enterprise Desktop 10.
- SuSE Linux Enterprise Desktop 11.
- CentOS 5.0.
- CentOS 6.0.

Supported Architectures

- Intel IA-32 (also known as x86, x86-32)
- Intel 64 or AMD64 (also known as x64, x86-64, EM64T)

Note: IA-64 (also known as Itanium) processors are not supported.

Gateway requirements

The computer on which you install the IBM Endpoint Manager for Remote Control gateway must have the minimum following items or specification:

1. At least a 1 GHz Intel® or AMD processor.

2. A minimum of 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
3. A minimum of 50 MB hard disk space.

Platform Support

The following operating systems are supported

- Windows 7
- Windows 8 and 8.1.
- Windows Server 2003.
- Windows Server 2003 R2.
- Windows Server 2008.
- Windows Server 2008 R2.
- Windows Server 2012.
- Windows Server 2012 R2.
- Red Hat Enterprise Linux 5.0.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 7.0.
- SuSE Enterprise Linux Server 10.
- SuSE Enterprise Linux Server 11.
- SuSE Linux Enterprise Desktop 10.
- SuSE Linux Enterprise Desktop 11.
- CentOS 5.0.
- CentOS 6.0.

Supported Architectures

- Intel IA-32 (also known as x86, x86-32)
- Intel 64 or AMD64 (also known as x64, x86-64, EM64T)

Note: IA-64 (also known as Itanium) processors are not supported.

Broker requirements

The computer on which you install the IBM Endpoint Manager for Remote Control broker must have the minimum following items or specification:

1. At least a 1 GHz Intel® or AMD processor.
2. A minimum of 1 gigabyte (GB) RAM (32-bit) or 2 GB RAM (64-bit)
3. A minimum of 50 MB hard disk space.
4. Adequate space for storing session video recordings. Recordings are stored temporarily on the hard disk and their size can vary depending on the duration and screen activity of the session. On average a 5-minutes session, 8-bits mode, can use about 2 MB of space. In true color 24-bit mode, recordings can take more space.

Platform Support

The following platforms are supported

The following operating systems are supported

- Windows Server 2003.
- Windows Server 2003 R2.

- Windows Server 2008.
- Windows Server 2008 R2.
- Windows Server 2012.
- Windows Server 2012 R2.
- Red Hat Enterprise Linux 5.0.
- Red Hat Enterprise Linux 6.0.
- Red Hat Enterprise Linux 7.0.
- SuSE Enterprise Linux Server 10.
- SuSE Enterprise Linux Server 11.
- CentOS 5.0.
- CentOS 6.0.

Supported Architectures

- Intel IA-32 (also known as x86, x86-32)
- Intel 64 or AMD64 (also known as x64, x86-64, EM64T)

Note: IA-64 (also known as Itanium) processors are not supported.

Chapter 3. Getting started

Now that you understand the terms and components available in IBM Endpoint Manager for Remote Control, you are ready to identify which components you need to install:

Table 5. Determining which components to install

Requirements	Target	Controller	Server	Gateway	Broker
I want others to remotely connect to this machine.	Yes	Yes			
I want to remotely connect to other machines by using the IBM Endpoint Manager for Remote Control console or by starting the standalone controller.	Yes	Yes			
To centrally manage users and targets, and their policies.	Yes	Optional *	Yes		
To maintain a central audit and recording repository.	Yes	Optional *	Yes		
Traverse firewalls in my infrastructure	Yes	Optional *	Yes	Yes	
Connect to targets outside my network.	Yes	Optional *	Yes	Yes **	Yes

* In a managed environment, the controller user starts remote control sessions from the IBM Endpoint Manager for Remote Control server interface. Starting sessions this way does not require the controller component to be installed separately. The IBM Endpoint Manager for Remote Control server interface starts a Java Web Start controller console, in context.

** A gateway is not strictly required in a broker deployment but it does increase security.

Chapter 4. Installing the IBM Endpoint Manager for Remote Control components

The IBM Endpoint Manager for Remote Control components can be installed in two ways. If you have access to the IBM Endpoint Manager for Remote Control console use the deployment fixlets to install the components. For more details see the IBM Endpoint Manager for Remote Control Console User's Guide. Alternatively use the component installation files.

There are various ways that you can obtain the installation files, choose the appropriate method for obtaining the required files. There is no specific order in which the different components must be installed.

Obtain the installation files

The installation files for installing the IBM Endpoint Manager for Remote Control components can be obtained in various ways.

Passport Advantage®

To install the IBM Endpoint Manager for Remote Control components, use the following images from Passport Advantage.

Table 6. Parts required for installing IBM Endpoint Manager for Remote Control

Part number	File name
Windows operating system CITM7ML - IBM Endpoint Manager for Remote Control V9.1 Image 1.	`IEM_Rem_Cntrl_V91_Image_1.zip`
Linux operating system CITM8ML - IBM Endpoint Manager for Remote Control V9.1 Image 2.	`IEM_Rem_Cntrl_V91_Image_2.tar`
Windows, Linux, AIX®, Solaris operating systems CITM9ML - IBM Endpoint Manager for Remote Control V9.1 Image 3.	`IEM_Rem_Cntrl_V91_Image_3.tar`

Depending on the operating system, and the component that you are installing, determines which image file you require.

`IEM_Rem_Cntrl_V91_Image_1.zip`
: Extract the installation files for the Windows operating system components from this image file. The Windows operating system executable files are in the `\windows` directory.

`IEM_Rem_Cntrl_V91_Image_2.tar`
: Extract the installation file for the Linux server component from this image file. The `trc_server_setup.bin` file is in the `\linux` directory. Use the `IEM_Rem_Cntrl_V91_Image_3.tar` file to access the installation files for the other Linux components.

`IEM_Rem_Cntrl_V91_Image_3.tar`
Extract the additional setup utility files, `trc_additional_setup.exe`, and `trc_additional_setup.bin` from this image file. Use the files to extract the installation files for Windows, Linux, and other supported operating system components. Go to the `\Disk1\InstData\`*`platform`*`\VM` directory where *platform* is relevant to your operating system. For more information about running the additional setup utility, see "Using the additional setup utility" on page 69.

Accessing the installation files on the installation DVD

The installation DVD contains the installation files that are required for installing the components.

Windows installation files
Go to the `\trc\windows` directory to access the required component installation file.

Linux server component
Go to the `\trc\linux` directory to access the `trc_server.bin` file, for installing the server. For all other component installation files, go to the `\Disk1\InstData\`*`platform`*`\VM` directory where *platform* is relevant to your operating system. Use the additional setup utility files `trc_additional_setup.exe` or `trc_additional_setup.bin` to extract the required installation files. For more information about running the additional setup utility, see "Using the additional setup utility" on page 69.

Downloading the files from the server UI

If you have the IBM Endpoint Manager for Remote Control server installed, you can download the installation files for the target, controller, and cli components. The controller installation file is for the standard controller. For the FIPS-compliant installation file, use the additional setup utility.

- Click **Tools** > **Downloads**.
- Select **Agent Downloads**.
- Select the relevant component file.

Installing the server

IBM Endpoint Manager for Remote Control server supports the following installation types:

Table 7. Server installation types

Automated installation - For more details, see "Installing by using the server installer" on page 25	Manual Installation - For more details, see "Installing on WebSphere Application Server version 8.5: deploying the war file" on page 32
Available on Windows® operating system and Linux® operating system.	Available on AIX® operating system and Solaris operating system and for any operating system that Websphere Application Server 8.5 supports.
Installs Derby as embedded or uses existing supported Database. Local or remote.	Database needs to be created or an existing supported database can be used.
All embedded components are installed locally on the one computer.	The database can be installed on a separate computer.

Note: The embedded Derby database is not supported in production.

Setting up the database

Before setting up the database, install the database software and create the instance where the database for IBM Endpoint Manager for Remote Control will be held.

Setting up DB2

To perform the database setup for DB2 complete the following steps. If you are using a Windows operating system, begin from step 2. If you are using Linux operating system or AIX operating systems, begin from step 1:

1. To verify that DB2 and the instance are ready for remote connectivity using TCP/IP complete the following steps:
   a. Run **`db2 get database manager configuration`** and verify that the value of **`svcename`** is a valid port.

      ```
      for example 50000

      or a reference mapped to a valid port
      for example,db2c_db2inst1.
      ```

   b. Ensure that the configured port is not used by other processes in the system, or blocked by a firewall that sits between the Application Server host and the DB2 server.
   c. Use the **`db2stop`** command to stop the DB2 instance.

      Set **`DB2COMM`** to tcpip with the command

      `db2set DB2COMM=tcpip`

      Run **`db2start`** to start the DB2 instance again.

   The DB2 server is now ready for accessing over the network.
2. Create the database that IBM Endpoint Manager for Remote Control will use by running the following command as the instance owner:

   Note: Not necessary when the database is local.

   `db2 create db` ***`databasename`*** **`using codeset UTF-8 territory`** ***`requiredtrerritory`***

   where *databasename* is the name required for the database. This database name must be the name that was referenced in any configuration settings. For example, TRCDB.

   requiredtrerritory is the required territory. For example, GB for Great Britain.
3. Verify the privileges that a specific user, for the database, needs to have. Do not use the **db2inst1** user as the user configured to access the IBM Endpoint Manager for Remote Control database. Create a new specific user for DB2 that has the database owner privileges.

With the blank database created and ready to use, the next step is to set up the WebSphere server, see “Setting up the application server” on page 32. It is possible to verify that the database is set up properly by using a DB2 client to connect to the database from another host. For more details see the DB2 Infocenter.

Setting up Oracle

To set up Oracle to use with IBM Endpoint Manager for Remote Control, create the database and then set up the database permissions.

Creating the database:

Run the Oracle database configuration assistant to create the database.

To create the Oracle database that will be used for IBM Endpoint Manager for Remote Control, complete the following steps:

1. Run the Oracle database configuration assistant.

   Windows systems

   For example, Select **Start** > **All Programs** > **Oracle** > **Configuration and Migration Tools** > **Database Configuration Assistant**.

   UNIX-based systems

   Enter the command `dbca` from the `$ORACLE_HOME/bin` directory.
2. Click **Next** on the welcome screen.
3. **Step 1**: Select **Create a Database**. Click **Next**.
4. **Step 2**: Select **General Purpose** for the template. Click **Next**.
5. **Step 3**:
   a. Specify a name for the database. For example, `TRCDB`.
   b. Specify an SID to be used to reference the database. For example, `TRCDB`.

   Click **Next**.
6. **Step 4**: Select the database management option that you require. For example, **Use Database Control for Database Management**. Click **Next**.
7. **Step 5**: Specify a password for the database and confirm the password. For example, `dboracle`. Click **Next**.
8. **Step 6**: Specify where the database will be stored. For example, `File System`. Click **Next**.
9. **Step 7**: Specify locations for the database files. For example, `Use Database File Locations from Template`. Click **Next**.
10. **Step 8**: Select the recovery options for the database. Click **Next**.
11. **Step 9**: On the Database Content window, click **Next**.
12. **Step 10**: On the Initialization Parameters screen select the **Character Sets** tab.
    a. Select the required Database Character Set
    b. Click **Next**.
13. When you are using Oracle 11g, the following two steps are also required.
    a. Security Settings, accept the enhanced 11g default security settings.
    b. Automatic Maintenance Tasks, enable automatic maintenance tasks.
14. **Step 11**: On the Database Storage window click **Next**.
15. **Step 12**: Select the required Creation Options. Click **Finish**.
16. On the Confirmation screen, click **OK** to start the database creation.

    Note: This may take some time as it goes through the different stages.
17. Click **Exit** when the database creation is complete.

The Oracle database that will be used for IBM Endpoint Manager for Remote Control is created.

Setting up database permissions:

When you have created the Oracle database that will be used for IBM Endpoint Manager for Remote Control you will need to configure its permissions.

To configure the database permissions complete the following steps:

1. Run Oracle SQL*Plus.

Windows systems

For example: Click **Start** > **Programs** > **Oracle-OraHomeName** > **Application Development** > **SQL Plus**.

Alternatively, enter the following command at a command prompt.

`sqlplusw` Log on using the database user name and password and click **OK**. See your database system administrator if you do not have this.

For example:

Username - system

Password - dboracle

Linux systems

Open a UNIX or a Windows terminal and enter the SQL*Plus command:

`sqlplus` *username* / *password* *@connect_identifier*

username and *password* are the database credentials required to connect to the database.

connect_identifier is the connection required for your specific database.

For example, @TRCDB as SYSDBA

@//*servername*:*port*/*DatabaseSID* as SYSDBA

servername is the server name or IP address of the system where your Oracle installation is located.

port is the port of the system where your Oracle installation is located.

DatabaseSID is the SID defined for the database you created.

The SQL*Plus executable is installed in `$ORACLE_HOME/bin`, which is included in your operating system PATH environment variable. You may need to change directory to the `$ORACLE_HOME/bin` directory to start SQL*Plus.

2. After SQL*Plus has started and connected to the database you can create the required users and grant permissions. There are two methods for creating users and granting permissions. Choose the appropriate method for creating the users.

Create one user ID in Oracle which will also be used to log on to IBM Endpoint Manager for Remote Control.

Create a single user. The user must be called Asset. This user ID is used by IBM Endpoint Manager for Remote Control to create and log on to the database, and use the database.

Issue the following commands to create the user ASSET.

a. **`connect SYS/PASSWORD@DATABASE AS SYSDBA;`**

   where *PASSWORD* is the default Oracle user password.

   and *DATABASE* is the database name that was defined when creating the database. For example, TRCBD.

b. **`CREATE USER ASSET IDENTIFIED BY PASSWORD DEFAULT TABLESPACE users TEMPORARY TABLESPACE temp;`**

   Note: PASSWORD can be changed to whatever you require, for the user ASSET.

c. **GRANT UNLIMITED TABLESPACE TO ASSET;**

d. **GRANT CONNECT TO ASSET;**

e. **GRANT CREATE INDEXTYPE TO ASSET;**

f. **GRANT CREATE SEQUENCE TO ASSET;**

g. **GRANT CREATE TABLE TO ASSET;**

h. **GRANT CREATE TRIGGER TO ASSET;**

i. **GRANT CREATE INDEXTYPE TO ASSET;**

j. **GRANT CREATE PROCEDURE TO ASSET;**

k. **GRANT CREATE VIEW TO ASSET;**

l. **GRANT ANALYZE ANY TO ASSET;**

Create a separate user ID to log on to IBM Endpoint Manager for Remote Control

Create 2 users. User 1 must be called Asset. This user has no specific permissions and is used only as a schema name. User 2 is the main user and can be called anything you require. This user is used by IBM Endpoint Manager for Remote Control to create and logon to the database, and use the database. Use the assistant tool to create user TRCDBU.

Complete the following steps to create the required permissions for user TRCDBU.

a. **GRANT UNLIMITED TABLESPACE TO ASSET;**

b. **GRANT UNLIMITED TABLESPACE TO TRCDBU;**

c. **GRANT ALTER ANY INDEX TO TRCDBU ;**

d. **GRANT ALTER ANY INDEXTYPE TO TRCDBU ;**

e. **GRANT ALTER ANY PROCEDURE TO TRCDBU ;**

f. **GRANT ALTER ANY SEQUENCE TO TRCDBU ;**

g. **GRANT ALTER ANY TABLE TO TRCDBU ;**

h. **GRANT ALTER ANY TRIGGER TO TRCDBU ;**

i. **GRANT COMMENT ANY TABLE TO TRCDBU ;**

j. **GRANT CREATE ANY INDEX TO TRCDBU ;**

k. **GRANT CREATE ANY INDEXTYPE TO TRCDBU ;**

l. **GRANT CREATE ANY SEQUENCE TO TRCDBU ;**

m. **GRANT CREATE ANY TABLE TO TRCDBU ;**

n. **GRANT CREATE ANY TRIGGER TO TRCDBU ;**

o. **GRANT CREATE INDEXTYPE TO TRCDBU ;**

p. **GRANT CREATE PROCEDURE TO TRCDBU ;**

q. **GRANT CREATE SEQUENCE TO TRCDBU ;**

r. **GRANT CREATE TABLE TO TRCDBU ;**

s. **GRANT CREATE TRIGGER TO TRCDBU ;**

t. **GRANT CREATE VIEW TO TRCDBU ;**

u. **GRANT DELETE ANY TABLE TO TRCDBU ;**

v. **GRANT INSERT ANY TABLE TO TRCDBU;**

w. **GRANT DROP ANY INDEX TO TRCDBU ;**

x. **GRANT DROP ANY INDEXTYPE TO TRCDBU ;**

y. **GRANT DROP ANY PROCEDURE TO TRCDBU ;**

z. **GRANT DROP ANY SEQUENCE TO TRCDBU ;**

aa. `GRANT DROP ANY TABLE TO TRCDBU ;`

ab. `GRANT DROP ANY TRIGGER TO TRCDBU ;`

ac. `GRANT EXECUTE ANY INDEXTYPE TO TRCDBU ;`

ad. `GRANT EXECUTE ANY LIBRARY TO TRCDBU ;`

ae. `GRANT EXECUTE ANY TYPE TO TRCDBU ;`

af. `GRANT SELECT ANY SEQUENCE TO TRCDBU ;`

ag. `GRANT SELECT ANY TABLE TO TRCDBU ;`

ah. `GRANT UNLIMITED TABLESPACE TO TRCDBU ;`

ai. `GRANT UPDATE ANY TABLE TO TRCDBU;`

aj. `GRANT ANALYZE ANY TO TRCDBU;`

Setting up MSSQL

To set up MS SQL to use with IBM Endpoint Manager for Remote Control, create the database and then set up the database permissions.

Creating the database:
Use the MS SQL management studio to complete the following steps:

Note: During the installation of MS SQL, mixed mode authentication should have been set up.

1. Click **Connect**.
2. Right-click the **server tree** and click **properties**.
3. Select **security**.
4. Ensure that SQL server and authentication mode is selected.
5. Expand the **server tree**.
6. Right-click **databases**.
7. Select **Create New Database**.
8. Enter a name for the database. For example, TRCDB. Click **OK**.

The default owner of the database is user *sa*, the system administrator. Create a new user, to be the owner of the database being used with IBM Endpoint Manager for Remote Control.

Database permissions

The default system administrator is the owner of the database and therefore has the required permissions for using the database. If you have created a new user, they also have the required permissions if they have been assigned as the owner of the database.

Installing by using the server installer

The IBM Endpoint Manager for Remote Control server installer can be used on Windows operating systems, Red Hat Linux operating systems, and SUSE Linux operating systems to install a fully functional self contained 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 9.x, 10.1, or 10.5 Workgroup(WSE) and Enterprise Edition(ESE), Oracle 10 g or 11 g, or MS SQL 2005, 2008, or 2012.

Note: Click **Cancel** at any time to end the installation.

Approximate installation time

- Specifying options in the installer: 5 - 10 minutes.
- Installation of the software: 5 minutes.

1. A minimum screen resolution of 1024 by 768 pixels is recommended when you are using the installer.
2. On a Linux operating system, you must install **`libstdc++.so.5`** when you are installing and configuring the operating system. If this package is not installed, you can install package **`compat-libstdc++-33`**, which contains **`libstdc++.so.5`**.

Note: During the file copy phase of the server installation, a backup copy of any existing installation is saved. This feature is useful if there are any problems with the installation when you are upgrading. The following directory is deleted if it exists.

`[INSTALLDIR]/trcserver.bak`.

The current server installation in `[INSTALLDIR]/wlp/usr/servers/trcserver` is then renamed or moved to `[INSTALLDIR]/trcserver.bak`.

You can access the backup directory to restore or recover anything from the previous installation.

To install the IBM Endpoint Manager for Remote Control server application, complete the following steps:

1. Run the server installation file relevant to your operating system.

   Windows systems
   `trc_server_setup.exe`

   Linux systems
   `trc_server_setup.bin`

   To obtain the installation file see "Obtain the installation files" on page 19.
2. Choose the language and click **OK**.
3. At the Introduction window click **Next**.
4. Click to accept both the IBM and non-IBM terms, click **Next**.
5. Accept the default location or click **Choose** to define a location for the installation files, click **Next**.

   Note: WebSphere Application Server cannot be installed in a directory whose name contains non-English-language characters. This installation installs an embedded version of WebSphere Application Server therefore you must not choose a destination for the installation files that contains non-English_language characters.
6. Select the database, click **Next**.

   Note: Derby (10.10) is embedded in the application and is installed locally. To use DB2 or Oracle, you must install them and create a database instance, before you install IBM Endpoint Manager for Remote Control.
7. Enter the options for your selected database and click **Next**.

   Derby

a. Specify a name for the database, click **Next**. For example, `TRCDB`.

   Note: If you are using an existing database, you can choose to drop the database.

DB2

Database server
The IP address or host name of your database server.

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

Port Port on which DB2 is installed.

Note:

a. For a Windows operating system, the DB2 default port is 50000. For a Linux operating system, the default port is 50000.
b. A remote DB2 installation is limited to type four connections. A local installation can use type two or four. For type two connections, set the port value to 0.

Administrator Userid
Specify the administrator user ID that is used for logging on to the database. The user ID requires admin access to the database. If you select **create database**, the user ID must have administrator access for DB2.

Administrator password
Specify the administrator password for connecting to the database.

Database Name
Specify a name for the database. For example, `TRCDB`.

Note: If you are using a remote database, type the name of the database that was created on the remote system.

Directory path to `db2jcc.jar` file
Specify the path to the DB2 JAR files, `db2jcc.jar`, and `db2jcc_license.jar`.

Note: If you are using a remote database share the drive, on the remote system, that the DB2 JAR files are in and put this shared drive location here.

Create Database
If DB2 is installed locally (127.0.0.1), you can select to have the installer 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 or drop database if you are using a remote database.

Path for database install
Specify the path where the database can be installed. If the installation is local and you selected to create the database, the admin user that is specified must have appropriate authority

to do so. In a Windows operating system, the user must be **db2admin**, in Linux they must be a member of **db2grp1**.

Note:

Linux systems
The directory must be a directory for which the admin user ID has read and write permissions.

Windows systems
Specify a hard disk letter.

Oracle

Database server
The IP address or host name of your database server.

Note: 127.0.0.1 can be used when Oracle is installed locally.

Port Port on which Oracle is installed.

Administrator Userid
Specify the administrator user ID that is used for logging on to the database. The user ID requires admin access to the database.

Note: For an Oracle installation, a user that is called **asset** must exist. This user ID can be used here or use an existing or new user.

Administrator password
Specify the administrator password for connecting to the database.

Database Name
Specify a name for the database. The name is the SID name on the server (not the one in **tnsnames.ora**). For example, `TRCDB`.

Directory path to the oracle Java JDBC library
Specify the path to the oracle Java JDBC library. The location can be obtained from the Oracle server installation. For example, `c:\oracle\ora92\jdbc\lib\ojdbc14.jar`

MSSQL

Database server
The IP address or host name of your database server.

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

Port Port on which MS SQL is installed.

Administrator Userid
Specify the administrator user ID that is used for logging on to the database. The user ID requires admin access to the database.

Administrator password
Specify the administrator password for connecting to the database.

Database Name
Specify a name for the database. For example, `TRCDB`.

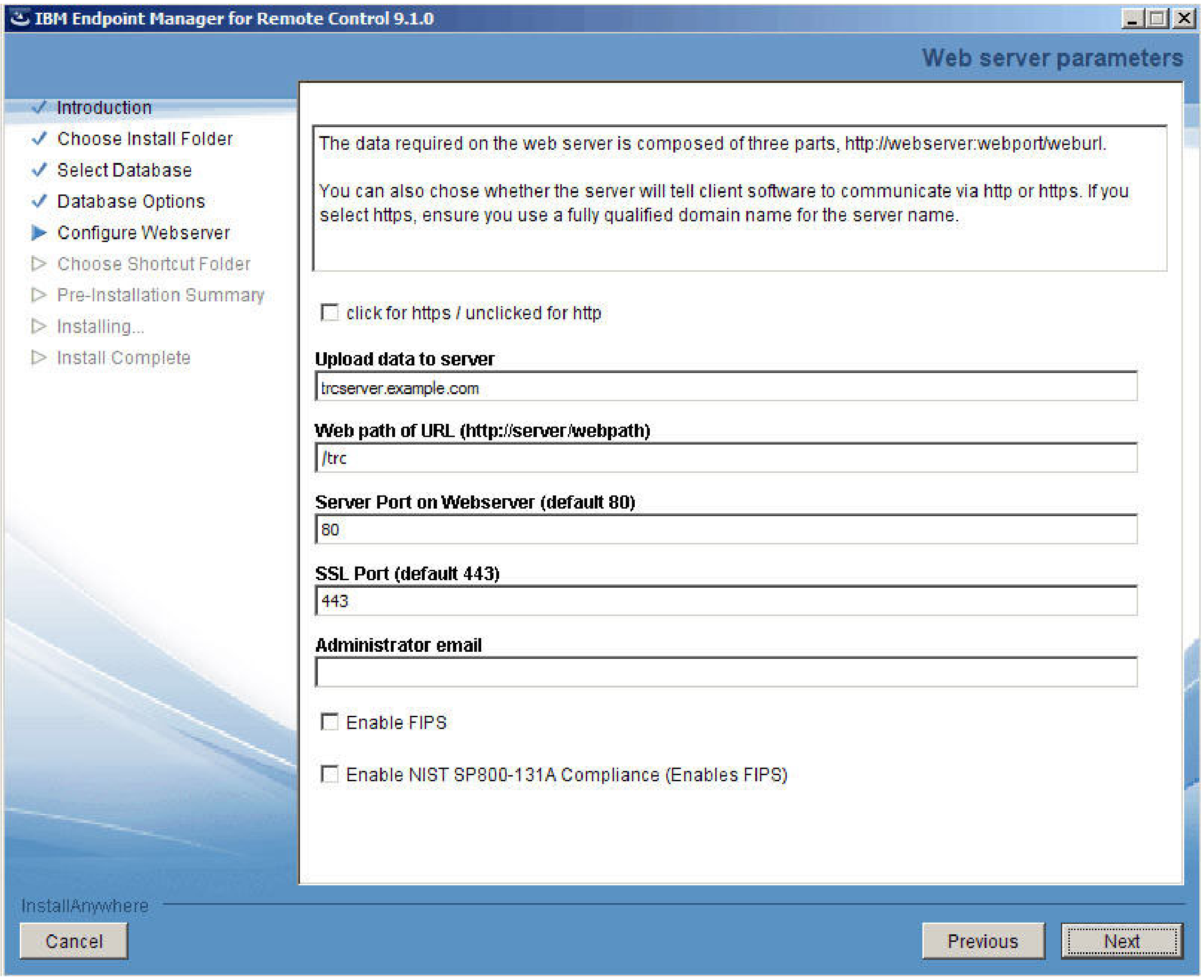
Directory path to the oracle MS JDBC Java files
Specify the path to the MS JDBC Java files. For example, `c:\mssql\jdbc2005\sqljdbc.jar`

If installed on the same server, select to create database
If MS SQL is installed locally, you can select to create the database.

Drop the database if installed locally
Select if you already have an existing database with the name that is entered for **Database Name** that you do not want to use.

If local, select path where to create the database
If you are creating the database on your local system, specify the path to where it is to be created.

8. Specify the web server parameters then click **Next**.



The data required on the web server is composed of three parts, http://webserver:webport/weburl.

You can also chose whether the server will tell client software to communicate via http or https. If you select https, ensure you use a fully qualified domain name for the server name.

□ click for https / unclicked for http

Upload data to server: trcserver.example.com

Web path of URL (http://server/webpath): /trc

Server Port on Webserver (default 80): 80

SSL Port (default 443): 443

Administrator email:

□ Enable FIPS

□ Enable NIST SP800-131A Compliance (Enables FIPS)

Figure 3. WEB server Parameters

click for https / unclicked for http
Select whether the server and target software communicates by using http or https.

Note: If you are using https, you must use a fully qualified domain name for the server name.

Upload data to server
The fully qualified name for the IBM Endpoint Manager for Remote Control server. For example, `trcserver.example.com`

Note: You must make sure that you enter the fully qualified name. The name is used for creating the URL in the `trc.properties` file that is passed to the target after 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. For example, `/trc`.

Server port on Webserver (default 80)
Specify a port for the server.

SSL Port (default 443)
Specify a port for SSL.

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

Note: To use the email function, you must have a mail server installed. Edit the `trc.properties` file after you install the IBM Endpoint Manager for Remote Control server. See the IBM Endpoint Manager for Remote Control Administrator's Guide for details of editing the properties files.

Enable FIPS
Select this option to enable FIPS compliance on the server. For more information about enabling FIPS compliance, see Chapter 8, "Federal Information Processing Standard (FIPS 140-2) compliance in IBM Endpoint Manager for Remote Control," on page 91.

Enable NIST SP800-131A Compliance (Enables FIPS)
Select this option to enable NIST SP800-131A compliance on the server. For more information about enabling NIST SP800-131A compliance, see Chapter 9, "NIST SP800-131A compliance in IBM Endpoint Manager for Remote Control," on page 101.

9. Select options for your SSL certificate and click **Next**. The certificate configuration is stored in the `ssl.xml` file.

Use an auto generated certificate store
Select this option to use a self-signed certificate that is generated by the installer.

Note: If the following options are not enabled, click **Use an auto generated certificate store** to enable them.

Overwrite an existing certificate store.

If a self-signed certificate store is already saved, the new certificate overwrites the saved certificate store. This option is the default option.

Password for a new or a previously generated certificate store.

Type a new password for the self-signed certificate. If you do not select to overwrite, type the password for your existing auto generated certificate store. If left blank, the default password **`TrCWebAS`** is saved as the password. The password must have a minimum of 6 characters.

Select an existing certificate store

Select this option to use an existing certificate store that is already saved.

Select existing certificate store location.

Click **Choose** to browse to the relevant certificate store. Select the certificate store. The file extension can be `.jks` or `.p12`.

When you use an existing certificate store, it is not copied to the installation directory during installation. The server software instance points to the location of the certificate store that you provide to function properly. Therefore, you must make sure that you save the certificate store to an adequate location on the server before you start the server installation. The certificate store must be stored in a location that does not get deleted. Therefore, do not save the file in the *`[installdir]`*`\wlp` directory or any of its subdirectories. Do not delete the certificate store at the end of the installation.If you select a previously saved auto-generated certificate store from the server installation directory, a warning is displayed. Choose **Copy file** to copy the file to a location that is not deleted during the installation. If the file is not copied successfully, you must manually copy the certificate store file to another location. Click **Choose** and select the new location of the file.

Click **Restore Default** to reset the field value to its original value.

Enter the certificate store password.

Type a password for the certificate store.

10. Select a location for the product icons to be displayed. If you select Other, click **Choose** to specify a location.

    Note: Product icons do not work when you are using Linux.
11. In the Summary window click **Install**.
12. Click **DONE** to complete the installation.

The IBM Endpoint Manager for Remote Control server software is installed including a set of properties files. These files can be edited to configure your environment.

Note:

1. It is important to make sure that the **`URL`** property in the `trc.properties` file contains the correct URL for the IBM Endpoint Manager for Remote Control server. This property is used when targets contact the server and for

determining the server during a remote target installation. If the URL property value is not correct, the remote targets are not able to contact the server successfully. Therefore, you might have problems when you start remote control sessions with the targets.

2. If the IP address of the server changes at any time, make sure that you update the URL property in `trc.properties`. Restart the server service because the targets try to contact to the old IP address until the change to the property is made.

Installing on WebSphere Application Server version 8.5: deploying the war file

IBM Endpoint Manager for Remote Control includes a license for WebSphere Application Server v8.5.

This license can be used for installations on AIX systems since the option of using the embedded Liberty profile is not available for these systems. However, this option is also available to customers that prefer to use the WebSphere Application Server on Windows systems or Linux systems too.

As described in the prerequisites section, a database needs to be created for IBM Endpoint Manager for Remote Control. After the database is created, add it to the WebSphere Data Sources.

Setting up the application server

To perform this task, a regular installation of WebSphere 8.5 Base must be installed.

Note: It is necessary to create the Websphere profile in a folder that does not include any spaces in its path. Failure to do this will cause irrecoverable issues when deploying the application war file.

Use the Websphere Integrated Solution Console to carry out the configuration.

To access the Integrated Solution Console complete the following steps:

1. In your browser type

   ```
   https://[server : port]/ibm/console
   where server is the IPaddress or name for the application server machine
   for example localhost or 192.0.2.0
   and port is the port that the server is listening on.
   ```

   The default port for the WAS admin console is 9060.
2. Log on with the ID and password that you defined when installing Websphere.

DB2 configuration:

Creating DB2 database authentication data*:*

Creating authentication data for connecting to a IBM Endpoint Manager for Remote Control DB2 database

Credentials to use for the database connection need to be established and added as a new entry to the JAAS-J2C authentication data.

To create an entry complete the following steps:

1. Click **Security > Global Security**.

2. On the right of the screen, expand **Java Authentication and Authorization Services** .
3. Click **J2C authentication data**.
4. Click **New** to add a new entry.
5. Supply the following information:

   Alias Specify a name for the authentication alias.

   Userid
   Type the user ID that was defined when DB2 was installed. Can be one of the following users.
   - The user who has permissions to access the TRCDB database, if a specific user was created.
   - The DB2 owner instance, **db2admin** in a Windows system and **db2inst1** in UNIX / Linux system.

   Password
   Type the password that you defined when you installed DB2.
6. Click **OK**.
7. Click **Save**.

Verifying the Websphere variables:
The JDBC Provider uses WebSphere environment variables to define the paths to the JDBC driver JAR files.

- db2jcc.jar
- db2jcc-javax.jar
- db2jcc-license_cu.jar
- db2jcc4.jar. If available.

Verify that the correct values are defined by completing the following steps:

1. Select **Environment / WebSphere Variables**.
2. Click **DB2UNIVERSAL_JDBC_DRIVER_PATH** and verify that this points to the DB2 libraries.

   Local DB2 database
   If you have installed the DB2 database locally the files are located in

   Windows systems

   ```
   \Program Files\ibm\sqllib\java
   ```

   Linux systems

   ```
   /opt/ibm/db2/VERSION/java
    where VERSION is the DB2 version number
   for example: /opt/ibm/db2/V8.1/java
   ```

   Remote DB2 database
   If you are using a remote DB2 database you must copy the jar files from the remote system to a location on your local system and put the path to the local files here.
3. Click **OK**.
4. Click **Save**.

Creating the DB2 data source*:*
When you have verified that the JDBC Provider is configured properly, the data source for IBM Endpoint Manager for Remote Control must be created using that JDBC Provider.

To create the data source complete the following steps:

1. Select **Resources** > **JDBC** > **Data Sources**.
2. Select the scope from the drop down menu that includes the node and the server. For example, Node=TEST-2008Node02, Server=server1.
3. Click **New**.
4. Specify the data source information.
   a. Enter basic data source information

      Data source name
      Specify a name for the data source. This can be any required name.

      JNDI Name
      This should be set to `jdbc/trcdb`

      Note: If this name is changed, you need to change the **common.properties** file also.

   b. Select JDBC Provider

      The data source will use the Universal JDBC Provider for DB2 that is predefined in WebSphere.

      1) If **DB2 Universal JDBC Driver Provider** is available, select **Select an existing JDBC provider** from the list. If it is not available, click **Create new JDBC provider**.
      2) In the Database type list, select **DB2**.
      3) Select **DB2 universal JDBC Driver provider**.
      4) From the **Implementation type** list, select **Connection pool data source**.
      5) Click **Next**.
      6) Accept the default values and click **Next**.

   c. Enter database specific properties for the data source

      Driver Type
      Select 4 from the list.

      Database name
      This is the name used when the **db2 create db** command was issued.

      Server name
      This is set to the IP or host name of the server where DB2 is installed. If DB2 is installed locally you can use localhost.

      Port number
      This is set to the port that was configured in DB2 for remote connections.

      Click **Next**.

   d. Setup security aliases

      1) From the **Component-managed authentication alias** list, select *your node*/DB2 where *your node* is the node you previously created for DB2.
      2) Accept the default of **none** in the remaining lists.
      3) Click **Next**.

   e. Review the summary and click **Finish**.
5. To save the configuration changes, click **Save**.

When the data source has been created and the changes to the profile are saved, test that the data source is correctly configured. Select the data source from the list of data sources and click Test connection. If the connection is successful, a conformation message is displayed. A failure in the test should be corrected before continuing with the installation, as IBM Endpoint Manager for Remote Control will not work without a valid data source.

Oracle configuration:

Creating Oracle database authentication data:
Credentials to use for the database connection need to be established and added as a new entry to the JAAS-J2C authentication data.

To create an entry complete the following steps:

1. Click **Security** > **Global Security**.
2. On the right of the screen, expand **Java Authentication and Authorization Services** .
3. Click **J2C authentication data**.
4. To add a new entry, click **New** .
5. Supply the following information:

   Alias Specify a name for the authentication alias.

   Userid
   Type the ID that was defined when the Oracle database was created.This is the user that you created permissions for.

   Password
   Type the password that was defined when Oracle was installed.
6. Click **OK**.
7. Click **Save**.

Creating the Oracle JDBC provider *:*
To establish access to your Oracle database you must create a JDBC provider for Oracle access.

To create the JDBC provider complete the following steps:

1. Select **Resources** > **JDBC** > **JDBC Provider**.
2. Select Scope and choose the one which has Node and Server.
3. Click **New**.
4. Specify the JDBC provider information

   Database type
   Set to `Oracle`.

   Provider Type
   Set to `Oracle JDBC Driver`.

   Implementation type
   Set to Connection Pool datasource.
5. Click **Next**.
6. The Class path is already pre-populated as `${ORACLE_JDBC_DRIVER_PATH}/ojdbc6.jar`. The directory location for `${ORACLE_JDBC_DRIVER_PATH}` to the jar files must be correct. This can be obtained from the Oracle server installation or downloaded from the Oracle website. For example, `C:\app\Administrator\product\11.2.0\dbhome_1\jdbc\lib`. Click **Next**.

7. Click **Finish**.
8. Click **Save**.

Verifying the Websphere variables:
The JDBC Provider uses WebSphere environment variables to define the paths to the JDBC driver JAR files. Verify that the correct values are defined by completing the following steps:

1. Select **Environment / WebSphere Variables**.
2. Click **ORACLE_JDBC_DRIVER_PATH** and verify that this points to the directory location chosen in step 6 on page 35 in the Creating the Oracle JDBC Provider section.
3. Click **OK**.
4. Click **Save**.

Creating the Oracle data source:
When you have verified that the JDBC Provider is configured properly, the data source for IBM Endpoint Manager for Remote Control must be created using that JDBC Provider.

To create the data source complete the following steps:

1. Select **Resources** > **JDBC** > **Data Sources**.
2. Select the scope with Node and Server.
3. Click **New**.
4. Specify the data source information
   a. Specify the data source information.

      Data source name
      Specify a name for the data source. This can be any required name.

      JNDI Name
      This should be set to `jdbc/trcdb`

      Note: If this name is changed, further changes to the **common.properties** file are also required.

      Click **Next**.

   b. Select JDBC provider

      Click **Select Existing JDBC provider** and select **Oracle JDBC Driver**. Click Next.

   c. Enter database specific properties for the data source.

      URL url=jdbc:oracle:thin@*dbserver*:1521:*SID*

      where *dbserver* is the IP address of the server.

      SID is the Oracle database SID.

      Data store helper class name
      Accept the default Data store helper class name, **Oracle 11g.data store helper**.

      Accept remaining default selected values and click **Next**.

   d. Set up security aliases

      1) Select **Component-managed authentication alias** and select the alias you previously created for Oracle.

   2) Accept the default of **none** in the remaining lists.
   3) Click **Next**.

   e. On the summary screen, click **Finish** to create the data source.

5. Click **Save**.

   You can select the newly created datasource and click **Test**, to test connectivity.

MS SQL configuration:

Creating authentication data:
Credentials to use for the database connection need to be established and added as a new entry to the JAAS-J2C authentication data.

To create an entry complete the following steps:

1. Click **Security > Global Security**.
2. On the right, expand **Java Authentication and Authorization Services** .
3. Click **J2C authentication data**.
4. To add a new entry, click **New**.
5. Supply the following information:

   Alias Specify a name for the authentication alias.

   Userid
   Type the ID that was defined when MS SQL was installed. This is the user that you created permissions for. Default is **sa**.

   Password
   Type the password that was defined when MS SQL was installed.
6. Click **OK**.
7. Click **Save**.

Creating the JDBC provider *:*
To establish access to your MS SQL database you must create a JDBC provider for MS SQL access.

To create the JDBC provider complete the following steps:

1. Select **Resources** > **JDBC** > **JDBC Provider**.
2. Select **Scope** and choose the one which has Node and Server.
3. Click **New**.
4. Specify the JDBC provider information.

   Database type
   Set to `SQL Server`.

   Provider Type
   Set to `Microsoft JDBC Driver` .
5. Select Connection pool data source.
6. Click **Next**.
7. To accept the path to the jar files, click **Next**.
8. Click **Finish**.
9. Click **Save**.

Verifying the Websphere variables:

The JDBC Provider uses WebSphere environment variables to define the paths to the JDBC driver JAR files. The correct jdbc driver software must be downloaded from Microsoft. The following version is recommended:

Microsoft JDBC Driver 4.0 for SQL Server - sqljdbc_4.0.2206.100_enu.exe

Download the SQL Server jdbc driver and copy it to the root drive of the server. Run the file to extract the driver. The `sqljdbc4.jar` file is extracted to the following directory structure:

C:\extract_path\sqljdbc_4.0\enu\

where *extract_path* is the directory chosen when you unzipped the file.

Note: The path cannot contain any spaces.

Verify that the correct values are defined by completing the following steps:

1. Select **Environment / WebSphere Variables**.
2. Click **MICROSOFT_JDBC_DRIVER_PATH** and verify that this points to the Microsoft SQL Server JDBC driver, sqljdcb4.jar file that you extracted.
3. Click **OK**.
4. Click **Save**.

Creating the MS SQL data source:
When you have verified that the JDBC Provider is configured properly, the data source for IBM Endpoint Manager for Remote Control should be created using that JDBC Provider.

To create the data source complete the following steps:

1. Select **Resources** > **JDBC** > **Data Sources**.
2. Select the scope with Node and Server.
3. Click **New**.
4. Specify the data source information
   a. Enter basic data source information

      Data source name
      Specify a name for the data source. This can be any required name.

      JNDI Name
      This should be set to **jdbc/trcdb**

      Note: If this name is changed, the **`datasource.context`** property in the `common.properties` must be changed after the WAR file is deployed. After the correct value is set, save the file and restart the application from the Websphere admin console.

   b. Select JDBC provider Select **Microsoft SQL Server JDBC Driver** or the required JDBC provider. Click **Next**.
   c. Enter database specific properties for the data source

      Database name
      This is the name used when you created the MS SQL database.

      Port number
      Port used when installing MS SQL. Default is 1433.

Server name
: This is set to the IP or hostname of the server containing the MS SQL installation. If MS SQL is installed locally you can use localhost.

d. Set up security Alias
   1) Select **Component-managed authentication alias** and select the alias you previously created for MS SQL.
   2) Accept the default of **none** in the remaining lists.
   3) Click **Next**.

e. On the summary screen, click **Finish** to create the data source.

5. Click **Save**.

Deploying the IBM Endpoint Manager for Remote Control application

When you have installed and set up the application server, deploy the application code for IBM Endpoint Manager for Remote Control on the WebSphere server. You will require the `trc.war` file which can be obtained by using the additional setup utility to extract the server installation media.

Note:

1. The heap size should be set to at least 512 MB for this type of installation.

To deploy the server application complete the following steps:

1. Extract the `trc.war` file by using the additional set up utility. For details about the files required and for running this utility, see Chapter 5, "Utility for extracting the component installation files," on page 69.
2. In the Websphere administrative console complete the following steps:
   a. Select **Applications** > **New Applications**.
   b. Click **New Enterprise Application**.
   c. Click browse and type the path to the **trc.war** file in a local or remote file system. Click **Next**.
   d. On the **Preparing for the application installation** screen select **Fast path**. Click **Next**
   e. **Step 1: Installation options** The default options can be left. The application name can be changed to something more descriptive but it must not contain any spaces. Click **Next**.
   f. **Step 2: Map modules to servers** Leave the default association to the server. Click **Next**.
   g. **Step 3: Map virtual hosts for Web modules** The default association to the default_host, virtual host can be changed if required by your setup. Click **Next**.
   h. **Step 4** It is recommended to use **`/trc`** as the context root, otherwise further changes are required in the `trc.properties` file. Click **Next**.
   i. **Step 5** displays a summary of the chosen deployment settings before proceeding with installing the IBM Endpoint Manager for Remote Control application.

      Click **Finish**A status page for the installation in progress and the outcome when the installation is finished is displayed.
   j. Click **Save** to save to the master configuration.

   The IBM Endpoint Manager for Remote Control application is displayed in the list of Enterprise Applications with the descriptive name that you entered in the Installation options step of the deployment process. Before starting the application, the default values provided in the `trc properties` files can be customized as needed. The properties files are deployed with the application and are located in the `installedApps` directory within WebSphere. For details about the defined properties in the files, see the IBM Endpoint Manager for Remote Control Administrator's Guide.

Note: Make sure that the correct value for the server IP address or server name is set in the URL field in the **trc.properties** file, to ensure that the targets connect to the correct server. If you are using HTTPS, the hostname or IP address that is set in the URL property must exactly match the value of the CN field of the SSL certificate installed on the server.

Installing from the IBM Endpoint Manager console

You can create and run a server installation task to install the server by using the IBM Endpoint Manager console. For more details, see the IBM Endpoint Manager for Remote Control Console User's Guide and the chapter about Managing target and server configuration.

Installing the target

The IBM Endpoint Manager for Remote Control target can be installed on every computer that you want to control remotely. You can also use it to start a remote control session over the internet, using a broker to make the connection.

IBM Endpoint Manager for Remote Control provides two ways to install the target component. If you have access to the IBM Endpoint Manager console, use the deployment fixlets to deploy the target. For more details, see the IBM Endpoint Manager for Remote Control Console User's Guide. Alternatively use the IBM Endpoint Manager for Remote Control target installation files.

Installing the Windows target

The `trc_target_setup.exe` file is required to install the IBM Endpoint Manager for Remote Control target component on a Windows system.

For details of how to obtain the Windows component installation files see, Chapter 4, “Installing the IBM Endpoint Manager for Remote Control components,” on page 19. Choose the appropriate method for obtaining the file.

1. Run the `trc_target_setup.exe` file.
2. Click **Next** at the welcome screen.
3. Accept the License Agreement. Click **Next**.
4. Accept the default location for the installation files, or click **Change** to select a different location.
5. Specify the host name of the IBM Endpoint Manager for Remote Control server that the target will connect to. For example `trcserver.example.com`. .

   Note: Select secure connections if you selected to us https during the server installation.
6. For advanced settings click **Advanced settings**

   Server port

   This should match the value entered for the **Server port on Webserver** parameter during the server installation.

Server Context
This is used as part of the URL for contacting the server and it should match the value entered after the '/' in the **Path to URL** field, on the Web server parameters screen during the server installation.

Use a FIPS certified cryptographic provider
Select this to enable FIPS compliance on the target. For more information about enabling FIPS compliance, see "Enabling FIPS compliance on the target" on page 97.

Enable NIST SP800-131A compliance (Enables FIPS)
Select this to enable NIST SP800-131A compliance on the target. For more information about enabling NIST SP800-131A compliance, see Chapter 9, "NIST SP800-131A compliance in IBM Endpoint Manager for Remote Control," on page 101.

7. Click **Next**.
8. On the Proxy settings screen if you are not using a proxy server click **Next**
   - To use a Proxy select **Use a proxy server or a Remote Control Gateway** and type in the required information
     a. Type in the IP address or hostname for the Proxy server.
     b. Type in the port that proxy server is listening on.
     c. Select whether you are using an HTTP proxy or a Remote Control Gateway.
     d. Select **Proxy requires authentication** if authentication is required with the proxy server. Enter the id and password required for authenticating to the proxy server.
     e. Click **Next**.
9. Accept or change the port value to be used to listen for incoming remote control sessions. Click **Next**

   Note: Your operating system may have a firewall installed by default. The inbound firewall rule for target port will default to 888. Incoming TCP connections to that port have to be open. If another port is configured instead for the IBM Endpoint Manager for Remote Control sessions, the same applies. Also traffic on the localhost loopback address 127.0.0.1 between `trc_base`, `trc_gui` and `trc_dsp` on arbitrary ports needs to be allowed.
10. Enable failover to peer to peer mode if required by selecting one of the following options :

Regardless of server status
A peer to peer session can be established between a controller and this target directly if the server is available or not. Click **Peer to Peer** policies to set the local policies that the target will use during a peer to peer session. Click **Next** to move through the peer to peer policies screens.

Only when server is down or unreachable
A peer to peer session can only be established between a controller and this target directly if the server is down or the target cannot connect to the server. Click **Peer to Peer** policies to set the local policies that the target will use during a peer to peer session. Click **Next** to move through the peer to peer policies screens.

Never A peer to peer session is not allowed directly between a controller and this target. If you select this option, continue from step 11 on page 51

Peer to Peer policies

Session Policies options

Table 8. Session policies option

Installation option	Target Property	Default Value	Description
Active	AllowActive	selected	Determines whether the target can take part in active peer to peer sessions. For more information about the different types of remote control session that can be started, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*. **selected** The target can take part in active peer to peer sessions and the Active option is available in the session type list in the controller window. The Open connection window also displays an Active option. **not selected** The target cannot take part in active peer to peer sessions and the Active option is not available in the session type list in the controller window.
Guidance	AllowGuidance	selected	Determines whether the target can take part in guidance peer to peer sessions. For more information about the different types of remote control session that can be started, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*. **selected** The target can take part in guidance peer to peer sessions and the Guidance option is available in the session type list in the controller window. The Open connection window also displays a Guidance option. **not selected** The target cannot take part in guidance peer to peer sessions and the Guidance option is not available n in the session type list in the controller window.
Monitor	AllowMonitor	selected	Determines whether the target can take part in monitor peer to peer sessions. For more information about the different types of remote control session that can be started, see the *IBM Endpoint Manager for Remote Control Controller User's Guide* . **selected** The target can take part in monitor peer to peer sessions and the Monitor option is available in the session type list in the controller window. The Open connection window also displays a Monitor option. **not selected** The target cannot take part in monitor peer to peer sessions and the Monitor option is not available in the session type list in the controller window.
Enable true color	EnableTrueColor	not selected	Determines whether true color is used as the initial color depth to display the target desktop, in the controller window at the start of a session. Used along with **Lock color depth**. **selected** The target desktop is displayed in true color 24-bit mode at the start of the session. **not selected** The target desktop is displayed in 8-bit color mode at the start of the session. This value is the default value.

Table 8. Session policies option (continued)

Installation option	Target Property	Default Value	Description
Lock color depth	LockColorDepth	not selected	Determines whether the color depth that a remote control session is started with can be changed during the session. Used along with `Enable true color`. **selected** The initial color depth, for the remote control session, is locked and cannot be changed during the session. The **Enable true color** icon is disabled in the controller window. **not selected** The initial color depth can be changed during the session.
Remove desktop background	RemoveBackground	not selected	If the target has a desktop background image set, this property can be used to remove the background 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 will stop transmitting screen updates and the controller displays a simulated screen saver, so that the controller user is aware that a screen saver is active on the remote display. The controller user can dismiss 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.

Policies options

Table 9. Peer to peer policy descriptions -

Installer screen names	Target Property	Default Value	Description
Disable chat	DisableChat	not selected	Determines whether you can 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 started from the open connection window. During the session the chat icon is available in the controller window.

Table 9. Peer to peer policy descriptions - (continued)

Installer screen names	Target Property	Default Value	Description
Save chat messages	AutoSaveChat	not selected	Determines whether the chat messages entered during a chat session are saved. **selected** The chat messages are saved as an html file with name starting chat, in the working directory of the target. The location is defined by the target property **WorkingDir**. For example on a Windows system, 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 messages are not saved to a file.
Disable file transfer from target to controller	DisableFilePull	not selected	Determine whether files can be transferred 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 from controller to target	DisableFilePush	not selected	Determines whether files can be transferred 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 this menu option 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 and you can 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	Determines whether the controller user can make and save a local recording of the session in the controlling system. Determines the availability of the record button on the controller window. For more information about recording sessions, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*. **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	Determines whether more than one controller can join a session. Determines the availability of the collaboration icon on the controller window. For details of collaboration sessions, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*. **selected** The collaboration icon is available in the controller window. **not selected** The collaboration icon is not available in the controller window.

Table 9. Peer to peer policy descriptions - (continued)

Installer screen names	Target Property	Default Value	Description
Allow session handover	AllowHandover	selected	Determines whether 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. For more details of collaboration sessions, see the *IBM Endpoint Manager for Remote Control Controller User's Guide* **selected** The handover button is available in the collaboration control panel **not selected** The handover button is not available in the collaboration control panel
Allow requests to disconnect existing session	AllowForceDisconnect	not selected	Determines whether a controller user is given the option to disconnect a session with a target so that they can connect to the target instead. Used in conjunction with the **`Managed`** and **`CheckUserLogin`** properties. For more information about disconnecting sessions, see the *IBM Endpoint Manager for Remote Control Controller User's Guide* **Set to Yes** A **Disconnect session** button is available in the message window that is displayed when you attempt to connect to the target. **Set to No** No **Disconnect session** button is available when you attempt to connect to the target. **`CheckUserLogin` must** be set to Yes and **`Managed`** set to No for **`AllowForceDisconnect`** to take effect.
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 given time, they will be automatically disconnected from the session . The timer takes effect only when **`AllowForceDisconnect`** and **`CheckUserLogin`** are set to Yes. The default value is 45.
Audit to Application Event 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 log can be used for audit purposes **selected** Entries are displayed in the application event log of the target corresponding to the each action carried out during the session. **not selected** No entries are logged to the application event log.

Security policies

Table 10. Peer to peer policy descriptions - Security policies

Installer screen names	Target property	Default Value	Description
Authenticate using Windows logon	CheckUserLogin	selected	Determines whether a logon window is displayed when the session type button is clicked on the Open Connection window. **Yes** The logon window is displayed to the controller user who must logon using a valid Windows ID and password. If the logon credentials are invalid the target refuses the session. **No** The user acceptance window does not appear and the peer to peer session is established.

Table 10. Peer to peer policy descriptions - Security policies (continued)

Installer screen names	Target property	Default Value	Description

Must be a member of these Windows groups	CheckUserGroup	see description	Default value is
			Windows systems
			`BUILTIN\Administrators`
			Linux systems
			`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 is refused. Multiple groups should be separated with a semicolon. For example: `wheel;trcusers`
			Note: By default, on a Windows system, only the administrator user is granted access. On a Linux system, by default no users are granted access. To resolve this you can complete one of the following steps
			1. If the users you want to grant access to should also be granted administrator rights, add them as members of the Administrators group on a Windows system or the wheel group on a Linux system.
			2. If the users 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 users 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.

Allow privacy	AllowPrivacy	selected	Determines whether a controller user can lock the local input and display 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.

Table 10. Peer to peer policy descriptions - Security policies (continued)

Installer screen names	Target property	Default Value	Description
Allow input lock	AllowInputLock	selected	This property works in conjunction with **Allow privacy** and on its own. Select **Allow input lock** to allow you 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:** It should be noted that if, during a session, the option to Enable Privacy is selected, the remote user input is automatically locked. It is not possible to enable privacy without also locking the input.
Enable privacy when session starts	EnablePrivacy	not selected	Determines whether the local input and display will be locked for all sessions and therefore the target user can interact with the target screen during a remote control session. **selected** The target screen is blanked out by the privacy bitmap when the session is established, preventing the target user from interacting with the screen during 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.
Enable input lock when session starts	EnableInputLock	not selected	This property works in conjunction with **Enable privacy**. Use `Enable input lock` to determine whether the target user can view their screen or not during a remote control session when privacy mode is enabled. **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 and the privacy bitmap is displayed on the target during the session. The target users mouse and keyboard are also disabled. **Note:** `Enable privacy` should be selected to allow `Enable input lock` to take effect.

Table 10. Peer to peer policy descriptions - Security policies (continued)

Installer screen names	Target property	Default Value	Description
Enable on-screen session notification	EnableOSSN	not selected	Determines whether a semi transparent layer is placed onto the target screen indicating that a remote control session is in progress. Should be used when privacy is a concern, so that the user is clearly notified when somebody can remotely view or control his PC. **selected** The semi transparent layer is displayed on the target screen displaying 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 layer does not intercept keyboard or mouse actions, therefore the user is still able to interact with their screen. **not selected** No semi transparent layer is displayed on the target screen. **Note:** This policy is only supported on targets that have a Windows operating system installed.
DisablePanicKey	DisablePanicKey	not selected	Determines whether the target user can use the Pause Break key 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 o use the Pause Break key to automatically end the remote control session.
Inactivity timeout	IdleTimeout	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.

User acceptance policies

Table 11. Peer to peer policy descriptions - User acceptance policies

Installer screen names	Target property	Default Value	Description
Take over session	ConfirmTakeOver	selected	Determines whether the user acceptance window is displayed when a remote control session is requested. **selected** The user acceptance window is displayed to the target user who can accept or refuse the session. **not selected** The user acceptance window is not displayed and the session is established.
Change session mode	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 11. Peer to peer policy descriptions - User acceptance policies (continued)

Installer screen names	Target property	Default Value	Description
File transfers	ConfirmFileTransfer	selected	Determines whether the user acceptance window is displayed when the controller user transfers files between the target and the controller. **selected** The acceptance window 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 window is not displayed and files are transferred automatically from the target to the controller system when requested.
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 on the system information icon in the controller window, the user acceptance window is displayed. The **target user** must accept or refuse the request to view the target system information. **not selected** The target system information is displayed automatically when the controller user clicks on the system information icon.
Local 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 is able to select where to save the recording to locally. If the controller user clicks **Refuse**, a message is displayed to the controller user saying that permission to record has been refused. **Note:** It should be noted that once the target user has accepted the request for recording, the acceptance window is not displayed if the controller user stops and then proceeds to restart local recording in the same session. Please also note that the message is displayed in English and is not translated. **not selected** When the controller user clicks the record icon on the controller window no message window is displayed and the controller user can then select where to save the recording to locally.

Table 11. Peer to peer policy descriptions - User acceptance policies (continued)

Installer screen names	Target property	Default Value	Description
Collaboration	ConfirmCollaboration	selected	Determines whether the user acceptance window is displayed when an additional controller user requests to join a collaboration session with a target. **selected** When the controller user tries to join the collaboration session, that the target is currently part of, 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 is not able to 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.
User 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 in conjunction with **Confirm incoming connections**. • Acceptable values 0 to 60 - If set to 0 the activity starts without displaying the message box for user acceptance on the target. **Note:** If **Confirm incoming connections** is selected, meaning that the target user is prompted to accept or refuse the session, **`Acceptance grace time`** MUST be set to a value >0 to allow the target user time to respond.
Proceed on acceptance timeout	AcceptanceProceed	not selected	Action to take if the user acceptance dialogue timeout lapses. The target user has not clicked accept or refuse within the number of seconds defined for **`Acceptance grace time`** . **selected** Session is established . **not selected** Session is not established.
Do not prompt for user acceptance when user is not logged on.	AutoWinLogon	selected	Determines whether the user acceptance window is displayed on the target, at session start, when the target user is not logged on. **selected** The acceptance window is not displayed on the target and the session is established. **not selected** The session is refused as there is no user logged on at the target to accept the session.
Enable Hide windows	HideWindows	not selected	Determines whether the **Hide windows** checkbox is displayed on the user acceptance window when **`Confirm incoming connections`** is also selected. **selected** The **Hide windows** checkbox is displayed on the user acceptance window **not selected** The **Hide windows** checkbox is not displayed on the user acceptance window.

Session scripts

Table 12. Peer to peer policy descriptions - Session scripts policies

Installer screen names	Target property	Default Value	Description
Run pre-session script	RunPreScript	not selected	Determines whether a user defined script, to perform operations on the target, should be run before the remote control session starts. It is run just after the session is authorized 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 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 details of setting up pre and post session scripts, see the Session policies chapter in 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 details of setting up pre and post session scripts, see the Session policies chapter in the *IBM Endpoint Manager for Remote Control Administrator's Guide*.
Proceed with session when script fails	ProceedOnScriptFail	not selected	Action to take if the pre or post script execution fails. A positive value or 0 is considered a successful run of the pre or post session script. A negative value, script not found or not finished running within 3 minutes is considered a failure. **selected** If the pre or post script run is a fail, the session continues. **not selected** If the pre or post script run is a fail, the session does not continue and is aborted.

11. Click **Install** to begin the installation.
12. When the installation is complete, click **Finish**.

Installing the Linux target

Use the `ibm-trc-target-`*`9.x.x`*`.i386.rpm` file to install the target component in Linux. For example, `ibm-trc-target-9.1.0.i386.rpm`. For details of how to obtain the Linux component installation files see, "Obtain the installation files" on page 19. Choose the appropriate method for obtaining the file.

You can install a default target RPM file and then configure the target after the installation.

Note: If you are using Red Hat Enterprise Linux 6.0 64-bit the following libraries along with their dependencies, need to be installed if they are not already installed, **`glibc.i686`**, **`libgcc.i686`**, **`libXmu.i686`**, **`libXtst.i686`**,**`libXp.i686`**,**`libXi.i686`**.
To install the RPM file, use the rpm command and the file specific to the version that you want to install. For example,

```
rpm -ivh ibm-trc-target-9.1.0.i386.rpm
```

When the target is installed, configure the target properties by editing the `etc/ibmtrct.conf` file. For details of target properties and their definitions, see "Installing the Windows target" on page 40.

Installing the target by using the SPB file

You can install the IBM Endpoint Manager for Remote Control target components on a Windows system and a Linux system by using the Software Package Block (SPB) installation method.

This method requires IBM® Tivoli®® Provisioning Manager. The following files are required for the installation.

Windows systems
: trc_target_win.spb

Linux systems
: trc_target_linux.spb

These files can be extracted by using the additional setup utility. For more information about using the additional setup utility, see "Using the additional setup utility" on page 69

Note: If you are using Red Hat Linux 6.0 64-bit operating system, the following libraries along with their dependencies, need to be installed if they are not already installed, `glibc.i686, libgcc.i686, libXmu.i686, libXp.i686, libXtst.i686`.

For more information about installing the software package block file please refer to the IBM Tivoli Provisioning Manager information center at : **http://pic.dhe.ibm.com/infocenter/tivihelp/v28r1/index.jsp** and the chapter that explains installing software products.

Note: Tivoli Common Agent (TCA) needs to be installed on the computers before the target can be installed using the SPB method.

Running a target custom install

Running an IBM Endpoint Manager for Remote Control target custom installation allows you to install the target software using various parameters which will allow you to perform three types of install.

unattended and silent
: No interaction is required by the user and no UI dialogs or progress bars are displayed to the user.

unattended
: No interaction is required by the user and an installation progress bar is displayed to the user.

attended
: The full installation UI is displayed and requires user interaction.

It allows you to customise installation settings and also assign the target to a specific group at install time.

Performing a target custom installation on a Windows system

To install the target software on a Windows system you need the **trc_target_setup.exe** file.

For more information about obtaining this file, see “Obtain the installation files” on page 19.

To install the target complete the following steps:

1. Create a folder in your root drive called `IBMTRC`.
2. Copy **trc_target_setup.exe** to IBMTRC.
3. Open a command prompt window and navigate to IBMTRC.
4. Type `DIR` to verify that the exe file is in this folder.
5. The command to install the target is typed in all in one line and has the following format :

   `trc_target_setup.exe /s /v"/qn [INSTALLPARAMETER1][INSTALLPARAMETER2]...[INSTALLPARAMETERX]"`You can use some or all of the install parameters below to customize your installation of the IBM Endpoint Manager for Remote Control target.

   Note: Ensure that the correct values are assigned to the parameters as no validation of the values is carried out.

   /s denotes a silent installation

   /v" The string attached to **/v** contains the parameters for `msiexec.exe`, which is a piece of software that executes the actual installation.

   /qn Performs a silent and unattended installation with no progress window and no UI.

   The above parameter can also be replaced with the following parameters

   /qb For an unattended installation with a basic UI and a small progress bar.

   /qr For an unattended installation with a reduced UI progress bar in large window.

   /qf For an attended installation with full UI.

   TRC_SERVER_HOSTNAME
   The host name or IP address of the server. This property is required. Default value is <blank>

   For example, `TRC_SERVER_HOSTNAME=trc.myserver.com`.

   TRC_SERVER_CONTEXT
   This parameter value needs to match the last part of the path in the server URL. Default value is **trc**

   For example, `TRC_SERVER_CONTEXT=trc`.

   TRC_SERVER_PORT
   If the server runs on a non-standard port, specify the port number. Default value is **80**

   For example, `TRC_SERVER_PORT=8080`.

   TRC_SERVER_PROTOCOL
   Choose between plain HTTP and secure HTTPS protocols. Valid values are http and https. Default value is http.

   For example, `TRC_SERVER_PROTOCOL=http`.

TRC_PROXY_HOSTNAME

Host name or IP address for the proxy server, if required. Default value is <blank>

TRC_PROXY_HOSTNAME=proxy.company.com.

TRC_PROXY_PORT

Port number for the proxy server. Default value is <blank>

TRC_PROXY_PORT=8080.

TRC_PROXY_USER_ID

The user ID, if the proxy requires authentication. Default value is <blank>

TRC_PROXY_USER_ID=proxyuser

TRC_PROXY_PASSWORD

The password, if the proxy requires authentication. Default value is <blank>.

TRC_PROXY_PASSWORD=v264xmpt.

TRC_PROXY_AUTH_B64

The user ID and password, format **user:password**, encoded in base64. Overrides the user ID and password properties. Use this if you do not want the password to be easily visible. Base64 is not encryption. Default value is <blank>.

TRC_PROXY_AUTH_B64=cHJveHl1c2VyOnYyNjR4bXB0

TRC_TARGET_PORT

To run the target on a non-standard port, specify the port number to use. Default value is 888

TRC_TARGET_PORT=888

TRC_SERVER_HEARTBEAT_RETRY

The amount of time, in minutes, that the target waits to retry a heartbeat when the server is not responding. Default value is 10.

TRC_SERVER_HEARTBEAT_RETRY=1

TRC_ACCESSIBILITY

Enables the accessible UI. Default value is No. Available on Windows operating system.

GROUP_LABEL

The label for the group that this target should be assigned to, if this feature is enabled on the server. To enable this feature, edit the `trc.properties` file and set **allow.target.group.override = true.** For more information about editing the properties files, see the *IBM Endpoint Manager for Remote Control Administrator's Guide*. Default value is **DefaultTargetGroup**.

Note:

a. This parameter is discarded if the target is already registered in the IBM Endpoint Manager for Remote Control server.

b. The target group specified must already be present on the server.

GROUP_LABEL=NewTargetGroup

INSTALLDIR

Use this parameter to specify the directory for installing the target software to.

For example : `INSTALLDIR= c:\trc\target`

ALLOWP2P

Use this parameter to enable P2P connections regardless of server status. Default is No.

ALLOWP2PFAILOVER

Use this parameter to enable failover to P2P when server is down or unreachable. Default is No.

AUDITTOSYSTEM

Use this parameter to log peer to peer session events in the targets application event log for auditing purposes. Default is No.

AUTOSAVECHAT

Use this parameter to save the contents of the chat window to a file on the target. Default is No.

AUTOWINLOGON

Determines whether the user acceptance window is displayed on a target where the user is not logged on. Default is Yes.

CHECKUSERGROUP

The user requesting the session must be a member of the listed groups. Default is `BUILTIN\Administrators` on Windows systems and *wheel* on Linux systems.

CHECKUSERLOGIN

Determines whether the login window is displayed when the session type button is clicked on the Open Connection window. Default is Yes

CONFIRMFILETRANSFER

Determines whether the user acceptance window is displayed when the controller user wants to transfer files from the target to the controller in a peer to peer session. Default is Yes.

CONFIRMMODECHANGE

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. Default is Yes.

CONFIRMSYSINFO

Determines whether the user acceptance window is displayed when the controller user requests to view the target system information. Default is Yes.

CONFIRMTAKEOVER

Determines whether the user acceptance window is displayed when a peer to peer session is requested. Default is Yes.

DISABLECHAT

Determines whether you can start a chat session with the target and also chat to the controller user during a peer to peer session. Default is No.

DISABLECLIPBOARD

Determines the availability of the clipboard transfer menu, which you can use to transfer the clipboard content between the controller and target during the peer to peer session. Default is No.

DISABLEFILEPULL
Determines whether you can transfer files from the target to the controller during a peer to peer session.

DISABLEFILEPUSH
Determines whether you can transfer files from the controller to the target during a peer to peer session. Default is No.

DEBUGTRACE
Enable debug logging. Debug messages are written to the target log file which can be used for problem determination. Default is No.

FIPSCOMPLIANCE
Enable the use of a FIPS certified cryptographic provider for all cryptographic functions. Default is No.

SP800131ACOMPLIANCE
Enable the use of NIST SP800-131A compliant algorithms and key strengths for all cryptographic functions. Default is No.

Note: In Silent install mode, if you want to re-configure the parameters on the existing installation, pass the parameter, **REINSTALL=ALL**. However, the parameter is ignored if it is used when you upgrade the target.

For example on the command line you would type the following command :

```
trc_target_setup.exe /s /v"/qn REINSTALL=ALL"
```

To modifying the target configuration and apply an upgrade, the following procedure can be carried out to avoid errors.

1. Perform a silent installation of the GA version of the target software with the required parameters.
2. Perform a silent installation with the new version of target software. **DO NOT** use any parameters here, if you do the target is upgraded but the parameters are ignored and are not updated.
3. Perform a silent reinstallation with REINSTALL=ALL and new parameters.

You can also specify the parameters that you want to override.

For example, to change the target port to 2222, type the following command

```
trc_target_setup.exe /s /v"/qn TRC_TARGET_PORT=2222 REINSTALL=ALL"
```

Note: To view Help options during the Installation the following command can be typed on the Command line. **trc_target_setup.exe --help**

Installing and configuring the target using the RPM file

RPM (Red Hat Package Manager) is the most common software package manager used for Linux distributions.

The following instructions will allow you to customise and build the IBM Endpoint Manager for Remote Control target RPM file.

Note: If you have the target CLI package already installed on the target you must uninstall this before installing the target software by running the following command

```
$ rpm -e ibm-trc-cli
```

Configuring the IBM Endpoint Manager for Remote Control RPM build tree:

The RPM build tree is where building an RPM takes place. By default, this tree is under `/usr/src`, but this requires building as the root user. It is recommended that you create your own RPM build tree.

Use the following steps to configure the RPM build tree in `src/rpm` in your home directory.

Type the following commands to configure the RPM build tree :

1. $ mkdir -p ~/src/rpm
2. $ cd ~/src/rpm
3. $ mkdir BUILD RPMS SOURCES SPECS SRPMS
4. $ mkdir RPMS/i[3456]86 RPMS/noarch RPMS/athlon
5. To override the default location of the RPM build tree, create or edit **.rpmmacros** in your home directory, or use the following command.

   $ echo -e "%_topdir\t${PWD}" > ~/.rpmmacros

   Note: this command overwrites the `.rpmmacros` file.
6. To verify that the configuration was successful, check that the following command gives the correct path to the **SOURCES** directory.

   $ rpm --eval %_sourcedir

   For example: `/home/yourusername/src/rpm/SOURCES`

Obtaining the IBM Endpoint Manager for Remote Control Target Source RPM package:

The source RPM package is obtained from the installation files. By default, this package will extract the install files for the target to the `IBM/Tivoli_Remote_Control` directory inside your home directory.

Installing the Source RPM package:

Installing a source RPM package installs the files that are needed to build or rebuild the package into the RPM build tree.

Use the following command to install the package for the Target:

```
$ rpm -ivh ~/IBM/Tivoli_Remote_Control/RCTarget/ibm-trc-target-9.x.x.src.rpm
```

Where *9.x.x* is relevant to the version that you want to install. For example, 9.1.0.

Note: This command might generate warnings about users and groups that do not exist. These warnings are because your system does not have the user and groups that were used to build the original package. You can ignore these warnings.

Examples of the warning messages:-

Warning: user *user name* does not exist - using root

Warning: group build does not exist - using root

Warning: group trc_build does not exist - using root

To verify that this step was successful, check the `SPECS` and the `SOURCES` directories and make sure that the following files are there:

```
$ ls SPECS/ SOURCES/
```

```
SOURCES/:ibm-trc-target.tar
```

```
SPECS/: ibm-trc-target.spec
```

Customizing the SPEC file:

To make sure that you can tell the customized package apart from the original package, you must customize the version number in the SPEC file. It is recommended that you use an identifier that is based on your organization's name. In this example "BFC Fiction Ltd" is used.

To customize the SPEC file, complete the following steps:

1. Edit the SPEC file. You can use your favorite editor instead of vi.
   ```
   $ vi SPECS/ibm-trc-target.spec
   ```
2. Change the line **`Version: ${_buildversion}`** to **`Version: 5.1.2.bfc`**
3. The release field must be updated as well. This field can be used to track the version of your customized builds.

   Change **`Release: %{_buildlevel}`** to **`Release: 1`**

Customising the default configuration file:

Before the configuration file can be customised, it needs to be extracted from the tar archive into a temporary directory.

To extract the configuration file complete the following steps:

1. Create a temporary directory
   ```
   $ mkdir SOURCES/ibm-trc-target
   $ cd SOURCES/ibm-trc-target
   ```
2. Extract all the files from the tar archive
   ```
   $ tar xvf ../ibm-trc-target.tar
   ```
3. Edit the configuration file with the customisations necessary for your environment.
   ```
   $ vi ibmtrct.conf
   ```
   For example: to enable the target for peer to peer failover set ALLOWP2P to Yes and ALLOWP2PFAILOVER to Yes. See
4. When the changes are complete the tar archive needs to be recreated so that the modifications are used by the RPM build process.
   ```
   $ tar cvf ../ibm-trc-target.tar *
   $ cd ../..
   ```

Building your customized IBM Endpoint Manager for Remote Control target RPM package:

The following command will rebuild the RPM package using your customized configuration file.

```
$ rpmbuild -ba SPECS/ibm-trc-target.spec
```

The RPM package will be saved to `RPMS/i386/ibm-trc-target-5.1.2.bfc-1.i386.rpm`

You should now run the following command to install your customised target.

```
$ rpm -ivh RPMS/i386/ibm-trc-target-5.1.2.bfc-1.i386.rpm
```

Installing the target by using the SPB file

You can install the IBM Endpoint Manager for Remote Control target components on a Windows system and a Linux system by using the Software Package Block (SPB) installation method.

This method requires IBM® Tivoli® Provisioning Manager. The following files are required for the installation.

Windows systems
trc_target_win.spb

Linux systems
trc_target_linux.spb

These files can be extracted by using the additional setup utility. For more information about using the additional setup utility, see "Using the additional setup utility" on page 69

Note: If you are using Red Hat Linux 6.0 64-bit operating system, the following libraries along with their dependencies, need to be installed if they are not already installed, `glibc.i686`, `libgcc.i686`, `libXmu.i686`, `libXp.i686`, `libXtst.i686`.

For more information about installing the software package block file please refer to the IBM Tivoli Provisioning Manager information center at : **http://pic.dhe.ibm.com/infocenter/tivihelp/v28r1/index.jsp** and the chapter that explains installing software products.

Note: Tivoli Common Agent (TCA) needs to be installed on the computers before the target can be installed using the SPB method.

Installing the controller

The IBM Endpoint Manager for Remote Control controller can be installed locally on your system, to be used for connecting to a target directly if peer to peer mode is enabled.

IBM Endpoint Manager for Remote Control provides two ways to install the controller component. If you have access to the IBM Endpoint Manager console use the deployment fixlets to deploy the controller. For more details, see the IBM Endpoint Manager for Remote Control Console User's Guide. Alternatively use the IBM Endpoint Manager for Remote Control controller installation files.

Installing the controller on a Windows system

The `trc_controller_setup.exe` file is required to install the controller component on a Windows system.

For more information about how to obtain the component installation files for a Windows system, see Chapter 4, "Installing the IBM Endpoint Manager for Remote Control components," on page 19. Choose the appropriate method for obtaining the file.

1. Run the `trc_controller_setup.exe` file.
2. On the file download window, select **Run** or **Save**

   Run Select **Run** to start the installation wizard for installing the controller software.

   a. Click **Next** at welcome screen.

b. Accept the license agreement, click **Next**.

c. Accept or change the location for the installation files, click **Next**.

d. Click **Install**.

e. Click **Finish**.

Note: If the controller software is already installed on the system, modify, repair, or remove options are available.

Save Select **Save** to save the `trc_controller_setup.exe` file to a selected location.

Note: Run this executable file to install the controller software by using the same procedure as in the Run section.

The controller is installed to the default location `\Program Files\IBM\Tivoli\Remote Control\Controller` or the location that is selected during the installation.

Installing the Linux controller

Use the `ibm-trc-controller-`*`9.x.x`*`.noarch.rpm` and `ibm-trc-controller-jre-`*`9.x.x`*`.i386.rpm` files to install the controller component in Linux. Where *9.x.x* is relevant to the version that you want to install. For example, 9.1.0. For details of how to obtain the Linux component installation files see, Chapter 4, “Installing the IBM Endpoint Manager for Remote Control components,” on page 19. Choose the appropriate method for obtaining the file.

You can install the controller in two modes in Linux, a FIPS-compliant controller or a standard controller.

Type the relevant command for installing the controller. Where *9.x.x* is relevant to the version that you want to install. For example, 9.1.0.

- For the standard controller type

  ```
  #rpm -ivh ~/IBM/Tivoli_Remote_Control/RCTarget/ibm-trc-controller-
  9.x.x.noarch.rpm
  ```

- For a FIPS-compliant controller, install the standard controller and the FIPS-compliant JRE by running both commands.

  ```
  #rpm -ivh ~/IBM/Tivoli_Remote_Control/RCTarget/ibm-trc-controller-
  9.x.x.noarch.rpm
  ```

  ```
  #rpm -ivh ~/IBM/Tivoli_Remote_Control/RCTarget/ibm-trc-controller-jre-
  9.x.x.i386.rpm
  ```

Note: Standard controller installations work with the `ibm-trc-controller-9.x.x.noarch.rpm` file, with an alternative JRE installed on the system. If the controller is to be FIPS-compliant, the `ibm-trc-controller-jre-9.x.x.i386.rpm` must be installed. The `ibm-trc-controller-jre-9.x.x.i386.rpm` file can also be installed even if the controller is not going to be run in FIPS mode.

You can start the controller from your applications list when it is installed.

Installing the controller in other supported operating systems

If you are using a supported operating system other than Windows operating system, Linux, AIX, or Solaris (SPARC), extract the controller files by using the additional setup utility. Then, copy the required files to the system that you are running the controller on. You must run the additional setup utility on a Windows, Linux, AIX, or Solaris(SPARC) system. For more information about obtaining the additional setup utility files, see Chapter 4, “Installing the IBM Endpoint Manager for Remote Control components,” on page 19.

Note: Ensure that you install a supported version of Java to run the controller on the other supported operating system. See “Controller requirements” on page 13.

To install the controller, complete the following steps:

1. After you extract the installation files, navigate to the `RCController` directory.
2. Copy the file `trc_console.zip` to the system that you are running the controller on.
3. Extract the files from the `trc_console.zip` file.
4. Type the following command to run the controller

   `java -jar TRCConsole.jar`

Installing a preconfigured controller component

You can configure the controller component by editing the `trc_controller.cfg` configuration file after the controller is installed. You can also apply custom configuration settings when you install the controller component.

Preconfiguring the controller is useful for unattended installations. You can set your configuration file values in the configuration file and copy the file to the computers that you want to install the controller on. Your configuration settings are installed together with the controller. The configuration values are set in the `trc_controller.cfg` file. You can create the file and add your custom values or you can edit a default configuration file. If you do not apply any preconfiguration, the default configuration file is installed when you install the controller component.

Preconfiguring the controller for a Windows operating system installation

1. Copy the `trc_controller.cfg` file to the same directory as the `trc_controller_setup.exe` or `trc_controller.msi file`.
2. Run the controller installation file.

The controller is installed with your configured settings.

Note: Preconfiguring the controller is not supported for installation on a Linux operating system. If necessary, you can modify and rebuild the controller `.rpm` file from the source `.rpm` file.

Use the content of the default configuration file to create your custom configuration file and set your own values.

```
# Licensed Materials - Property of IBM
#
# 5725-C43
#
# Copyright International Business Machines Corp. 2011, 2014. All Rights Reserved
#
# US Government Users Restricted Rights - Use, duplication or disclosure
# restricted by GSA ADP Schedule Contract with IBM Corp.

fips.compliance=false

sp800131a.compliance=false
```

```
enable.address.history=true

enable.user.history=false

enable.domain.history=true

history.max.items=20

tool01.ToolName = Control Panel
tool01.ToolCommand = [SystemFolder]\\control.exe
tool01.ToolParameters =
tool01.ToolUser =

tool02.ToolName = Command Prompt
tool02.ToolCommand = [SystemFolder]\\cmd.exe
tool02.ToolParameters =
tool02.ToolUser =

tool03.ToolName = Administrator Command Prompt
tool03.ToolCommand = [SystemFolder]\\cmd.exe
tool03.ToolParameters =
tool03.ToolUser = admin

tool04.ToolName = Task Manager
tool04.ToolCommand = [SystemFolder]\\taskmgr.exe
tool04.ToolParameters =
tool04.ToolUser =

tool05.ToolName = Windows Explorer
tool05.ToolCommand = [WindowsFolder]\\explorer.exe
tool05.ToolParameters =
tool05.ToolUser =

tool06.ToolName=Terminal
tool06.ToolCommand=/usr/bin/gnome-terminal
tool06.ToolParameters =
tool06.ToolUser =

tool07.ToolName=Control Panel
tool07.ToolCommand=/usr/bin/gnome-control-center
tool07.ToolParameters =
tool07.ToolUser =

tool08.ToolName=
tool08.ToolCommand=
tool08.ToolParameters =
tool08.ToolUser =

tool09.ToolName=
tool09.ToolCommand=
tool09.ToolParameters =
tool09.ToolUser =

tool10.ToolName=
tool10.ToolCommand=
tool10.ToolParameters =
tool10.ToolUser =

# Custom keys

# example.KeySequenceName = Inject F1
# example.KeySequenceValue = [F1]
#
# For a list of supported key codes, please refer to the User's Guide

key01.KeySequenceName =
key01.KeySequenceValue =

key02.KeySequenceName =
key02.KeySequenceValue =

key03.KeySequenceName =
key03.KeySequenceValue =
```

Installing the command line tools

The command line tools contain two utilities that can be run from the command line to start a remote control session with a target or run commands on a target system without target user interaction. These commands can be useful if you want to connect to a target without using the usual IBM Endpoint Manager for Remote Control Server interface or for using as part of a script to run multiple commands in an automated fashion. The command line tools are only available to run on Windows operating systems and Linux operating systems.

IBM Endpoint Manager for Remote Control provides two ways to install the command line tools. If you have access to the IBM Endpoint Manager console, use the deployment fixlets to deploy the tools. For more information about deploying the components, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*. Alternatively use the IBM Endpoint Manager for Remote Control controller installation files.

Installing the cli tools on a Windows system

The `trc_cli_setup.exe` file is required to install the controller component on a Windows system.

For more information about how to obtain the Windows component installation files see, Chapter 4, "Installing the IBM Endpoint Manager for Remote Control components," on page 19. Choose the appropriate method for obtaining the file.

1. Run the `trc_cli_setup.exe` file.
2. On the file download window select **Run** or **Save**

   Run Select **Run** to start the install shield wizard for installing the command line software.

   a. Click **Next** at the welcome screen.
   b. Accept the license agreement, click **Next**.
   c. Accept or change the location for the installation files, click **Next**.
   d. On the server address screen type in the required information and click **Next** :

Server host name
Enter the IP address or server name of the IBM Endpoint Manager for Remote Control server.

Use secure connections (https)
Select https to use secure connections to contact the server.

Advanced settings
Click **Advanced settings** for more configuration settings.

Server port
Enter the port number that the server is listening on.

Server context
Enter a value for the server context. For example, `trc`.

Use a FIPS certified cryptographic provider
Select **Use a FIPS certified cryptographic provider** for installing FIPS compliant tools.

Enable NIST SP800-131A compliance (Enables FIPS)
Select **Enable NIST SP800-131A compliance (Enables FIPS)** for installing NIST SP800-131A compliant tools.

e. On the Proxy settings panel if you are not using a proxy server click **Next**.
   - If you are using a Proxy select **Use a proxy server or a Remote Control Gateway**. Type in the relevant information
     1) Type in the IP address or host name for the proxy server.
     2) Type in the port that proxy server is listening on.
     3) Select **Use an HTTP proxy** or **Use a Remote Control Gateway**.
     4) Select **Proxy requires authentication** and enter the user ID and password for authenticating to the proxy server.
     5) Click **Next**.

f. Accept the default port or type in a required value, click **Next**

g. Click **Install**.

h. Click **Finish**.

Save Select **Save** to save the `trc_cli_setup.exe` file to a specific location.

Note: Run this executable file to install the command-line software.

The following executable files are in the selected directory.

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 information about using the command line tools, see the*IBM Endpoint Manager for Remote Control Controller User's Guide*

Installing the tools in Linux

Use the `ibm-trc-cli-9.x.x.i386.rpm` file to install the cli tools in Linux. Where *9.x.x* is relevant to the version that you want to install. For example, 9.1.0. For more information about obtaining the Linux component installation files, see Chapter 4, "Installing the IBM Endpoint Manager for Remote Control components," on page 19. Choose the appropriate method for obtaining the file.

Note: If the `ibm-trc-target` RPM file is installed, you do not need to install the `ibm-trc-cli` RPM file because the CLI commands are already included in the target. For more information about using the commands, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*.

1. Type, the following command to install the command-line software. Where *9.x.x* is relevant to the version that you want to install. For example, 9.1.0.

   ```
   $ rpm -ivh ~/IBM/Tivoli_Remote_Control/RCTarget/ibm-trc-cli-
   9.x.x.i386.rpm
   ```
2. When the installation is complete edit the `/etc/ibmtrct.conf` file and set your configuration.
   - Set the value of **ServerURL** to the host name or IP address of your IBM Endpoint Manager for Remote Control Server.
   - For FIPS-compliance set the value of **FIPSCompliance** to Yes.
   - For NIST SP800-131a compliance, set the value of *SP800131ACompliance* to yes.
3. Save the file.

For more information about using these commands, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*.

Installing gateway support in IBM Endpoint Manager for Remote Control

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

IBM Endpoint Manager for Remote Control provides two ways to install the gateway support. If you have access to the IBM Endpoint Manager console use the deployment fixlets to deploy gateway support. For more details, see the IBM Endpoint Manager for Remote Control Console User's Guide. Alternatively you can use the IBM Endpoint Manager for Remote Control gateway support installation files.

Installing Windows gateway support

The `trc_gateway_setup.exe` file is required to install gateway support in a Windows operating system. For more information about how to obtain the Windows gateway support files see, Chapter 4, "Installing the IBM Endpoint Manager for Remote Control components," on page 19. Choose the appropriate method for obtaining the file.

Note: You can also install gateway support with no user interaction by performing a silent installation. For more information about a silent installation, see "Installing the gateway support by performing a silent installation" on page 66.

To install gateway support, complete the following steps:

1. Run the `trc_gateway_setup.exe` file.
2. Click **Next** at the Welcome screen.
3. Accept or change the installation location and click **Next**.
4. Click **Install**.
5. Click **Finish** when the installation is complete.

When the gateway support is installed you must configure it for your environment. For more information about configuring gateway support, see the *IBM Endpoint Manager for Remote Control Administrator's Guide*.

Installing the gateway support by performing a silent installation

To install the gateway support on a Windows system by performing a silent installation, complete the following steps :

1. Create a folder in your root drive called `IBMTRC`.
2. Copy `trc_gateway_setup.exe` file to `IBMTRC`.
3. Open a command prompt window and navigate to `IBMTRC`.
4. Type in the following command all in one line : `trc_gateway_setup.exe /s /v"/qn"`

   /s Denotes a silent installation.

   /v" The string attached to /v contains the parameters for `msiexec.exe`, which is a piece of software that runs the actual installation.

   /qn Perform a silent installation with no progress window.

For more information about configuring gateway support, see the *IBM Endpoint Manager for Remote Control Administrator's Guide*.

Installing Linux gateway support

Use the `ibm-trc-gateway-`*9.x.x*`.i386.rpm` file to install gateway support in Linux. Where *9.x.x* is the version that you want to install. For more information about obtaining the Linux gateway support files, see Chapter 4, "Installing the IBM Endpoint Manager for Remote Control components," on page 19. Choose the appropriate method for obtaining the file.

Type the following command at a command prompt to install the gateway support. Where *9.x.x* is the version that you want to install. For example, 9.1.0.

```
$ rpm -ivh ibm-trc-gateway-9.x.x.i386.rpm
```

When the gateway support installed, configure it for your environment. For more information about configuring gateway support, see the *IBM Endpoint Manager for Remote Control Administrator's Guide* .

Installing broker support

Broker support should be installed on the machines that connect the controller to the target machine when the target machine is not directly accessible by the controller and the connection is made across the internet.

IBM Endpoint Manager for Remote Control provides two ways to install the broker support. If you have access to the IBM Endpoint Manager console, use the deployment fixlets to deploy the broker support. For more details, see the IBM

Endpoint Manager for Remote Control Console User's Guide. Alternatively use the IBM Endpoint Manager for Remote Control broker installation files.

Installing Windows broker support

The IBM Endpoint Manager for Remote Control broker installation files are executable files that can be used to install broker support on a Windows computer.

The `trc_broker_setup.exe` file is required to install broker support on a Windows system. For more information about how to obtain the Windows broker support files, see Chapter 4, “Installing the IBM Endpoint Manager for Remote Control components,” on page 19. Choose the appropriate method for obtaining the file.

To install broker support on a Windows computer, complete the following steps.

1. Run the `trc_broker_setup.exe` file.
2. Click **Next** at the welcome screen.
3. Accept licence terms and click **Next**.
4. Accept the default location or change the installation destination folder. Click **Next**.

   Default location is `\Program Files\IBM\Tivoli\Remote Control\Broker`
5. Click **Install**.
6. Click **Finish**.

The following files are installed in the ***[working dir]***`\Broker` directory, where ***[working dir]*** is determined by the version of Windows operating system that you are installing the broker support on.

For example, `\Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control`.

- `trc_broker.properties`
- `TRCICB-`*`computername-day`*`.log` where *computername* is the computer name of the machine that the broker is installed on and *day* is the day of the week that the broker is installed on.

You must check that the **IBM Endpoint Manager for Remote Control- Internet Connection Broker** service has registered and is started.

Installing Linux broker support

You can install the broker support on a Linux computer by using the RPM file that is provided in the IBM Endpoint Manager for Remote Control installation files.

Use the `ibm-trc-broker-`*`9.x.x`*`.i386.rpm` file to install the broker support in Linux. Where *9.x.x* is the version that you want to install. For example, 9.1.0. For more information about obtaining the Linux component installation files, see Chapter 4, “Installing the IBM Endpoint Manager for Remote Control components,” on page 19. Choose the appropriate method for obtaining the file.

At a command prompt type, the following command to install the command-line software. Where *9.x.x* is the version that you want to install. For example, 9.1.0.

```
rpm -ivh ibm-trc-broker-9.x.x.i386.rpm
```

The following files are installed in the `/opt/ibm/trc/broker` directory.

- libcrypto.so.1.0.0
- libssl.so.1.0.0
- trc_icb
- a licence directory

The `trc_broker.properties` file is installed in the `/etc` directory.

When the broker support is installed, configure the broker properties by editing the `trc_broker.properties` file.

Chapter 5. Utility for extracting the component installation files

IBM Endpoint Manager for Remote Control provides a utility that you can use to extract the installation files required for each component.

Note: This utility can only be run on computers with a Windows, Linux, AIX, or **Solaris SPARC** operating system installed. For computers running a supported operating system other than these, for example HP-UX, extract the installation files by running the utility on another computer. Copy the extracted files to the required computer.

Use the following files to run the additional setup utility:

Windows systems
`trc_additional_setup.exe`

AIX, Linux, Solaris systems
`trc_additional_setup.bin`

For more information about how to obtain these files, see "Obtain the installation files" on page 19.

You can extract the following component installation files.

- **Server Installation media**: to extract the server files and copy then to a specific location. Use these files to perform a manual server installation. The `trc.war` file and instructions are extracted.
- **Target Installation media**: to extract the target files and copy them to a specific location. The target .msi, .exe, .rpm, .spb, and instructions files are extracted.
- **Controller installation media**
- **Command Line Interface Installation Media**
- **Gateway Installation Media**
- **Internet Connection Broker Installation Media**

Using the additional setup utility

To run the additional setup utility complete the following steps:

1. Run the `trc_additional_setup` file relevant to your operating system. For more details of which file you should use. see Chapter 5, "Utility for extracting the component installation files"
2. Select the required language and click **OK**.
3. Accept the licence agreement and click **Next**.
4. Deselect the options that you **do not** want to extract the files for. Only the options you require must remain selected.
   a. **Server Installation media**: to extract the files for installing the server.
   b. **Target Installation media**: to extract the files for installing the target.
   c. **Controller Installation media**: to extract the files for installing the controller.
   d. **Command Line Interface Installation media**: to extract the files for running the command line interface.

   e. **Gateway Installation media**: to extract the files for installing gateway support.
   f. **Internet Connection Broker Installation media**: to extract the files for installing broker support.
5. Click **Next**.
6. Accept or change the installation folder. Click **Next**.
7. On the summary screen, click **Install**.
8. When complete, click **Done**.
9. Navigate to the chosen installation folder.

The installation files are in the following directories:

- `RCServer` - server installation file, `trc.war`.
- `RCTarget` - target installation files.
- `RCController` - controller installation files.
- `RCCLI` - command line tools installation files.
- `RCGateway` - gateway installation files.
- `RCBroker` - broker installation files.

Chapter 6. Managing the component services

After you install the IBM Endpoint Manager for Remote Control components, if you change their configuration, you can stop, start, or restart the component services.

Follow the steps in the section that is relevant to your operating system.

Starting, stopping, or restarting the Windows components

You can start, stop, or restart the IBM Endpoint Manager for Remote Control Windows components from within the Control Panel.

To manage the IBM Endpoint Manager for Remote Control Windows components, complete the following steps.

1. In **Control Panel** select **Administrative tools** > **Services**.
2. Highlight the relevant service.

   Server service
   : **IBM Endpoint Manager for Remote Control- Server**

   Target service
   : **IBM Endpoint Manager for Remote Control- Target**

   Gateway service
   : **IBM Endpoint Manager for Remote Control- Gateway**

   Broker service
   : **IBM Endpoint Manager for Remote Control- Internet Connection Broker**
3. Choose the appropriate method for selecting an action for the service. You can right-click and select **start**, **stop**, or **restart** or select **Start**, **Stop**, or **Restart** from the list on the left.

Starting, stopping, or restarting the Linux components

You can start, stop, or restart the IBM Endpoint Manager for Remote Control Linux components from within the Control Panel.

Depending on the version of Linux you are using, use one of the following commands to manage the components.

- `/sbin/service` *`component action`*
- `/etc/init.d/`*`component action`*

where *component* is the component service that you want to manage and *action* is start, stop, or restart.

server For example, to start the server service.
- `/sbin/service trcserver start`
- `/etc/init.d/trcserver start`

target For example, to stop the target service.
- `/sbin/service ibmtrct stop`
- `/etc/init.d/ibmtrct stop`

gateway

For example, to restart the gateway service.

- `/sbin/service ibmtrcgw restart`
- `/etc/init.d/ibmtrcgw restart`

broker

For example, to restart the broker service.

- `/sbin/service ibmtrcicb restart`
- `/etc/init.d/ibmtrcicb restart`

Chapter 7. Performing required configuration

After you have installed the IBM Endpoint Manager for Remote Control server and target software, some configuration might be required to allow you to set things up to your requirements.

Enabling email

To use the email function, for example for a forgotten password, to export and email a report, or to request access to certain targets, you should have an email server installed and set up.

To enable the email function complete the following steps :

1. Logon to IBM Endpoint Manager for Remote Control server with a valid admin id and password.
2. Click **Admin** > **Edit properties files**.
3. Select **trc.properties**.
4. Edit the following variables

   email.enabled
   Set to true to enable email.

   smtp.server
   Set this to the address of your mail server.

   smtp.authentication
   Set to true of false depending on whether you want the SMTP server to authenticate with the smtp id and password or not .

   smtp.userid
   Userid for the smtp server .

   smtp.password
   Password for the smtp server .
5. Click **Submit**.

The email function is enabled.

Configuring LDAP

IBM Endpoint Manager for Remote Control provides Lightweight Directory Access Protocol Version 3 support that you can use to enable authentication and integration of users and their associated group membership into the IBM Endpoint Manager for Remote Control database.

All configuration information required for LDAP authentication is located in the file `ldap.properties`. Before beginning the configuration, some prerequisite information should be obtained. This information will simplify the configuration process and includes :

- A username and password to be used by IBM Endpoint Manager for Remote Control to establish a connection with the Active Directory server. This username should have the authority necessary to read all the required information from the directory tree.

- The fully qualified server hostname or IP address of the Active Directory server to be used with IBM Endpoint Manager for Remote Control.
- In an Enterprise scenario, a secondary backup LDAP server would also be configured in IBM Endpoint Manager for Remote Control.

Setting up LDAP synchronization

To enable LDAP authentication, synchronization with the LDAP server must also be enabled. Edit values in the `common.properties` file and the `ldap.properties` file to enable synchronization.

To perform the basic configuration for LDAP authentication complete the following steps :

1. Click **Admin** > **Edit properties file**.
2. Ensuring that you are editing the `common.properties` file, edit the following properties

   authentication.LDAP
   to enable or disable LDAP authentication.

   true LDAP user authentication is performed.

   Note: It should be noted that when LDAP has been enabled, new users and new user groups should be created in Active Directory and **not** in IBM Endpoint Manager for Remote Control. This is because each time the synchronization with Active Directory takes place the users and user groups are deleted from the IBM Endpoint Manager for Remote Control database and then imported from Active Directory.

   false LDAP user authentication is not performed. Users are authenticated using the IBM Endpoint Manager for Remote Control database.

   ```
   authentication.LDAP=true
   ```

   authentication.LDAP.config
   Defines the file containing the LDAP configuration properties

   ```
   authentication.LDAP.config=ldap.properties
   ```

   sync.ldap
   used to synchronize the users and groups from Active Directory with the IBM Endpoint Manager for Remote Control database. Takes the values true, to synchronize or false, for no synchronization.

   true The LDAP server is synchronized with the IBM Endpoint Manager for Remote Control database to reflect any changes made in LDAP.

   false No synchronization takes place. If synchronization is disabled, you should manually import the users into the IBM Endpoint Manager for Remote Control database otherwise they will not be able to logon to the IBM Endpoint Manager for Remote Control server. The users must exist in the IBM Endpoint Manager for Remote Control database so that they can be associated with the relevant permissions required to establish remote control sessions.

   Note: The synchronization is performed by running a scheduled task which pulls the LDAP info from the LDAP server and updates the database with any changes that have been made to the user or group information. Within the trc.properties file there are two attributes which define the time interval that the scheduler uses to check for scheduled tasks

scheduled.interval
The frequency, in numeric value, that the server should check for scheduled tasks. The number of units of time between each checking period. Default is 60.

Note: If you change this value, restart the server service for the new value to take effect.

scheduled.interval.period
The unit of time to be used along with the scheduled interval to specify how often the server should check for scheduled tasks. Default is minutes.

The **scheduled.interval** attribute is set to 60 as default and the **scheduled.interval.period** set to minutes, that is, the server checks for and runs any scheduled tasks every 60 minutes. To accurately reflect any changes made to the users or groups, set the **scheduled.interval** attribute to a lower value so that the synchronization can occur more frequently.

3. Click **Submit**.

Verifying connection information

The parameters in this section define how IBM Endpoint Manager for Remote Control will connect to the LDAP server. The connection is used query the LDAP server for the user and group information that is imported into IBM Endpoint Manager for Remote Control.

Any changes to the ldap.properties file will not take effect until the IBM Endpoint Manager for Remote Control application is reset using **Admin**,**Reset Application**. To avoid multiple restarts or an extended outage use an LDAP browser and the **LDAP Configuration Utility** as an aid to the entire configuration process.

To verify the connection information using an LDAP browser, define an LDAP server profile by entering the fully qualified hostname and credential information. When opening an LDAP browser for the first time, provide details for a new profile.

The profile usually includes the following information

Host hostname or FQDN of the preferred LDAP Server

Port port used to communicate with the directory. Typically, this would be port 389 but if your environment contains child domains port 3268 should be used instead. Port 3268 points to the Global Catalog which will include the child domains.

Base DN
The 'root' point to bind to the server

```
for example

 DC=mydomain,DC=mycompany,DC=com
```

After the information has been entered, the LDAP Browser displays attribute names and values available at the root of the Active Directory tree.

When a connection is established use the same information used in the LDAP browser to set the parameters in the `ldap.properties` file.

- Click **Admin** > **Edit properties files**
- Select **ldap.properties** from the list
- When modifications are complete, click **Submit**

The application must be reset for the changes to take effect. Click **Admin** > **Reset Application** or restart the server service.

The properties file can also be edited manually by locating it on the IBM Endpoint Manager for Remote Control Server, which is usually in the following location `[`*`installdir`*`]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes` directory (where *installdir* is the directory that the IBM Endpoint Manager for Remote Control Server is installed in

```
for example :
C:\Program Files\IBM\Tivoli\TRC\server\wlp\usr\servers\trcserver
\apps\TRCAPP.ear\trc.war\WEB-INF\classes
```

Note: IBM Endpoint Manager for Remote Control is provided with a default `ldap.properties` file and many of the extended configuration options are commented out. To enable these, the file must be edited manually

Configuring connection credentials

Use the following properties to set valid credentials for connecting to the LDAP server.

Note: Check that a successful connection to the LDAP browser can be established by using these credentials to verify that they are valid.

1. Edit the `ldap.properties` file.
2. Configure the following properties.

   ldap.connectionName

   The username that is used to authenticate to a read-only LDAP connection. If left not set, an anonymous connection is attempted.

   ```
   For example : administrator@mydomain.mycompany.com
   ```

   ldap.connectionPassword

   The password that is used to establish a read-only LDAP connection. The password can be entered here in plain text or it can be encrypted.

   ldap.connectionPasswordEncrypted

   True The LDAP password is encrypted.

   False The LDAP password is not encrypted and entered as plain text.

   Use the following method to generate the encrypted password.

   In a Windows system.

   a. Open a command prompt window and type

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

where *installdir* is the IBM Endpoint Manager for Remote Control server installation directory For example,

```
cd \Program Files\IBM\Tivoli\TRC\server\wlp\usr\servers\trcserver\
apps\TRCAPP.ear\trc.war\WEB-INF\lib
```

b. Type the following command

   `java -cp ./trc.jar com.ibm.uk.greenock.authentication.Encrypt` **<*password*>**

   where *password* is the LDAP password to be encrypted

   For example,

   `java -cp ./trc.jar com.ibm.uk.greenock.authentication.Encrypt myPassw0rd`

   Note: This command is all on one line with a space between **`jar`** and **`com`**.

c. The output from the command is the following

   Encrypted Password : [encrypted password]

   Decrypted Password : [text version of password]

   For example,

   Encrypted Password: 10|ydEBl67atSSbrAA=

   Decrypted Password: myPassw0rd

   Edit the `ldap.properties` file and set the **`ldap.connectionPassword`** property to the encrypted password value. The decrypted password is shown to verify that the encryption is valid.

In a UNIX or Linux system, (see the Windows operating system steps for details of the commands)

a. Open a terminal window and type

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

   where *installdir* is the IBM Endpoint Manager for Remote Control server installation directory

b. Type the following command

   `java -cp ./trc.jar com.ibm.uk.greenock.authentication.Encrypt <password>`

c. The output from the command is the following

   Encrypted Password : [encrypted password]

   Decrypted Password : [text version of password]

ldap.connectionURL

The directory URL used to establish an LDAP connection. Type in here the URL of your LDAP server.

```
ldap://myldapserver.mydomain.mycompany.com
```

Connection Security

The following properties define the level of security to be used on the connection to the LDAP server. Set the following parameter to **simple** so that the IBM Endpoint Manager for Remote Control can communicate with the majority of Active Directory servers.

ldap.security_authentication

Specifies the security level to use. Value can be set to one of the following strings: none, simple, strong. If this property is unspecified, the behavior is determined by the service provider.

```
ldap.security_athentication=simple
```

While most LDAP servers support simple plain text login, some Active Directory administrators require a secure connection. IBM Endpoint Manager for Remote Control supports two types of secure connections to an Active Directory server, **SASL** (Digest-MD5) or **SSL**. If you are having trouble connecting to the Active Directory server and see the following error in the `trc.log`:

```
LDAP Authentication.exception[LDAP: error code 8 - 00002028: LdapErr: DSID-0C09018A,
comment: The server requires binds to turn on integrity checking if SSL\TLS are not
already active on the connection, data 0, vece ]
```

IBM Endpoint Manager for Remote Control will need to be configured for either SASL or SSL connections.

SASL (Simple Authentication and Security Layer)

The following parameters relate to using SASL to secure the connection to the LDAP server. If you are not using SASL these parameters should not be edited and be commented out. The values represented below have been used to configure IBM Endpoint Manager for Remote Control to connect to Active Directory using SASL in a test environment. These may not work in all cases and are shown below for example purposes only. Consult your organizations active directory support team to acquire the correct values for your company.

ldap.security_authentication

Specifies the security level to use. If this property is unspecified, the behavior is determined by the service provider. If using SSL the value is set to simple. If using SASL the value is set to the SASL mechanism DIGEST-MD5

```
ldap.security_authentication= DIGEST-MD5
```

ldap.connectionRealm

The Realm name where the userid and password resides

```
ldap.connectionRealm= mydomain.mycompany.com
```

ldap.connectionQop

This value can be one of:

- **auth** = Authentication only
- **auth-int** = Authentication and integrity checking by using signatures
- **auth-conf** = (SASL only) Authentication, integrity and confidentiality checking by using signatures and encryption.

```
ldap.connectionQop= auth-conf
```

ldap.connectionMaxbuf

Number indicating the size of the largest buffer the server is able to receive when using auth-int or auth-conf. The default is 65536.

```
ldap.connectionMaxbuf= 16384
```

ldap.connectionStrength

Connection strength can be one of: low, medium, high

```
ldap.connectionStrength= high
```

SSL (Secure Socket Layer)

The following parameters define the use of SSL to connect to the Active Directory server. To use SSL you should install a Root CA public key certificate (keystore) on the IBM Endpoint Manager for Remote Control Server. The location of the keystore and its password need to entered in the last two parameters. If SSL is not used these parameters can be commented out in the `ldap.properties` file.

ldap.security_protocol

Specifies the security protocol to use. The value is a string determined by the service provider. For example, ssl. If this property is unspecified, the behavior is determined by the service provider.

```
ldap.security_protocol =ssl
```

ldap.ssl_keyStore

Location of the keystore file

```
ldap.ssl_keyStore=PathOfKeyStoreFile
```

ldap.ssl_keyStorePassword

Location of the keystore password

```
ldap.ssl_keyStorePassword=KeystorePassword
```

Setting user authentication properties

Authenticating the user

Use the following properties to define how the user should be authenticated when they attempt to logon to the IBM Endpoint Manager for Remote Control server. To configure the following sections use the LDAP browser as described for each parameter, to derive the correct settings.

ldap.digest

Digest algorithm used by LDAP. Values are SHA, MD2, or MD5 only. The default is cleartext. If the LDAP servers returns a password, IBM Endpoint Manager for Remote Control uses the Digest algorithm to encrypt the user input password and compare it with the password it receives from the LDAP server. If no password is returned from the LDAP server, IBM Endpoint Manager for Remote Control uses the username and password provided by the end-user to authenticate with LDAP.

```
ldap.digest=SHA
```

ldap.userid

`ldap.userid` is the LDAP attribute which contains the userid that is mapped to the userid field in the IBM Endpoint Manager for Remote Control database. The **`userPrincipalPattern`** property then needs to know whether the *@domainname*, UPN suffix, is added for Active Directory authentication.

sAMAccountName

sAMAaccount should be used so that the userid only portion of the logon, without the UPN Suffix, is used.

userPrincipalName

userPrincipalName should be used to force all logons to use the full User Principal Name

Note: It is recommended to set **`ldap.userid`** to this value as it ensures that it does not contain any invalid characters . For example an apostrophe.

The **ldap.userid** relates to other configuration values in the `ldap.properties` file.

For example, if the ldap.userid is set to userPrincipalName, the user needs to logon to IBM Endpoint Manager for Remote Control with their full id. For example **awilson@example.com**

- The **ldap.userSearch** variable would be (userPrincipalName={0})
- The **ldap.principalPattern** would be {0}

If the ldap.userid is set to use sAMAccountName, the user should logon to IBM Endpoint Manager for Remote Control with just the userid part of their id. For example **awilson**. The parameters below should be set so that the fully qualified name will be appended.

For example

- The **ldap.userSearch** variable would be (userPrincipalName={0}@mydomain.mycompany.com)

  For a user awilson@example.com the ldap.userSearch variable would be (userPrincipalName={0})
- The **ldap.principalPattern** would be {0}@mydomain.mycompany.com

  For a user awilson@example.com the ldap.principalPattern would be {0}@example.com

ldap.userPassword

The name of the LDAP **attribute** in the user's directory entry containing the user's password. In Active Directory, password is the default name of the attribute.

```
ldap.userPassword=password
```

ldap.userEmail

the name of the LDAP attribute in the user's directory entry containing the user's email address.

Note: **ldap.userEmail** cannot have a null value. If your Active Directory Tree does not contain email information a different attribute should be used. For example **ldap.userEmail** could be set to **userPrincipalName**.

ldap.userRealm

Realm name used for end-user authentication. This setting is optional and can be commented out, in the ldap.properties file, for most configurations.

```
ldap.userRealm=users.company.domain.com
```

ldap.principalPattern

Pattern for construction of user principal for using LDAP authentication. Some LDAP servers require email address, for example, **userid@domain.com** and others just require the userid only. The string "{0}" is substituted by the end-users userid entered at the login screen. See **ldap.userid**, above, for the usage in each scenario

Searching for the users directory entry

The method available for finding the end-users information involves defining a starting point in the Active Directory tree and allowing IBM Endpoint Manager for Remote Control to recursively search through the tree for the userid. For most Active Directory implementations this is the preferred method as users are usually spread out in several locations in an Active Directory tree. This method is especially helpful if user information is contained under a single branch of the tree but broken up by department or underneath the branch

Note: It should be noted that when LDAP has been enabled, new users and new user groups should be created in Active Directory and **not** in IBM Endpoint Manager for Remote Control. This is because each time the synchronization with Active Directory takes place the users and user groups are deleted from the IBM Endpoint Manager for Remote Control database and then imported again from Active Directory.

To use the recursive search configure the following parameters:

ldap.userBase

The base LDAP directory entry for looking up users that match the search criteria. If not specified, the search base is the top-level element in the directory context.

```
for example OU=mylocation,DC=mycompany,DC=com
```

You can refine your search by going deeper into the OU structure and selecting to search only within a specific organizational unit for example an OU called Users and therefore you would set the property value as

```
 ldap.userBase=OU=Users,ou=mylocation,dc=mydomain,dc=mycompany,dc=com
```

This would instruct IBM Endpoint Manager for Remote Control to look for users matching the criteria, only within the Users OU (and any OUs that belong to the Users OU if ldap.groupSubtree is set to true)

ldap.userSearch

Defines the LDAP query that is used to import Active Directory users to IBM Endpoint Manager for Remote Control. The defined query needs to filter the results such that only those users which match the search criteria are imported to IBM Endpoint Manager for Remote Control. The default value is

(objectClass=user)

which means, look for users in any object that is a user object within the userbase. That is import all Active Directory users to IBM Endpoint Manager for Remote Control.

Note: When using the above it should be noted that some environments can have thousands of users therefore it is important to create a filter which will only import the required users. To limit the users that are imported to only those users who match the search criteria and are members of the groups that were imported into IBM Endpoint Manager for Remote Control through the **`ldap.groupSearch`** filter, you should set the property **`ldap.userInGroup`** to true. It should also be noted that as well as being imported into the relevant groups that are returned in the group search, users are also imported into the **DefaultGroup**. Setting **`ldap.userInGroup`** to false will import all users who match the search criteria, regardless of their group membership.

The search can therefore be further refined by using more complex queries. For example if you have the following values set

```
ldap.groupBase=(OU=mylocation.DC=mycompany.DC=com)
Ldap.userSearch: (&(objectClass=user)(|(memberOf=CN=Department1,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com) (memberOf=CN=Department3,OU=GROUPS,
OU=mylocation,DC=mycompany,DC=com))(name={0}))
```

If there were three groups defined, Department1, Department2 and Department3 the above query would authenticate and import any users that are defined as objectclass user and are members of the Department1 OR Department3 groups. Users from Department2 would not be able to logon to IBM Endpoint Manager for Remote Control.

The (&(name={0}) is added to the end to specify that the name attribute is used for logging in. This value has to match whatever attribute was specified as ldap.userid.

ldap.userSubtree
Set this value to true if you want to recursively search the sub tree of the element specified by the userBase attribute for the user's directory entry. The default value of false causes only the top level to be searched (a nonrecursive search). This is ignored if you are using the userPattern expression.

```
ldap.userSubtree=true
```

Importing Active Directory Groups

One of the greatest benefits of integrating with Active Directory is being able to use existing Active Directory groups. After Active Directory groups are imported, an administrator only has to define the permissions for each group and group membership is handled inherently by Active Directory. To import Active Directory groups configure the following properties in the `ldap.properties` file.

ldap.groupName
the ldap **attribute** name that is used to perform a group search.

```
ldap.groupName=cn    OR   ldap.groupName=name
```

ldap.groupDescription
the ldap attribute name to be used to get the description for this group. This is set to **description** by default.

```
ldap.groupDescription=description
```

ldap.groupNameTrim
Set to true or false. Limits the group name which is imported to the IBM Endpoint Manager for Remote Control database to 64 characters. The recommended value is **false**.

ldap.groupMembers
ldap **attribute** name to be used to find the members of the groups that are returned as a result of the specified search. The default value is **member**

```
ldapgroupMembers=member
```

ldap.groupSubtree
If set to true, IBM Endpoint Manager for Remote Control will search recursively through the subtree of the element specified in the **ldap.groupBase** parameter for groups associated with a user. If left unspecified, the default value of false causes only the top level to be searched, and no recursive search is performed. True or False (default).

ldap.groupBase
The base LDAP directory entry for starting the search for groups to synchronize. If left unspecified, the default is to use the top-level element in the directory context.

`for example` **`OU=mylocation,DC=mycompany,DC=com`**

To refine your search and go deeper into the OU structure, select to start the search only within a specific organizational unit, for example, an OU called Test. To refine this search set the property value as

`OU=Test,OU=mylocation,DC=mycompany,DC=com`

This would instruct IBM Endpoint Manager for Remote Control to look for groups matching the criteria, only within the Test OU (and any OUs that belong to the Test OU if **`ldap.groupSubtree`** is set to true)

ldap.groupSearch
Defines the LDAP query that is used to import AD groups to IBM Endpoint Manager for Remote Control. The defined query needs to filter the results such that only those groups which are needed are imported to IBM Endpoint Manager for Remote Control.

ldap.groupSearch=(objectClass=group)
Imports all AD groups found in the OU specified in the **`ldap.groupBase`** property to IBM Endpoint Manager for Remote Control. Be aware some environment can have thousands of groups.

ldap.groupSearch=(&(objectClass=group)(cn=*SMS*))
Imports all groups that contain SMS in the cn attribute, for example visio-sms-users

ldap.groupSearch=(&(objectClass=group)(cn=admins))
Imports all groups that are named admins.

ldap.groupSearch=(&(objectClass=group)(cn=admins*))
Imports all groups which have admins in the name for example administrators, server-administrators.

ldap.groupMembers
ldap **attribute** name to be used to find the members of the groups that are returned as a result of the specified search. The default value is **member**.

These queries can be tested using the LDAP browsers directory search option or the LDAP configuration utility.

Testing the Connection

When the `common.properties` & `ldap.properties` files have been updated, reset the IBM Endpoint Manager for Remote Control application by selecting **Admin** > **Reset Application**.

When the service has restarted logon to the IBM Endpoint Manager for Remote Control server using an Active Directory userid and password. If the entries in the LDAP properties file are correct you are authenticated and logged on successfully.

IBM Endpoint Manager for Remote Control Server connects directly to LDAP therefore, any password changes within LDAP are immediately effective as long as the LDAP password change has synchronized to the LDAP server which is set within the ldap.properties file.

Note: The default ADMIN userid within the IBM Endpoint Manager for Remote Control Server application will always authenticate against the IBM Endpoint Manager for Remote Control Server database regardless of whether LDAP authentication is enabled. This is to allow a mechanism for accessing the application, should there be a connectivity problem between IBM Endpoint Manager for Remote Control Server and LDAP.

If there are any errors in the `ldap.properties` file you will see a message that the login has failed. The Logon screen is displayed with an Invalid username or wrong password message.

To determine the cause of the failure look in the `trc.log` file. View the application log using the Admin menu by completing the following steps.

- In the IBM Endpoint Manager for Remote Control Server UI, click **Admin** > **View application log**
- Click **CTRL+END** to reach the end of the file.

Some common errors are listed below. Please note that the presence of these errors indicates that there was a problem creating the initial connection between IBM Endpoint Manager for Remote Control Server and Active Directory.

AcceptSecurityContext error, data 525
Returns when username is invalid

AcceptSecurityContext error, data 52e
Returns when username is valid but password or credentials are invalid. Will prevent most other errors from being displayed as noted.

AcceptSecurityContext error, data 530
Logon failure: account logon time restriction violation. Displays only when presented with valid username and password credential.

AcceptSecurityContext error, data 531
Logon failure user not allowed to log on to this computer. Displays only when presented with valid username and password credential

AcceptSecurityContext error, data 532
Logon failure: the specified account password has expired. Displays only when presented with valid username and password credential.

AcceptSecurityContext error, data 533
Logon failure account currently disabled. Displays only when presented with valid username and password credential.

AcceptSecurityContext error, data 701
The user's account has expired. Displays only when presented with valid username and password credential.

AcceptSecurityContext error, data 773
The user's password must be changed before logging on the first time. Displays only when presented with valid username and password credential.

AcceptSecurityContext error, data 775
The referenced account is currently locked out and may not be logged on to. Displays even if invalid password is presented.

LDAP Authentication.exceptionmyserver.mydomain.com:389
Displays when the server name specified by **`ldap.connectionURL`** is unreachable.

Verifying that groups have been imported

When authentication is successful and you are logged on to the IBM Endpoint Manager for Remote Control server, click **User groups** > **All User Groups** to verify that the correct groups have been imported from Active Directory.

After the groups have been imported into IBM Endpoint Manager for Remote Control, define permissions for the newly imported groups.

Sample LDAP Configuration File

The file is a sample configuration file. It uses a simple connection to Active Directory with importing of Active Directory groups

```
# Licensed Materials - Property of IBM Corporation

# 5724-N88 5725-C431

# (C) Copyright IBM Corp. 2004, 2014

# All Rights Reserved

# US Government Users Restricted Rights - Use, duplication or

# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

# LDAP Properties

# Server Authentication definition

# The directory URL used to establish an LDAP connection

ldap.connectionURL=ldap://myldapserver

# define the secondary LDAP server name, if the primary is down we can use an alternative LDAP server

#–ldap.alternateURL=

# The username used to authenticate a read-only LDAP connection. If left not set, an anonymous connection is made.

ldap.connectionName=administrator@mydomain.MyCompany.com

# The password used to establish a read-only LDAP connection.

ldap.connectionPassword=myPassword

# Instructs Remote Control to read the value of the password parameter as encrypted ( true) or plain text ( false). See Admin guide for instructions on generating encrypted password

ldap.connectionPasswordEncrypted=false

# The fully qualified Java class name of the JNDI context factory to be used for

# this connection. If left unset, the default JNDI LDAP provider class is used.

# --- -ldap.contextFactory=com.sun.jndi.ldap.LdapCtxFactory

# ##################### SASL Definition
##########################################
```

```
# specifying the security level to use. Its value is one of the following strings:
"simple" or "DIGEST-MD5".

# . If using SSL, you have to use simple.

ldap.security_authentication=simple

#Identifies the realm or domain from which the connection name should be chosen

# ---- ldap.connectionRealm=

#Quality of protection

# QOP can be one of: auth, auth-int, auth-conf

# auth -- Authentication only

# auth-int --Authentication and integrity checking by using signatures

# auth-conf -- (SASL only) Authentication, integrity and confidentiality checking

# by using signatures and encryption.

# ----ldap.connectionQop=auth

# Number indicating the size of the largest buffer the server is able to receive
when

# using "auth-int" or "auth-conf". The default is 65536.

# ldap.connectionMaxbuf=16384

# Strength can be one of: low,medium,high

# ----ldap.connectionStrength=high

# ########################### SSL Definition
############################################

# specifying the security protocol to use. Its value is a string determined by

# the service provider (for example: "ssl"). If this property is unspecified, the
behaviour

# is determined by the service provider.

# ----ldap.security_protocol=ssl

# Access the keystore, this is where the Root CA public key cert was installed

# No need to specify the keystore password for read operations

# ----ldap.ssl_keyStore=PathOfKeyStoreFile

# ----ldap.ssl_keyStorePassword=KeystorePassword
# specifying how referrals encountered by the service provider are to be processed.

# The value of the property is one of the following strings:

# "follow" -- follow referrals automatically

# "ignore" -- ignore referrals

# "throw" -- throw ReferralException when a referral is encountered.

# If this property is not specified, the default is determined by the provider.

# ----ldap.referrals=follow

# ########################## define Group search for LDAP
########################

# The base LDAP directory entry for looking up group information. If left
unspecified,

# the default is to use the top-level element in the directory context.

ldap.groupBase=OU=Groups,OU=mylocation,DC=mydomain,DC=mycompany,

DC=com

#The LDAP filter expression used for performing group searches.

ldap.groupSearch=(&(objectClass=group) (name=TRC*))

# Set to true if you want to recursively search the subtree of the element specified
in

# the groupBase attribute for groups associated with a user. If left unspecified, the
default

# value of false causes only the top level to be searched (a nonrecursive search).

ldap.groupSubtree=true

#The LDAP attribute that we should use for group names.

ldap.groupName=name

#The LDAP attribute that we should use for group descriptions

ldap.groupDescription=description

# This is the attribute specifying user members within a group

ldap.groupMembers=member

# ########################## User search definition ########################

#The base of the subtree containing users
```

```
#If not specified, the search base is the top-level context.

ldap.userBase=OU=Users,OU=mylocation,DC=mydomain,DC=mycompany,DC=com

# The LDAP filter expression to use when searching for a user's directory entry, with {0} marking

# where the actual username is inserted.

ldap.userSearch=(&(objectClass=User)(sAMAccountName={0}))

# Set this value to true if you want to recursively search the subtree of the element specified by

# the userBase attribute for the user's directory entry. The default value of false causes only the

# top level to be searched (a nonrecursive search).

ldap.userSubtree=true

#Set this value to true if a user has to be a member of the groups found in the group search

ldap.userInGroup=true

# Digest algorithm (SHA, MD2, or MD5 only)

# Remote control will use it to encrypt the user input password and

# compare it with password it receives from the LDAP server. If left unspecified, the default value is "cleartext".

# ---- ldap.digest=SHA

#LDAP attribute used for userids

ldap.userid=sAMAccountname

# LDAP User password attribute

ldap.userPassword=password

# LDAP Attribute containing the Users Email address

ldap.userEmail=userPrincipalName

# If the following parameters are defined they is mapped into the local remote control database

ldap.forename=givenName

ldap.surname=sn

ldap.title=title
ldap.initials=initialsg

ldap.company=company

ldap.department=department

ldap.telephone=telephoneNumber

ldap.mobile=mobile

ldap.state=st

ldap.country=Co

#### Other property definitions

#Set this value to the page size of LDAP search retrievals (default=500).

# Do not set this to anything greater than the max page size for the LDAP server (
for example, AD has a limit of 1000)
```

```
ldap.page.size=500
```

Chapter 8. Federal Information Processing Standard (FIPS 140-2) compliance in IBM Endpoint Manager for Remote Control

The US Federal Information Processing Standard 140-2 (FIPS 140-2) is a cryptographic function validation program that defines security standards for cryptographic modules that are used in IT software. In FIPS 140-2 mode, IBM Endpoint Manager for Remote Control uses the FIPS 140-2 approved cryptographic providers; IBMJCEFIPS (certificate #1081), IBMJSSEFIPS (certificate 409), and OpenSSL FIPS Object Module (certificate #1747). The certificate for IBMJCEFIPS (certificate #1081) is held on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2009.htm#1081. The certificate for IBMJSSEFIPS (certificate 409) is held on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2004.htm#409. The certificate for OpenSSL FIPS Object Module (certificate #1747) is held on the NIST website at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2012.htm#1747. To enable FIPS for IBM Endpoint Manager for Remote Control you must configure all components, the server, controller, and target.

IBM Endpoint Manager for Remote Control version 9.x.x uses:

IBM Java JCE FIPS 140-2 Cryptographic Module version 1.3.1 Tested as meeting Level 1 with Windows XP Professional SP2 operating system using IBM JVM 1.6 (single-user mode) FIPS-approved algorithms:

- AES (Cert. #805);
- DSA (Cert. #297);
- HMAC (Cert. #445);
- RNG (Cert. #463);
- RSA (Cert. #387);
- SHS (Cert. #803);
- Triple-DES (Cert. #687).

IBM Java JSSE FIPS 140-2 Cryptographic Module version 1.1 Tested as meeting Level 1 with

- Windows 2000 Professional SP3 operating system (JVM 1.3.1_03 and JVM 1.4.1_04), Windows 2000 Advanced Server SP4 operating system (JVM 1.4.1)
- Sun Solaris 5.8 (JVM 1.3.1 and 1.4.1)
- AIX 5.2 (JVM 1.3.1 and 1.4.1)
- SuSE Linux Enterprise Server 8 (JVM 1.4.1_05)
- Red Hat Linux Advanced Server 2.1(JVM 1.4.1_05)
- IBM OS/400® V5R2M0 (JVM 1.4.1)
- z/OSV1R4 (JVM 1.4.1)

FIPS-approved algorithms:

- SHA-1 (Cert. #148);
- Triple-DES (Cert. #163);
- AES (Cert. #53);
- DSA (Cert. #83);

- RSA (PKCS#1, vendor affirmed);
- HMAC-SHA-1 (Cert. #148, vendor affirmed);

OpenSSL FIPS Object Module version 2.0.2 Tested as meeting Level 1 with

- Android 2.2 (gcc Compiler Version 4.4.0); Android 2.2 running on Qualcom QSD8250 (ARMv7) with NEON (gcc Compiler Version 4.4.0); Android 2.2 running on OMAP 3530 (ARMv7) with NEON (gcc Compiler Version 4.1.0); Android 3.0 (gcc Compiler Version 4.4.0); Android 4.0 (gcc Compiler Version 4.4.3); Android 4.0 running on TI OMAP 3 (ARMv7) with NEON (gcc Compiler Version 4.4.3); Android 4.1 running on TI DM3730 (ARMv7) (gcc Compiler Version 4.6); Android 4.1 running on TI DM3730 (ARMv7) with NEON (gcc Complier Version 4.6); Android 4.2 running on Nvidia Tegra 3 (ARMv7) (gcc Compiler Version 4.6); Android 4.2 running on Nvidia Tegra 3 (ARMv7) with Neon (gcc Compiler Version 4.6) (single-user mode).
- Microsoft Windows 7 (32 bit) (Microsoft 32 bit C/C++ Optimizing Compiler Version 16.00); Microsoft Windows 7 (64 bit) (Microsoft C/C++ Optimizing Compiler Version 16.00); Microsoft Windows 7 running on Intel Core i5-2430M (64-bit) with AES-NI (Microsoft ® C/C++ Optimizing Compiler Version 16.00 for x64);
- Microsoft Windows 2008 running on Intel Xeon E3-1220v2 (32-bit under vSphere) (Microsoft 32-bit C/C++ Optimizing Compiler Version 16.00 for 80x86); Microsoft Windows 2008 running on Intel Xeon E3-1220v2 (64-bit under vSphere) (Microsoft C/C++ Optimizing Compiler Version 16.00 for x64);
- uCLinux 0.9.29 (gcc Compiler Version 4.2.1);
- Fedora 14 running on Intel Core i5 with AES-NI (gcc Compiler Version 4.5.1);
- HP-UX 11i (32 bit) (HP C/aC++ B3910B); HP-UX 11i (64 bit) (HP C/aC++ B3910B);
- Ubuntu 10.04 (32 bit) (gcc Compiler Version 4.1.3); Ubuntu 10.04 (64 bit) (gcc Compiler Version 4.1.3); Ubuntu 10.04 running on Intel Core i5 with AES-NI (32 bit) (gcc Compiler Version 4.1.3);
- Linux 2.6 (gcc Compiler Version 4.3.2); Linux 2.6.27 (gcc Compiler Version 4.2.4); Linux 2.6.32 (gcc Compiler Version 4.3.2); Linux 2.6.33 (gcc Compiler Version 4.1.0); Linux 2.6 (gcc Compiler Version 4.1.0);
- VxWorks 6.8 (gcc Compiler Version 4.1.2);
- Oracle Solaris 10 (32 bit) (gcc Compiler Version 3.4.3); Oracle Solaris 10 (64 bit) (gcc Compiler Version 3.4.3); Oracle Solaris 11(32 bit) (gcc Compiler Version 4.5.2); Oracle Solaris 11 (64 bit) (gcc Compiler Version 4.5.2); Oracle Solaris 11 running on Intel Xeon 5675 with AES-NI (32 bit) (gcc Compiler Version 4.5.2); Oracle Solaris 11 running on Intel Xeon 5675 with AES-NI (64 bit) (gcc Compiler Version 4.5.2); Oracle Solaris 11 (32 bit) (Sun C Version 5.12); Oracle Solaris 11 (64 bit) (Sun C Version 5.12);
- Oracle Linux 5 (64 bit) (gcc Compiler Version 4.1.2); Oracle Linux 5 running on Intel Xeon 5675 with AES-NI (gcc Compiler Version 4.1.2); Oracle Linux 6 (gcc Compiler Version 4.4.6); Oracle Linux 6 running on Intel Xeon 5675 with AES-NI (gcc Compiler Version 4.4.6);
- CascadeOS 6.1 (32 bit) (gcc Compiler Version 4.4.5); CascadeOS 6.1 (64 bit) (gcc Compiler Version 4.4.5);
- Apple iOS 5.1 (gcc Compiler Version 4.2.1);
- Microsoft Windows CE 6.0 (Microsoft C/C++ Optimizing Compiler Version 15.00 for ARM); Microsoft Windows CE 5.0 (Microsoft C/C++ Optimizing Compiler Version 13.10 for ARM);
- DSP Media Framework 1.4 (TMS320C6x C/C++ Compiler v6.0.13);

- NetBSD 5.1 (gcc Compiler Version 4.1.3);
- RHEL 6 running on Intel Xeon E3-1220v2 (32-bit under vSphere) (gcc Compiler Version 4.4.6); RHEL 6 running on Intel Xeon E3-1220v2 (64-bit under vSphere) (gcc Complier Version 4.4.6);

FIPS-approved algorithms:

- AES (Certs. #1884, #2116, and #2234);
- DRBG (Certs. #157, #229, and #264);
- DSA (Certs. #589, #661, and #693);
- HMAC (Certs. #1126, #1288, and #1363);
- RNG (Certs. #985, #1087, and #1119);
- RSA (Certs. #960, #1086, and #1145);
- SHS (Certs. #1655, #1840, and #1923);
- Triple-DES (Certs. #1223, #1346, and #1398);
- ECDSA (Certs. #264, #270, #315, #347 and #378);
- CVL (Certs. #10, #12, #24, #36 and #49).

Enabling FIPS compliance on the server

Enabling FIPS compliancy on a server installation with a stand-alone Websphere Application Server

The IBM Endpoint Manager for Remote Control Server uses the middleware infrastructure provided by WebSphere secure HTTP communications, therefore enabling FIPS for a manual IBM Endpoint Manager for Remote Control Server installation requires configuring WebSphere for FIPS compliant mode as well as configuring the IBM Endpoint Manager for Remote Control Server through a setting in the `common.properties` configuration file.

To enable FIPS compliance for a manual installation complete the following steps :

1. Configure Websphere

   The WebSphere documentation describes how to enable FIPS mode in WebSphere for:

   - WebSphere Application Server :
     - **v7.0** : http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tsec_fips.html
     - **v8.5**http://pic.dhe.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/tsec_fips.html
   - WebSphere Application Server Network Deployment:
     - **v7.0** : http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/rovr_fips.html
     - **v8.5** : http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp?topic=%2Fcom.ibm.websphere.nd.doc%2Fae%2Ftsec_fips.html
   - WebSphere Application Server - Express®:
     - **v7.0** :http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.express.doc/info/exp/ae/tsec_fips.html
     - **v8.5** :http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/index.jsp?topic=%2Fcom.ibm.websphere.express.doc%2Fae%2Ftsec_fips.html

Note: It should be noted that running in FIPS mode in IBM WebSphere with the IBM JRE and the IBM JSSE provider currently does not work when using an MS SQL database. These options will work with MS SQL when FIPS is **not** enabled in IBM Websphere.

2. Log on to the IBM Endpoint Manager for Remote Control Server with a valid admin id and password.
3. Click **Admin** > **Edit properties files**
4. In the `common.properties` file set **`FIPS.compliance`** to true.
5. Click **Submit**.
6. Click **Admin** > **Reset Application**.

Note: It should be noted that the FIPS enablement changes in Websphere would affect all other applications running on that server so browser settings for the users accessing those other applications should be changed to support Transport Layer Security (TLS), if required by their browser version.

For example to enable TLS in Internet Explorer complete the following steps :

- Click **Tools** > **Internet Options**.
- On the **Advanced** tab select **Use TLS 1.0**.
- Click **Apply**
- Click **OK**.

Enabling FIPS compliance on an automated server installation

To enable FIPS compliance on an automated IBM Endpoint Manager for Remote Control Server installation complete the following steps:

1. Edit the java.security file found at the following location

   Windows systems

   %TRC_SERVER_PATH%`\java\jre\lib\security\java.security`

   where *%TRC_SERVER_PATH%* is the path for the installation directory for the IBM Endpoint Manager for Remote Control Server.

   Linux / UNIX systems

   $TRC_SERVER_PATH`/java/jre/lib/security/java.security`

   where *$TRC_SERVER_PATH* is the path for the installation directory for the IBM Endpoint Manager for Remote Control Server.

2. Modify the *security.provider.x=* list so the following entry is the first one in the list:

   security.provider.1=com.ibm.crypto.FIPS.provider.IBMJCEFIPS

   Fix the number sequence of the other items in this list so that all items are numbered in sequence. For example, the full list after these changes is:

```
security.provider.1=com.ibm.crypto.FIPS.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.10=com.ibm.security.sasl.IBMSASL
security.provider.11=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.12=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.13=org.apache.harmony.security.provider.PolicyProvider
```

3. Save the file.
4. Log on to the IBM Endpoint Manager for Remote Control Server with a valid admin id and password.
5. Click **Admin** > **Edit properties files**
6. In the `common.properties` file set **`FIPS.compliance`** to true.
7. Click **Submit**.
8. Click **Admin** > **Reset Application**. Restart the server service.

Check to see if the IBM Endpoint Manager for Remote Control Server is configured for FIPS by completing the following step

- Click **Admin** > **View Current Server Status**.

The fields showing FIPS compliancy enablement are

- Enabled FIPS mode: - The value of this is determined by the **`FIPS.compliance`** property in the `common.properties` file.
- JVM configured for FIPS: - The value of this is determined by the configuration of the JVM and the security providers listed in the `java.security` file.

Enabling FIPS compliance on the controller

The IBM Endpoint Manager for Remote Control controller is a Java application that requires a FIPS certified cryptographic provider when FIPS compliance is enabled. Only the IBM Java Runtime Environment (JRE) is supported in FIPS-compliant mode.

The IBM JRE for Windows operating system and Linux (Intel) operating systems is included with IBM Endpoint Manager for Remote Control and is installed when you install the controller software.

If you are using Windows operating system , the JRE is included in the controller package `trc_controller_setup.exe` and `trc_controller.msi`. For Linux operating system, the JRE is included in the package `ibm-trc-controller-jre-`*`9.x.x`*`.i386.rpm`. Where *9.x.x* is the version that you want to install. For example, 9.1.0. These packages install the IBM Java Runtime Environment pre-configured with the IBM FIPS certified cryptographic provider. They also register the MIME type `application/x-ibm-trc-jws` and a file association for `*.trcjws` files. The file types are used by the IBM Endpoint Manager for Remote Control server in FIPS-compliant mode to start the controller. For more information about installation instructions for the controller, see “Installing the controller” on page 59.

To use a different installation of the IBM JRE, the IBM Endpoint Manager for Remote Control controller uses the FIPS-compliant cryptography module that is included with the IBM Java virtual machine. To enable FIPS mode, the settings of the JVM (Java virtual machine) that are used to run the controller need to be modified. When you enable FIPS compliance, any other Java applications that are running on the default JVM can also use the FIPS provider and the other security providers that are listed in the `java.security` file.

Note: Enabling FIPS on the controller is not supported if you are using an Oracle JVM.

To enable FIPS compliance on the controller if you are not using the version of IBM JRE supplied with IBM Endpoint Manager for Remote Control, complete the following steps:

1. Edit the `java.security` file

   Windows systems
   : `%JRE_HOME%\lib\security\java.security`

     Where *%JRE_HOME%* is the path to the directory where the Java virtual machines Java Runtime Environment (JRE) is installed.

   Linux / UNIX systems
   : `$JRE_HOME/lib/security/java.security`

     Where *$JRE_HOME* is the path to the directory where the Java virtual machines Java Runtime Environment (JRE) is installed.

2. Modify the **`security.provider.x= list`** so that the following two entries are the first ones in the list:

   ```
   security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPS
   security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
   ```

   Fix the number sequence of the other items in this list so that all items are numbered in sequence. For example,

   ```
   security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPS
   security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
   security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
   security.provider.4=com.ibm.crypto.provider.IBMJCE
   security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
   security.provider.6=com.ibm.security.cert.IBMCertPath
   security.provider.7=com.ibm.security.sasl.IBMSASL
   security.provider.8=com.ibm.xml.crypto.IBMXMLCryptoProvider
   security.provider.9=com.ibm.xml.enc.IBMXMLEncProvider
   security.provider.10=org.apache.harmony.security.provider.PolicyProvider
   security.provider.11=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
   ```

   Note:

   a. Applies to all supported versions of the IBM JVM.
   b. You must make a file association for the `*.trcjws` files before you start the first session with a target. Use the following commands

      Windows systems
      : `%JRE_HOME%\jre\bin\javaws`

        Where *%JRE_HOME%* is the path to the directory where the Java virtual machines Java Runtime Environment (JRE) is installed.

      Linux / UNIX systems
      : `$JRE_HOME/jre/bin/javaws.exe`

        Where *$JRE_HOME* is the path to the directory where the Java virtual machines Java Runtime Environment (JRE) is installed.

Check to see whether the controller is configured for FIPS by completing the following step during a remote control session.

- Click **Controller tools** > **Show session information** in the controller window.

Edit the `trc_controller.cfg` file on the system that the controller is installed on.

Note: Only required if you are running the controller locally for establishing peer to peer sessions. For details of installing the controller to your local system, see "Installing the controller" on page 59.

Windows systems

[controller install dir]\trc_controller.cfg

Where *[controller install dir]* is the installation directory that is chosen when you install the controller.

Linux systems

`opt/ibm/trc/controller/trc_controller.cfg`

Set the **`fips.compliance`** property to true and save the file.

Enabling FIPS compliance on the target

The IBM Endpoint Manager for Remote Control target ships with FIPS-capable OpenSSL libraries. You can enable FIPS compliance at installation time or by editing the target registry on a Windows system or by changing the configuration file on a Linux system.

For more information about installing the target, see the IBM Endpoint Manager for Remote Control Installation Guide.

Using the target user interface, choose the appropriate option to verify that the target is in FIPS mode.

- On the IBM Endpoint Manager for Remote Control- Target user interface, click **Actions Menu** > **Connection info**
- Hover the mouse over the IBM Endpoint Manager for Remote Control icon in the system notification area.

Enabling FIPS compliance on a Windows target

On a Windows system, you can enable FIPS compliance on the target in two ways; during installation or by editing the target registry after installation.

Enabling FIPS compliance by using the target installer

Enable the FIPS compliance target property during installation by completing the following steps:

1. On the **Server Address** panel of the target installer, click **Advanced settings**.
2. Select **Use a FIPS certified cryptographic provider** and **Use secure connections (https)**. Continue with the rest of the target installation.

Performing a silent installation

When performing a silent target installation, run the installation command and use the **`FIPSCOMPLIANCE`** property to enable FIPS on the target . For more details of performing a silent installation, see "Performing a target custom installation on a Windows system" on page 52.

Use the following properties when enabling FIPS mode

- TRC_SERVER_PROTOCOL=https
- TRC_SERVER_PORT=443
- FIPSCOMPLIANCE=yes

For example : **trc_target_setup.exe /s /v"/qn TRC_SERVER_HOSTNAME=yourserver TRC_SERVER_PROTOCOL=https TRC_SERVER_PORT=443 FIPSCOMPLIANCE=yes"**

where ***yourserver*** is the hostname or IP address of your IBM Endpoint Manager for Remote Control Server.

Enabling FIPS compliance after target installation

After you install the IBM Endpoint Manager for Remote Control target, you can enable FIPS compliance by editing the target registry. To enable FIPS compliance, complete the following steps.

1. Run the **regedit** command at a command prompt window.
2. In the Windows registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Tivoli\Remote Control\Target`
3. Right-click **FIPSCompliance** and select **Modify**.
4. Type `yes` in the **Value data** field and click **OK**.
5. Restart the target service. For more information about restarting the target service, see Chapter 6, "Managing the component services," on page 71. Follow the steps in the section that is relevant to your operating system.

Enabling FIPS compliance in Linux or UNIX based operating systems

After you install the IBM Endpoint Manager for Remote Control target you can enable FIPS compliance by editing the `ibmtrct.conf` file. To enable FIPS compliance, complete the following steps:

1. Edit the `/etc/ibmtrct.conf` file.
2. Set the value of *FIPSCompliance* to yes and save the file.
3. Restart the target service. For more information about restarting the target service, see Chapter 6, "Managing the component services," on page 71. Follow the steps in the section that is relevant to your operating system.

Enabling FIPS compliance on the gateway

You can enable FIPS compliance on the gateway component by editing the gateway configuration file that is created when you install gateway support.

The `trc_gateway.properties` file is in the following directory.

Windows systems

`\Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control\Gateway` for Windows 2000, Windows XP, and Windows 2003 operating systems.

`\ProgramData\IBM\Tivoli\Remote Control\Gateway` for Windows Vista operating system and later.

Linux systems

`/etc`

To enable FIPS compliance, complete the following steps.

1. Edit the `trc_gateway.properties` file.
2. Set **FIPSCompliance = Yes**.
3. Save the file.

4. Restart the gateway service. For more information about restarting the gateway service, see Chapter 6, “Managing the component services,” on page 71. Follow the steps in the section that is relevant to your operating system.

Enabling FIPS compliance on the broker

You can enable FIPS compliance on the broker component by editing the broker configuration file that is created when you install broker support.

The `trc_broker.properties` file is in the following directory.

Windows systems

`\Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control\broker` for Windows 2000, Windows XP, and Windows 2003 operating systems.

`\ProgramData\IBM\Tivoli\Remote Control\broker` for Windows Vista operating system and later.

Linux systems

`/etc`

To enable FIPS compliance, complete the following steps.

1. Edit the `trc_broker.properties` file.
2. Set **`FIPSCompliance = Yes`**.
3. Save the file.
4. Restart the broker service. For more information about restarting the broker service, see Chapter 6, “Managing the component services,” on page 71. Follow the steps in the section that is relevant to your operating system.

Chapter 9. NIST SP800-131A compliance in IBM Endpoint Manager for Remote Control

IBM Endpoint Manager for Remote Control version 9.1.0 components can be configured for NIST SP800-131A compliance.

The National Institute of Standards and Technology (NIST) Special Publications (SP) 800-131A standard strengthens algorithms and increases the cryptographic key lengths to improve security.

The following prerequisites are required:

- Ensure that all keys have at least a key security strength greater than or equal to 112 bits. RSA keys must be at least 2048 bits.
- Ensure that all certificates are created with the new key strengths. Any RSA certificates that use keys shorter than 2048 bits must be replaced with a certificate that uses 2048-bit keys or higher.
- Ensure that all certificates are signed by an allowed signature algorithm of minimum SHA-2.

When you enable NIST SP800-131A compliance, the TLSv1.2 protocol is used for providing secure connections. Therefore, you must ensure that your browser is compatible.

Table 13. Browser compatibility for TLSv1.2. The following table provides information about the supported browser versions that are compatible with TLSv1.2.

	TLSv1.2 not supported	**TLSv1.2 supported but disabled but default**	**TLSv1.2 supported and enabled by default**
Internet Explorer	All versions of IE on Windows XP and Windows Vista operating systems, (IE6, IE7, IE8, IE9)	IE8, IE9, IE10 on Windows 7 and Windows 8 operating system..	IE11 on Windows 7 operating system and later
Firefox	<24	24	None

Compliance with NIST SP800-131A also requires that the cryptographic provider is FIPS 140-2 certified. When SP800-131A compliance is enabled, FIPS 140-2 compliance is enabled automatically, even when it is disabled in the settings.

For NIST SP800-131A compliance, you must configure all your components. There is no compatibility with earlier versions of the components.

Note: There is no support for NIST SP800-131A with Oracle JVMs. Therefore, to take advantage of the NIST support, you must install the stand-alone controller component.

Enabling NIST SP800-131A compliance on the server

You can enable NIST SP800-131A compliance on the IBM Endpoint Manager for Remote Control server during installation, when you are using the server installer program. You can also enable NIST compliance after installation. To enable NIST SP800-131A compliance for a manual IBM Endpoint Manager for Remote Control Server installation you must configure theIBM Endpoint Manager for Remote Control Server and WebSphere.

Enabling NIST SP800-131A compliance during the server installation

To enable NIST SP800-131A compliance during installation, follow the instructions in "Installing by using the server installer" on page 25. Select **Enable NIST SP800-131A compliance (Enables FIPS)** on the Web server parameters panel during the installation.

Enabling NIST SP800-131A compliance on a server with a stand-alone WebSphere Application Server

The IBM Endpoint Manager for Remote Control Server uses the middleware infrastructure that is provided by WebSphere secure HTTP communications. Therefore, to enable NIST SP800-131A compliance for a manual IBM Endpoint Manager for Remote Control Server installation you must configure IBM Endpoint Manager for Remote Control Server and WebSphere.

To enable NIST SP800-131A compliance for a manual server installation, complete the following steps after you install the server.

1. Configure WebSphere

   The WebSphere documentation describes how to enable NIST SP800-131A in WebSphere. Follow the instructions relevant to your version of WebSphere.

   - WebSphere Application Server:
     - **v7.0:** http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_config_strictsp300.html
     - **v8.5:**http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.base.iseries.doc/ae/tsec_config_strictsp300.html
   - WebSphere Application Server Network Deployment:
     - **v7.0:** http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.doc/info/ae/ae/tsec_config_strictsp300.html
     - **v8.5:** http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.nd.doc/ae/tsec_config_strictsp300.html
   - WebSphere Application Server - Express:
     - **v7.0:**http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.express.doc/info/exp/ae/tsec_config_strictsp300.html
     - **v8.5:**http://pic.dhe.ibm.com/infocenter/wasinfo/v8r5/topic/com.ibm.websphere.express.iseries.doc/ae/tsec_config_strictsp300.html
2. Log on to the IBM Endpoint Manager for Remote Control Server with a valid admin id and password.
3. Click **Admin** > **Edit properties files**
4. In the `common.properties` file set **`sp800131a.compliance`** to true.
5. Click **Submit**.
6. Click **Admin** > **Reset Application**.

7. Restart the server service. For more information about restarting the server service see, Chapter 6, “Managing the component services,” on page 71. Follow the steps in the section that is relevant to your operating system.

Note: NIST SP800-131A enablement changes in WebSphere would affect all other applications that are running on that server. Therefore, browser settings for the users who access those other applications must be changed to support Transport Layer Security (TLS).

To enable TLS in Internet Explorer, complete the following steps.
- Click **Tools** > **Internet Options**.
- On the **Advanced** tab select **Use TLS 1.2**.
- Click **Apply**
- Click **OK**.

To enable TLS in Firefox, complete the following steps.
- In the browser, go to the **about:config** page.
- Click **I'll be careful, I promise**.
- In the search field search for **`security.tls.version.max`**.
- Set the value to 3.

Enabling NIST SP800-131A compliance after you install the server

After you install the server by using the installer program, you can enable NIST SP800-131A compliance in a number of ways.

However, if you did not already enable FIPS you must enable if first. For more information about enabling FIPS after you install the server, see “Enabling FIPS compliance on an automated server installation” on page 94.

You must also make sure that the server certificate is compliant by ensuring that you follow the prerequisites for NIST support. For more information about certificate prerequisites, see Chapter 9, “NIST SP800-131A compliance in IBM Endpoint Manager for Remote Control,” on page 101.

To enable NIST SP800-131A compliance after an automated IBM Endpoint Manager for Remote Control Server installation, complete the following steps.
1. Choose the appropriate method for enabling the NIST configuration.

   Option 1

   a. Go to the tools directory that is in the server installation directory.
   b. Edit the `trcsetup.cmd` or `trcsetup.sh` file, depending on your operating system.
   c. In the line that calls the `ssl.cmd` or `ssl.sh` file, change the 0 that is before **`trc`** to a 1. Change the 0 that is at the end of the command to a 1 also. For example,

      The command before the change is,

      ```
      ...\tools\ssl.cmd" "C:\Program Files (x86)\IBM\Tivoli\TRCServer"
       1 0 "C:\" "%CERTSTOREPW%" "servername.localnet" 0 trc
       "%CERSTOREPWSELF%" "TrC" "0"
      ```

      The command after the change is,

```
...\tools\ssl.cmd" "C:\Program Files (x86)\IBM\Tivoli\TRCServer"
 1 0 "C:\" "%CERTSTOREPW%" "servername.localnet" 1 trc
 "%CERSTOREPWSELF%" "TrC" "1"
```

d. Save the file.

e. In the same directory, edit tmem.sh or tmem.cmd, depending on your operating system.

f. Set the value of **NIST800=1**. Set the value of **FIPSON=1** if it is not already set.

g. Run the following command.

```
trcsetup userid password certpassword
```

Where *userid* and *password* are the database connection credentials and *certpassword* is your certificate file password.

Note: Derby does not have database credentials, therefore use userid and password for the credentials. Type the following command when you are using Derby.

```
trcsetup userid password certpassword
```

Option 2 - Temporary NIST configuration

Note: The configuration changes set in this option are overwritten if you run the trcsetup or tmem files again.

a. Edit the ssl.xml file that is in the [installdir]\wlp\usr\servers\trcserver directory.

where

[installdir]
Is the server installation directory.

b. Add **sslProtocol="TLSv1.2"** to the line **ssl id="defaultSSLConfig"**. For example,

```
<server>
<ssl id="defaultSSLConfig" sslProtocol="TLSv1.2"
/>
<keystore id="defaultKeyStore" password="TrCWebAS"
/>
</server>
```

c. Save the ssl.xml file.

d. In the same directory, edit the jvm.options file.

e. Add the line, **-Dcom.ibm.jsse2.sp800-131=strict**.

f. Save the file.

2. Log on to the IBM Endpoint Manager for Remote Control Server with a valid admin ID and password.
3. Click **Admin** > **Edit properties files**
4. In the common.properties file, set **sp800131a.compliance** to true.
5. Click **Submit**.
6. Click **Admin** > **Reset Application**. Restart the server service. For more information about restarting the server service, see Chapter 6, “Managing the component services,” on page 71. Follow the steps in the section that is relevant to your operating system.

Check to see whether the IBM Endpoint Manager for Remote Control Server is configured for NIST SP800-131A by completing the following step.

- Click **Admin** > **View Current Server Status**.

The fields that show that NIST SP800-131A compliance is enabled are as follows.

- Enabled NIST SP800-131A mode
- JVM configured for NIST SP800-131A mode

Enabling NIST SP800-131A compliance on the controller

The IBM JRE for Windows operating system and Linux (Intel) operating systems is included with IBM Endpoint Manager for Remote Control and is installed when you install the controller software.

If you are using a Windows system, the JRE is included in the controller package `trc_controller_setup.exe` and `trc_controller.msi`. For Linux systems, the JRE is included in the package `ibm-trc-controller-jre-9.1.0.i386.rpm`. These packages install the IBM Java Run-time Environment preconfigured with the IBM FIPS certified cryptographic provider and NIST SP800-131A enabled. The packages also register the MIME type `application/x-ibm-trc-jws` and a file association for `*.trcjws` files.

To check whether the controller is connected in FIPS or NIST SP800-131A mode during a remote control session, click **Controller tools** > **Show session information**. Encryption is set to AES FIPS when FIPS mode is enabled and is set to TLSv1.2 when NIST mode is enabled.

Enabling NIST SP800-131A compliance in the stand-alone controller

After you install the stand-alone controller, you can edit the properties file to enable NIST SP800-131A compliance.

If you install the controller component locally to start peer to peer remote control sessions, you must edit the `trc_controller.cfg` file to enable NIST SP800-131A compliance. To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `trc_controller.cfg` file on the system that the controller is installed on.

   Windows systems

   [controller install dir]\trc_controller.cfg

   where *[controller install dir]* is the installation directory you chose when you installed the controller.

   Linux systems

   `opt/ibm/trc/controller/trc_controller.cfg`
2. Set **`sp800131a.compliance`** to true.
3. Save the file.

NIST SP800-131A compliance on the target

You can enable NIST SP800-131A compliance on the IBM Endpoint Manager for Remote Control target in various ways. NIST SP800-131A compliance can be enabled during installation when you are using the target installation program. You can enable NIST SP800-131A compliance after the installation by editing the target registry on Windows systems, or by editing the configuration file on Linux systems.

Using the target user interface, choose the appropriate option to verify that NIST SP800-131A compliance is enabled on the target.

- On the IBM Endpoint Manager for Remote Control- Target user interface, click **Actions Menu** > **Connection info**.
- Hover the mouse over the IBM Endpoint Manager for Remote Control icon in the system notification area.

Enabling NIST SP800-131A compliance in a Windows target

When you are using a Windows operating system, you can enable NIST SP800-131A compliance on the target in two ways. You can enable compliance during installation or by editing the target registry after installation.

Enabling NIST SP800-131A compliance during the target installation

To enable the NIST SP800-131A compliance target property during installation, follow the instructions in "Installing the target" on page 40. On the **Server Address** screen of the target installer, click **Advanced settings**. Select **Enable NIST SP800-131A compliance (Enables FIPS)**.

Enabling NIST SP800-131A compliance during silent installation of the target

To enable NIST SP800-131A compliance during a silent installation of the target, you can use the **`SP800131A`** parameter in the installation command. For more information about a target silent installation, see "Performing a target custom installation on a Windows system" on page 52.

Use the following parameters to enable NIST SP800-131A compliance.

- TRC_SERVER_PROTOCOL=https
- TRC_SERVER_PORT=443
- SP800131A=yes

For example, `trc_target_setup.exe /s /v"/qn TRC_SERVER_HOSTNAME=`*`yourserver`* `TRC_SERVER_PROTOCOL=https TRC_SERVER_PORT=443 SP800131A=yes"`

where *yourserver* is the host name or IP address of your IBM Endpoint Manager for Remote Control Server.

Enabling NIST SP800-131A compliance after target installation

After you install the IBM Endpoint Manager for Remote Control target, you can enable NIST SP800-131A compliance by editing the target registry. To enable NIST SP800-131A compliance, complete the following steps.

1. Run the **`regedit`** command at a command prompt window.
2. In the Windows registry, go to `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Tivoli\Remote Control\Target` On a 64-bit system, the 32-bit registry keys are under the WOW6432Node key. For example, `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\IBM\Tivoli\Remote Control\Target`.
3. Right-click **SP800131ACompliance** and select **Modify**.
4. Type `yes` in the **Value data** field and click **OK**.
5. Restart the target service. For more information about restarting the target service see, Chapter 6, "Managing the component services," on page 71. Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on Linux or UNIX based targets

After you install the IBM Endpoint Manager for Remote Control target you can enable NIST SP800-131A compliance by editing the `ibmtrct.conf` file. To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `/etc/ibmtrct.conf` file.
2. Set the value of *SP800131ACompliance* to yes and save the file.
3. Restart the target service. For more information about restarting the target service see, Chapter 6, "Managing the component services," on page 71. Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on the gateway

You can enable NIST SP800-131A compliance on the gateway component by editing the gateway configuration file that is created when you install gateway support.

The `trc_gateway.properties` file is in the following directory.

Windows systems

`\Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control\Gateway` for Windows 2000, Windows XP, and Windows 2003 operating systems.

`\ProgramData\IBM\Tivoli\Remote Control\Gateway` for Windows Vista operating system and later versions.

Linux systems

`/etc`

To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `trc_gateway.properties` file.
2. Set **`SP800131ACompliance = Yes`**.
3. Save the file.
4. Restart the gateway service. For more information about restarting the gateway service see, Chapter 6, "Managing the component services," on page 71. Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on the broker

You can enable NIST SP800-131A compliance on the broker component by editing the broker configuration file that is created when you install broker support.

The `trc_broker.properties` file is in the following directory.

Windows systems

`\Documents and Settings\All Users\Application Data\IBM\Tivoli\Remote Control\broker` for Windows 2000, Windows XP, and Windows 2003 operating systems.

`\ProgramData\IBM\Tivoli\Remote Control\broker` for Windows Vista operating system and later.

Linux systems

`/etc`

To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `trc_broker.properties` file.
2. Set **`SP800131ACompliance = Yes`**.
3. Save the file.
4. Restart the broker service. For more information about restarting the broker service see, Chapter 6, “Managing the component services,” on page 71. Follow the steps in the section that is relevant to your operating system.

Enabling NIST SP800-131A compliance on the CLI tools

NIST SP800-131A compliance can be enabled during installation when you are installing the CLI tools on a Windows operating system. You can enable NIST SP800-131A after you install the CLI tools in Linux by editing the configuration file.

Enabling NIST SP800-131A compliance when you install the Windows cli tools

To enable NIST SP800-131A compliance during the installation of the command line interface tools, follow the instruction in “**Installing the cli tools on a Windows system**” on page 63. Click **Advanced settings** on the **Server Address** screen, and select **Enable NIST SP800-131A compliance (Enables FIPS)** during the installation.

Enabling NIST SP800-131A compliance on the cli on Linux or UNIX based targets

After you install the cli tools you can enable NIST SP800-131A compliance by editing the `ibmtrct.conf` file. To enable NIST SP800-131A compliance, complete the following steps.

1. Edit the `/etc/ibmtrct.conf` file.
2. Set the value of *SP800131ACompliance* to yes.
3. Save the file.

Chapter 10. Verifying the server installation

When you have completed the server installation you can verify it by completing the following steps :

1. In a browser window type in the address for the IBM Endpoint Manager for Remote Control server. For example`http://`*`yourservername`*`/trc` where *yourservername* is the hostname or IP address of your IBM Endpoint Manager for Remote Control server.
2. Verify that the IBM Endpoint Manager for Remote Control logon screen is displayed.
3. Logon with the following admin id and password - *id=admin, password=password*.
4. At the change details screen change the password by following the instructions given.

Chapter 11. Recovering from installation errors

If you experience installation errors use this chapter to identify the problem and address it.

Recovery steps

Use the following information as a starting point to find log files and other information to help you recover from installation errors.

If you must contact IBM Software Support, gather the following information.

- If you are using a Windows operating system, any event log that is relevant to the installation error.
- The installation log files.
- Operating system version, including any service packs.
- The version of the WebSphere Application Server, database server, and Java.
- Hardware description.
- Installation media type.
- Windows services that were active during the unsuccessful installation. For example, antivirus software.

The following files can also be used to gather information about any errors that might occur.

`\tsetup.ini`
Contains some basic information, logged during an automated installation.

`[installdir]\install.log`
Contains internal debug messages.

`[installdir]\inst.ini`
Contains all parameters about the installation.

`[installdir]\wlp\usr\server\trcserver`
Contains configuration xml files.

`[installdir]\wlp\usr\server\trcserver\logs\messages.log`

`[installdir]\wlp\usr\server\trcserver\logs\messages_xxxxxxx.log`

`[installdir]\wlp\usr\server\trcserver\logs\ffdc directory`

Errors during installation

The following topics describe recovery actions for errors which might occur during anIBM Endpoint Manager for Remote Control server installation when using the server installer program.

Not enough memory

Symptom
Memory error reported during installation and the installation does not continue.

Cause The memory check at the beginning of the installation has determined that the machine that you are installing on does not have the required minimum memory for installation.

Solution
For details of the requirements for memory, see "Server requirements" on page 9.

DB2 connection error when database options are verified

Symptom
DB2 Database connection error reported during installation.

Causes
During the installation if you have selected DB2 as the database, the installer verifies the information given in the database options screen. The user ID, password and port values are used to establish a connection to the database. If a connection is not successful an error is reported. This error also contains the error reported by DB2.

Solution

This error can be reported for any of the following reasons

- Incorrect values entered in the database options screen. Go back to the previous screen and verify the information that was entered.
- There is no database instance present. If you are planning to use DB2 it should be installed prior to the IBM Endpoint Manager for Remote Control server and a database instance should be created.
- Cannot connect to the remote database. If you are using a remote database verify that you can ping the IP address of the remote system

Oracle pre checks

Symptom
Oracle Database connection error reported during installation.

Cause During the installation if you have selected Oracle as the database, the installer verifies the information given in the database options screen by connecting to the database. If the connection fails, an error is reported. The error message contains the error that is returned from Oracle.

Solution

Go back to the previous screen and use the information given to correct the problem.

For example: If the Oracle database has not been created prior to installation the following error is reported.

```
Failed to verify userid, password, server, database and driver
file combination supplied.Please verify details and try again.
 ( Listener refused the connection with the following error:
ORA-12505. TNS:listener does not currently know of SID given in
connect descriptor
The Connection descriptor used by the client was:
127.0.0.1:1521:TRCDB
```

In this case you should cancel the installation and create the Oracle database before proceeding to install IBM Endpoint Manager for Remote Control again.

libstdc++.so.5 error when installing the server using the installation program

Symptoms

The server installation aborts with the following exception error in Linux.

```
This application has unexpectedly quit:Invocation of this Java
application has caused an InvocationTargetException. This
application will now exit".
```

The installation log may show the following error

```
java.lang.unsatisfiedlinkerror :fontmanager (libstdc++.so.5: can not
open shared object file:No such file or directory)
```

Causes

Missing package required.

Solution

Install the **libstdc++.so.5** package. This can be installed by installing the **compat-libstdc++-33** package which includes libstdc++.so.5.

Errors after installation

When the installation of IBM Endpoint Manager for Remote Control is complete and the application service starts, you can log on. If you cannot log on successfully, use the following information to resolve the problem.

- Check that the server service is running.

  Windows systems

  In Windows services, check that the following service is started

  IBM Endpoint Manager for Remote Control-Server.

  Linux systems

  The following service is created `/etc/init.d/trcserver` or `/etc/rc.d/init.d/trcserver` and started.

  Note: To manually stop or start the server type the following command.

  `/etc/init.d/trcserver [`*`parameter`*`]` Where *parameter* is *stop*, *start*, or *restart*.
- Check the log files in the `[installdir]\wlp\usr\server\trcserver\logs` directory for any reported errors. You can also check the `trc.log` file in the server installation directory.
- If you are using an Oracle database, check that the user ASSET exists.

Out of memory error

Symptom

Out of memory errors are reported in the log files when the IBM Endpoint Manager for Remote Control Server is started. `Failed to instantiate heap` is reported in them.

Causes

There is not enough memory available to run the application. The reason for the error is that the maximum memory allocated to the heap is too high, and can be affected by other applications that are running or installed.

During installation, the installer attempts to set up the IBM Endpoint Manager for Remote Control application to use up to 70% of available RAM. The percentage is lowered if a Java Virtual Machine (JVM) cannot be started. However, if other software is installed, an out of memory error might also be reported in the IBM Endpoint Manager for Remote Control log files.

Solution

The solution to this problem is to use a supplied script to manually set the memory parameters to a lower value. This script, can be found in the IBM Endpoint Manager for Remote Control installation directory. Use the script to set the memory parameters and the number of threads and web connections.

- `tmem.cmd` - for Windows systems.
- `tmem.sh` - for UNIX-based systems.

Run the following command from the IBM Endpoint Manager for Remote Control installation directory:

```
tmem.cmd minmem maxmem
```

Note: Use **`tmem.sh`** for UNIX-based systems.

`minmem; maxmem`
Sets the minimum and maximum memory to be allocated.

Note: The 32-bit Java that is supplied in 32-bit eWAS can use a maximum of 2.7 GB only, no matter how much RAM is available.

You can also use the **`tmem.cmd`** and **`tmem.sh`** command to adjust the following parameters.

`maxwebconn`
Sets the number of web connections allowed. The default is 85 and can increase to 175.

`maxthreads; minthreads`
Sets the minimum and maximum threads allowed. Maximum threads are 50, increasing to 150.

To edit these parameters in version 9.x.x, complete the following steps:

1. Edit `trcsetup.cmd` or `trcsetup.sh`.
2. Edit the line that contains the call to the `memory.cmd` file. For example, C:\TRC\server\tools\memory.cmd 163 49 135 1

   where

   - **`maxwebconn`** = parameter 1 (163)
   - **`minthreads`** = parameter 2 (49)
   - **`maxthreads`** = parameter 3 (135)

   Do not edit parameter 4. Keep the value 1.
3. Change the required values.
4. Save the `trcsetup` file.
5. Type the following command.

   ```
   trcsetup userid password certpassword
   ```

   Where *userid* and *password* are the database connection credentials and *certpassword* is your certificate file password.

Note: Derby does not have database credentials, therefore use userid and password for the credentials. Type the following command when you are using Derby:

`trcsetup userid password` *certpassword*

Database connection authorization failure

Symptom
A database connection authorization failure error is reported in the log files.

Causes
The database password might be invalid.

Solution
Change the password by running the following command from the IBM Endpoint Manager for Remote Control installation directory:

Windows systems
[installdir]`\tools\tdbpasswd.cmd` *userid password*. Where *installdir* is the IBM Endpoint Manager for Remote Control installation directory and *userid* and *password* are the database log on credentials.

UNIX-based systems
[installdir]`/tools/tdbpasswd.sh` *userid password*. Where *installdir* is the IBM Endpoint Manager for Remote Control installation directory and *userid* and *password* are the database log on credentials.

Run the command to change the database password for the application. Restart the IBM Endpoint Manager for Remote Control service after you run the command.

Application welcome page does not display

Symptom
The IBM Endpoint Manager for Remote Control server welcome page does not appear when you type in the IBM Endpoint Manager for Remote Control server URL in your browser.

Cause The issue can occur for a number of reasons, which are reported in the log files.

Solution
Look through the `install.log` file in the server installation directory, for any reported errors.

DB2 connection error when database options are verified

Symptom
DB2 Database connection error reported during installation.

Causes
During the installation if you have selected DB2 as the database, the installer verifies the information given in the database options screen. The user ID, password and port values are used to establish a connection to the database. If a connection is not successful an error is reported. This error also contains the error reported by DB2.

Solution

This error can be reported for any of the following reasons

- Incorrect values entered in the database options screen. Go back to the previous screen and verify the information that was entered.
- There is no database instance present. If you are planning to use DB2 it should be installed prior to the IBM Endpoint Manager for Remote Control server and a database instance should be created.
- Cannot connect to the remote database. If you are using a remote database verify that you can ping the IP address of the remote system

Cannot see targets contacting the server

Symptom

Targets are not registering or updating their details on the IBM Endpoint Manager for Remote Control Server.

Causes

The target does not have the correct URL for the server or the host name part of the URL, that is used to contact the server, does not match the common name in the server's SSL certificate.

Solution

When you install the target software the target contacts the server by using http or https, and the server URL that is defined during the installation of the target. However, there are two important things to note to ensure that the connection between the server and target is successful.

- The target must have the correct URL for the server.
- The host name part of the URL must match the common name in the server's SSL certificate.

When the IBM Endpoint Manager for Remote Control Server is installed with the installation program you must ensure that you supply the correct values in the Web server parameters window. By default, the **upload data to server** field is populated with the computer name from the Windows operating system settings. The server installer program uses the field value to generate the server URL. The URL is then saved in the `trc.properties` file, in the **`url`** property and is also saved in the SSL certificate. Therefore, make sure that you specify the correct computer name during the installation. If you specify an incorrect value, the following problem might occur.

When a target contacts the server for the first time, it uses the **`ServerURL`** property from the target registry or configuration file to contact the server. When the server responds to the target it includes the server address that is assigned to the **`url`** property in the `trc.properties` file. The target now uses this URL to contact the server. If the address that is sent to the target is incorrect, the symptoms you will see are that the target can register once and then is not able to contact the server again. After a while the target is marked as being offline. You are also unable to start sessions with this target, because the target does not have a correct working URL with which to authenticate an incoming session.

The common name that is in the server's SSL certificate has to be a host name that actually resolves to the IP address of the server. If the SSL certificate has, for example, *mytrcserver*, but on the target there is no way to translate *mytrcserver* to the IP address of the server, your environment is not correctly configured. The only names that are correctly supported for this are fully qualified domain names that are registered in the DNS. For example, **mytrcserver.example.ibm.com**. If you use only *mytrcserver*, that will only work if the server and target are on the same local network and have WINS configured.

You can check that the DNS server is properly configured by using the **nslookup** command to query the full computername and IP address.

For example: At a command prompt type the following commands

```
C:\>nslookup

Default Server:  gbibp9ph1--31ndcr.wan.ibm.com
Address:  192.0.2.0



Type in the hostname of your server

> mytrcserver.example.ibm.com
Server:  gbibp9ph1--31ndcr.wan.ibm.com
Address:  192.0.2.0

Name:    mytrcserver.example.ibm.com
Address:  192.0.2.1



Type in the ip address of your server

> 9.169.86.25
Server:  gbibp9ph1--31ndcr.wan.ibm.com
Address:  192.0.2.0

Name:    mytrcserver.example.ibm.com
Address:  192.0.2.1
```

In the example you can see that the server hostname resolves to the correct IP address.

Errors when using Oracle as the database

Symptom

java.lang.ArrayIndexOutOfBoundsException error reported when using an Oracle database.

Cause There is a problem with the Oracle jdbc drivers.

Solution

Choose the appropriate option to resolve this problem

- Use the Oracle 10.2g JDBC 4 drivers. These will work with oracle 9, 10 and 11.
- If you are using the Oracle 11g drivers, manually edit the `trc.properties` file and set the following property **`oracle.increment.keys.off=1`**.

  Note: Restart the server service.

Errors when trying to connect to the Microsoft SQL database in FIPS compliancy mode

Symptom
Errors when trying to connect to the Microsoft SQL database in FIPS compliancy mode

Cause Using the IBM JRE and the IBM JSSE provider and Websphere Application Server, which has been enabled for FIPS compliancy currently, does not work when using an MS SQL database.

Solution
These options only work with MS SQL when FIPS is **not** enabled in IBM Websphere.

Chapter 12. Uninstalling the components

After you install the various IBM Endpoint Manager for Remote Control components you can uninstall them in various ways.

Uninstalling the server

To remove the IBM Endpoint Manager for Remote Control server, the method you choose depends on the type of installation that was performed. If you installed the server using the IBM Endpoint Manager for Remote Control installation program you can uninstall the software using the installer or by using Add or Remove programs. If you performed a manual installation of IBM Endpoint Manager for Remote Control Server you should uninstall the software using the IBM Websphere Application Server administration console.

Uninstalling the server by using the installer

Use the following procedure to uninstall the IBM Endpoint Manager for Remote Control server software if you are using a Windows operating system or a Linux operating system.

To uninstall the IBM Endpoint Manager for Remote Control server by using the installer, complete the following steps :

1. Navigate to the IBM Endpoint Manager for Remote Control server installation directory. The default directory or the specific directory that you chose when you installed the server. For example,

   Windows systems

   ```
   \Program Files\ibm\Tivoli\TRC\server
   ```

   Linux systems

   ```
   /opt/IBM/Tivoli/TRC/server
   ```
2. Double click **Uninstall IBM Endpoint Manager for Remote Control - Server.exe**
3. Click **Uninstall**.
4. Click **Done** when finished.

The IBM Endpoint Manager for Remote Control features, files, and folders that were created by the installer are removed.

Uninstalling the server application in IBM Websphere Application Server

If you have performed a manual installation of the IBM Endpoint Manager for Remote Control Server software, you can uninstall the software using the IBM Websphere Application Server administration console by completing the following steps:

To access the Administrative Console complete the following steps:

1. In your browser type

   ```
   https://[server : port]/ibm/console
   where server is the ipaddress or name for the application server machine
   for example localhost or 192.0.2.0 and port is the port that the server is listening on.
   ```

2. Logon with the ID and password that were defined when installing Websphere.
3. Expand Applications and click **Enterprise applications**.
4. Select the check box for the IBM Endpoint Manager for Remote Control server application.
5. Click **Uninstall**.
6. Select **Save** to save to the Master Configuration.

Uninstalling the server using Add or Remove programs

If you are using a Windows operating system you can uninstall the server software, using Add or Remove Programs by completing the following steps :

1. Open the **Control Panel**.
2. Double click **Add or Remove Programs**.
3. Select **IBM Endpoint Manager for Remote Control - Server**.
4. Click **Change /Remove**.
5. Click **Uninstall**.
6. Click **Done** when finished.

Uninstalling the target on Windows systems

Using **Add or Remove Programs** to remove the target software from a Windows system.

To remove the target software using Add or Remove Programs complete the following steps:

1. Open the **Control Panel**.
2. Double click **Add or Remove Programs**.
3. Select **IBM IBM Endpoint Manager for Remote Control - Target**.
4. Click **Remove**.
5. Click **Yes** at the prompt.

The IBM Endpoint Manager for Remote Control target software is removed from your system.

Uninstalling the target on Linux systems

To remove the target software on Linux systems, complete the following steps :

1. To find the IBM Endpoint Manager for Remote Control package name that is installed run the following command.
   ```
   rpm -qa |grep trc
   ```
2. Run the following command:
   ```
   rpm -e <trcpackage>
   ```
   where *trcpackage* is your package name.
   ```
   For example: rpm -e ibm-trc-target
   ```

You can verify the target is removed by completing the following steps:

1. Run the command in step 1 to make sure that there is no IBM Endpoint Manager for Remote Control package installed.
2. Run the following command to make sure that there is no IBM Endpoint Manager for Remote Control process running.

```
ps -ef |grep trc
```

Chapter 13. Upgrading from previous versions

The following limitation is not an issue when you upgrade from version 9.0.0 or 9.0.1 to version 9.1.0.

IBM Endpoint Manager for Remote Control version 9.0.0 introduced new capabilities that can cause some backwards compatibility issues if the different components are not upgraded in the correct order.

This limitation applies only to environments where the gateway and broker components have been deployed. In these environments, the broker and gateway must be updated before the server or the target components. After they are upgraded, the targets and server can be upgraded in the order that best suits your environment, since there are no dependencies between them.

It is recommended to always back up any properties files as a precaution, however it must be noted that this is mandatory for the controller upgrade in this release, as any existing properties will be lost.

Upgrading the gateway component

You can upgrade the gateway component by using any of the following methods:

Using the installation files

For more information about obtaining the component installation files, see "Obtain the installation files" on page 19. For more information about installing the gateway support on a Windows system, by using the installation files, see "Installing Windows gateway support" on page 65. For details about installing the gateway support in Linux, using the installation files, see "Installing Linux gateway support" on page 66.

Using the IBM Endpoint Manager console

If you have the IBM Endpoint Manager console infrastructure installed you can use the update fixlets to upgrade the gateway support. For more information about the upgrade fixlets, see the *IBM Endpoint Manager for Remote Control Console User's Guide*.

Upgrading the broker component

You can upgrade the broker support by using any of the following methods:

Using the installation files

For more information about obtaining the component installation files, see "Obtain the installation files" on page 19. For more information about installing the broker support on a Windows system, by using the installation files, see "Installing Windows broker support" on page 67. For more information about installing the broker support in Linux, by using the installation files, see "Installing Linux broker support" on page 67.

Using the IBM Endpoint Manager console

If you have the IBM Endpoint Manager console infrastructure installed you can use the update fixlets to upgrade the broker support. For more information about the upgrade fixlets, see the *IBM Endpoint Manager for Remote Control Console User's Guide*.

Upgrade the server component

If you already installed the IBM Endpoint Manager for Remote Control Server software, you can upgrade the component by carrying out a similar installation type to your original installation.

Before you start the upgrade, you must back up your property files and any recording files if applicable. Back up any certificates, if applicable. For more information about backing up and restoring certificates, see the *IBM Endpoint Manager for Remote Control Administrator's Guide*

Property files

- `common.properties`
- `ldap.properties`
- `trc.properties`
- `log4j.properties`
- `controller.properties`

The files are in the following directories.

Windows systems

`[`*`InstallDir`*`]wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes\` Where *InstallDir* is the IBM Endpoint Manager for Remote Control server installation directory. For example, `C:\Program Files (x86)\IBM\Tivoli\TRC\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes\`

Linux systems

`[`*`InstallDir`*`]wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes/` Where *InstallDir* is the IBM Endpoint Manager for Remote Control server installation directory.

Recordings Files

The video recordings folder is defined by the **rc.recording.directory** property in the **trc.properties** file.

You can upgrade the server component by using any of the following methods:

Using the installation files

For more information about obtaining the component installation files, see "Obtain the installation files" on page 19. For details about installing the server, by using the installer, see "Installing by using the server installer" on page 25.

Note: During the installation, select to keep existing property files and do not select to drop the database.
For information about installing the server, on WebSphere 8.5, see "Installing on WebSphere Application Server version 8.5: deploying the war file" on page 32.

Using the IBM Endpoint Manager console

If you have the IBM Endpoint Manager console infrastructure installed you can create and run a server installation task to upgrade the server. For more information about using the wizard to create a server configuration task, see the IBM Endpoint Manager for Remote Control Console User's Guide.

Note: When you create the server task, do not select the drop database option if you want to keep your existing database.

When you complete the upgrade verify that the new version is installed, manually edit the new properties files. Update the values with the values that are in your backed up properties files. Restore your recording files and certificates if applicable

Upgrading the target component

You can upgrade the target component by using any of the following methods:

Using the installation files

For more details about obtaining the component installation files, see "Obtain the installation files" on page 19. For more information about installing the target component on a Windows system, using the installation files, see "Installing the Windows target" on page 40. For more information about installing the target component on a Linux system, by using the installation files, see "Installing the Linux target" on page 51.

Using the IBM Endpoint Manager console

If you have the IBM Endpoint Manager console infrastructure installed you can use the update fixlets to upgrade the target component. For more information about the upgrade fixlets, see the *IBM Endpoint Manager for Remote Control Console User's Guide*.

Upgrading the controller component

The controller component upgrade is a major upgrade. Any existing properties are backed up and added to the new properties file.

If you are using a Linux operating system and are upgrading from IBM Endpoint Manager for Remote Control version 9.0.1 or earlier, edit the `trc_controller.cfg.rpmnew` file. Compare the property values in the file with the values in the `trc_controller.cfg` file. Merge the differences into the `trc_controller.cfg` file and save the file.

Any of the following methods can be used to upgrade the controller component:

Using the installation files

For more information about obtaining the component installation files, see "Obtain the installation files" on page 19. For more information about installing the controller component on a Windows system, by using the installation files, see "Installing the controller on a Windows system" on page 59. For more information about installing the controller component in a Linux system, by using the installation files, see "Installing the Linux controller" on page 60.

Using the IBM Endpoint Manager console

If you have the IBM Endpoint Manager console infrastructure installed you can use the update fixlets to upgrade the controller component. For more information about using the update fixlets, see the *IBM Endpoint Manager for Remote Control Console User's Guide*.

Chapter 14. Maintaining the target installation

The IBM Endpoint Manager for Remote Control Target installation can be modified using a maintenance program.

You can access the maintenance program on a system with Microsoft Windows by running the `trc_target_setup.exe` program. To access the maintenance program complete the following steps :

1. Navigate to the directory that the IBM Endpoint Manager for Remote Control target software was installed to

   ```
   for example : \Program Files\ibm\Tivoli Remote Control\RCTarget
   ```
2. Double click `trc_target_setup.exe`.
3. At the welcome screen click **Next**.
4. Select the required option and click **Next**

   Modify

   Select this option to navigate through the target installation screens to modify the previously installed values.To modify the installation properties follow from step 5 on page 40

   Repair

   Select this option to fix missing or corrupt files, shortcuts, and registry entries.

   a. Click **Repair**.
   b. Click **Finish**.

   Remove

   Select this option to remove the target software and all of its features.

   a. Click **Remove**.
   b. Click **Finish**.

Appendix. Support

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

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services that are offered in the USA.

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, MD-NC119
Armonk, NY 10504-1785
United States of America

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

Programming interface information

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 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 Minister for the Cabinet Office, 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.

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Index

Product Number: 5725-C43

Printed in USA