IBM Endpoint Manager for Remote Control Administrator's Guide

Version 9.1.0

IBM Endpoint Manager for Remote Control Administrator's Guide

Version 9.1.0

Note
Before using this information and the product it supports, read the information in "Notices" on page 333.

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. 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.

Chapter 2. Setting a secure environment

By default, IBM Endpoint Manager for Remote Control is configured for http access and https with a default self-generated certificate. Learn how to configure more advanced security parameters for your environment.

Using a secure URL

Selecting https during installation

During a server installation, when you are using the server installer, you can enable https. Selecting to enable https changes the URL property that is passed to the target. The https server url is sent to the target. However, http is still enabled.

The **secure.url** property is prefilled during the installation with the secure url.

When you select the https check box, the following property is set

url=secure.url

When you do not select the https check box the property is set as:

url=regular http address

where regular http address is the server IP address that is used for http access.

Disabling http

If during the server installation you select to use https, you can also disable http completely on the web server by setting the **Server Port on Webserver** field in the installer screens, or the **HTTP port** field in the **IBM Endpoint Manager for Remote Control Server Installer Wizard**, to 0.

Enforcing logon via https

Currently the logon page can be accessed and posted by using http or https. To force https, the webserver on http must be disabled. You can disable http by specifying port 0 for the http port in the server installer, during the installation. There are also properties in the `trc.properties` file that you can use to force logons from the server GUI to use https.

`enforce.secure.weblogon=`

Modifiable Field	**enforce.secure.weblogon**
Field Description	Make the default logon action from the web user interface use https. This requires **secure.url** to be set with the full host name.
Possible Values	true / false

Value Definition	**True** Logons from the IBM Endpoint Manager for Remote Control Server GUI use https. Logons using http through another tool or page are not prevented. Https is not shown in the url, but the logon page with USERID/PASSWORD is posted via https. The **secure.url** parameter is used. If this is set incorrectly the logon will not succeed. **False** Logon via http or https, whichever has been entered in the browser url.

`enforce.secure.alllogon=`

Modifiable Field	**enforce.secure.alllogon**
Field Description	Force any logon action to use https, deny any non https logon. This requires **secure.url** to be set with the full host name.
Possible Values	true / false
Value Definition	**True** Any logon attempt using http is rejected and redirected to the logon page. **False** Logon via http or https, whichever has been entered in the browser url

The difference between the parameters is as follows. Use the **enforce.secure.weblogon** parameter to ensure that the user ID and password are passed from the logon page and posted over https regardless of the url. However you can still logon using http either via a custom page or another tool. Use **enforce.secure.alllogon** to restrict this behaviour. The logon link rejects any non https connection, when **enforce.secure.alllogon** is set.

Note:

1. The **secure.url** property must be set with a proper host name, not localhost.
2. The session after the logon, remains in https. Unless other enforce.secure parameters have been set, there is nothing to stop a user using http for the duration of the session.

Secure communication configuration

You can use the following properties in `trc.properties` to control, how secure communications is enforced.

`secure.url=`

Modifiable Field	**secure.url**
Field Description	Determines the base url that is used to redirect requests when secure communications are required.
Possible Values	User-defined - for example **https://*X.X.X.X*/trc** where *X.X.X.X* is the IP address of your IBM Endpoint Manager for Remote Control server. **Note:** This separate url property is required because replacing http with https in the base url does not work because the ports for each URL might be different.

Value Definition	User-defined. URL and context root of application when you are using secure connections.

`enforce.secure.web.access=`

Modifiable Field	**enforce.secure.web.access**
Field Description	An http request that is not a callhome, upload, or validation request is redirected to the same url. The value that is set in the **secure.url** property is used as a base.
Possible Values	true / false
Value Definition	**True** The http request is redirected to the secure url. **False** The http request is not redirected to the secure url. **Note:** When you change the value of this property, you must restart the IBM Endpoint Manager for Remote Control server service for the new value to take effect.

`enforce.secure.endpoint.callhome=`

Modifiable Field	**enforce.secure.endpoint.callhome**
Field Description	Determines the url that a target uses to contact the IBM Endpoint Manager for Remote Control server.
Possible Values	true / false
Value Definition	**True** If a callhome is received by using http, the request is redirected to the secure url. The secure url is also returned in the response from the server. Targets are forced to use the secure url when they send heartbeats to the IBM Endpoint Manager for Remote Control server. **False** Targets are not forced to use the secure url when they send heartbeats to the IBM Endpoint Manager for Remote Control server. This value is the default value. **Note:** When you change the value of this property, you must restart the IBM Endpoint Manager for Remote Control server service for the new value to take effect.

`enforce.secure.endpoint.upload=`

Modifiable Field	**enforce.secure.endpoint.upload**
Field Description	Determines whether the controller or target uses the secure url to upload the recordings and audit information to the server.
Possible Values	true / false

Value Definition	**True** If an upload or a validation request is received by using http, the server redirects the request to an equivalent url built with the value defined in **secure.url** as a base. It also uses the value of **secure.url** as a base to provide the upload and validation urls to the controller and target when the session starts. **False** If an upload or a validation request is received by using http, the server does not redirect to the secure url. **Note:** When you change the value of this property, you must restart the IBM Endpoint Manager for Remote Control server service for the new value to take effect.

The following examples consider scenarios that reflect different security requirements that you might have about communications with the IBM Endpoint Manager for Remote Control Server:

- *All endpoint and user communications with the server must be encrypted with SSL*

  Configuration

  – Set **secure.url** in the trc.properties file to contain the https url.
  – Set the three enforce.secure properties to true by editing the trc.properties file
  – The Target and CLI do not need to be explicitly configured to use the https url, but doing so avoids the first redirection.

- *All user communications with the server must be encrypted with SSL. Endpoint communications that are not CallHomes must be encrypted. For example, audit and recording uploads or validating session requests.*

  Configuration

  – Configure the regular non https url to be used by the callhomes in the url property in the trc.properties file.
  – Configure the https url to be used by the users, endpoint uploads, and the API in the **secure.url** property
  – enforce.secure.web.access = true.
  – enforce.secure.endpoint.callhome = false.
  – enforce.secure.endpoint.upload = true.
  – Target and CLI tools are configured with the http url.

- *All user communications with the server must be encrypted with SSL. Endpoint communications do not need to be encrypted.*

  Configuration

  – Configure the regular non-https url to be used by the endpoints callhome and uploads in the url property in the trc.properties file.
  – Configure the https url to be used by the users and the API in the **secure.url** property.
  – enforce.secure.web.access = true.
  – enforce.secure.endpoint.callhome = false.
  – enforce.secure.endpoint.upload = false.
  – Target and CLI tools are configured with the http url .

- *No need for enforcement other than via the regular configuration options (url property and ServerURL)*

Configuration

The new properties keep their default values:

- secure.url = https://localhost/trc
- enforce.secure.web.access = false
- enforce.secure.endpoint.callhome = false
- enforce.secure.endpoint.upload = false

Signed certificate management

By default, IBM Endpoint Manager for Remote Control creates a self-signed certificate for the website.

You can change the default certificate by installing your own certificate. For more information about installing a certificate see, "Installing a certificate."

The default certificate is in the following directory.

Windows systems

`\[installdir]\wlp\usr\servers\trcserver\resources\security`

Linux systems

`/[installdir]/wlp/usr/servers/trcserver/resources/security`

where [*installdir*] is the IBM Endpoint Manager for Remote Control installation directory.

The file name is `key.jks` and has a default password of **`TrCWebAS`**.

The configuration for the certificate file is stored in the `ssl.xml` file in the following directory.

Windows systems

`\[installdir]\wlp\usr\servers\trcserver`

Linux systems

`/[installdir]/wlp/usr/servers/trcserver`

where [*installdir*] is the IBM Endpoint Manager for Remote Control installation directory. Any changes to the `ssl.xml` file are overwritten by configuration changes when you reinstall or upgrade the IBM Endpoint Manager for Remote Control server, or rerun **`trcsetup.cmd`**.

Installing a certificate

To install a certificate in IBM Endpoint Manager for Remote Control you can either use an existing `P12` or `JKS` keystore or import an existing certificate into the existing keystore.

Any changes that are made to the certificate configuration are overwritten if you reinstall or upgrade the IBM Endpoint Manager for Remote Control server. Choose the appropriate method to install a certificate for IBM Endpoint Manager for Remote Control. You can also configure the SSL certificate by using the server installer. For more information about configuring the SSL certificate during installation, see the IBM Endpoint Manager for Remote Control Installation Guide

1. To use an existing keystore, complete the following steps:
   a. Edit the `ssl.xml` file.

b. Locate the **<keystore/>** parameter. Set appropriate values for your certificate keystore.

id The default value is **defaultKeyStore**. You can change the value to an id of your choice or keep the default value.

password
The default value is **TrCWebAS**. Replace the password with the password for the existing certificate store. You can enter the password in plain text, or encode the password by using the `securityUtility` tool. Use the following command to encode your password. For example, on a Windows system use `securityUtility.bat`.

```
[installdir]\wlp\bin\securityUtility encode
```

where *[installdir]* is the IBM Endpoint Manager for Remote Control server installation directory. Enter your password. Use the generated string for the password parameter.

location
Enter the absolute path to the existing keystore. The value can be the path to a `jks` file or a `p12` file.

type Determines the type of keystore file. If you are using a `p12` file use **PKCS12**. If you are using a `jks` file, you do not need to define a type value.

c. Save the file.

d. Restart the IBM Endpoint Manager for Remote Control server.

2. To generate a signed certificate, complete the following steps:

a. Open a command line window.

b. Go to the IBM Endpoint Manager for Remote Control installation directory.

c. Change to the `java\jre\bin` subdirectory on a Windows system or the `java/jre/bin` subdirectory on a Linux system.

d. Run **ikeyman.sh** on a Linux system or **ikeyman.exe** on a Windows system.

e. In the GUI window select **Key Database File** > **Open**.

a. Go to the `\[installdir]\/wlp/usr/servers/trcserver/resources/security` directory, where [*installdir*] is the IBM Endpoint Manager for Remote Control installation directory.

b. Select **key.jks**. This file is the default keystore.

c. Click **open**.

d. Enter the password `TrCWebAS`.

e. Carry out the appropriate procedure to install the certificate.

- Create a certificate request
  1) Select **Create** > **Create New Certificate Request**.
  2) Provide a **Key Label** name. The name is displayed in the GUI.
  3) Type in any additional optional information as required.
  4) Click **OK**.
  5) A `certreq.arm` file is generated and saved to the location specified. This file must be sent to the certificate authority to be signed and a `cert.arm` file is returned.
  6) When you receive the signed certificate, select **Receive**.
  7) Browse to your `cert.arm` signed file.

8) Click **OK**.

- Externally sign the existing certificate
  1) Select **Recreate Request**.
  2) A `certreq.arm` file is generated and saved to the location specified. This file must be sent to the certificate authority to be signed and a `cert.arm` file is returned.
  3) When you receive the signed certificate, select **Receive**.
  4) Browse to your `cert.arm` signed file.
  5) Click **OK**.

3. You can see a second certificate listed. Delete the default certificate.
4. Save and overwrite the `key.jks` file. When you are prompted for the password, type `TrCWebAS`.
5. Restart the server. The https port is signed with the correct certificate.

Backing up your certificate file

Back up your certificate file if you are upgrading your IBM Endpoint Manager for Remote Control server and you previously manually installed a certificate.

The following information applies only when you previously used the server installer to install the IBM Endpoint Manager for Remote Control server with an embedded WebSphere Application Server 8.5 Liberty Profile.

If you are using the default keystore and `key.jks` file, back up the following file and directory.

Windows systems

`\[installdir]\wlp\usr\servers\trcserver\resources\security\key.jks`

Linux systems

`/[installdir]/wlp/usr/servers/trcserver/resources/security/key.jks`

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

If the default keystore file is not in the default directory or you changed the default keystore password, also back up the `ssl.xml` file. The file is in the following location.

Windows systems

`\[installdir]\wlp\usr\servers\trcserver\ssl.xml`

Linux systems

`/[installdir]/wlp/usr/servers/trcserver/ssl.xml`

where [*installdir*] is the IBM Endpoint Manager for Remote Control installation directory.

Note: If your`key.jks` file is not in the default keystore directory, but is still within the IBM Endpoint Manager for Remote Control server installation directory you must back up the `key.jks` file.

Setting password rules

You can use properties in the `trc.properties` file to create a set of password rules. The rules can define the type of passwords that can be created, how the passwords must be created, and whether the passwords must be periodically changed.

`password.encrypt=`

Modifiable Field	**password.encrypt**
Field Description	Determines whether passwords are encrypted in the database.
Possible Values	Yes/No, 1/0
Value Definition	If Yes, passwords are encrypted in the database; if No, passwords are not encrypted in the database.

`password.reuse=`

Modifiable Field	**password.reuse**
Field Description	Determines whether users can reuse passwords.
Possible Values	Yes/No, 1/0
Value Definition	If Yes, users can reuse passwords; if No, users cannot reuse passwords.

`expire.new.password=`

Modifiable Field	**expire.new.password**
Field Description	Determines whether users are required to set their own password after they receive the computer-generated password.
Possible Values	True/False, 1/0
Value Definition	If True, users must set their own password after they receive the computer-generated password; if No, users do not have to set their own password after they receive the computer-generated password.

`password.timeout=`

Modifiable Field	**password.timeout**
Field Description	Determines whether passwords expire.
Possible Values	True/False, 1/0
Value Definition	If True, passwords expire; if False, passwords do not expire.

`password.timeout.period=`

Modifiable Field	**password.timeout.period**
Field Description	Defines after how many days passwords expire.
Possible Values	User-defined
Value Definition	User-defined integer

password.period=

Modifiable Field	**password.period**
Field Description	Maximum number of days before a password can be reused.
Possible Values	User-defined
Value Definition	User-defined integer

password.check=

Modifiable Field	**password.check**
Field Description	Determines whether to enable password rule checking.
Possible Values	True/False, 1/0
Value Definition	If True, creation of passwords must follow certain rules; if False, creation of passwords does not have to follow rules.

password.must.have.non.numeric=

Modifiable Field	**password.must.have.non.numeric**
Field Description	Determines whether passwords must contain non-numeric characters.
Possible Values	True/False, 1/0
Value Definition	If True, passwords must contain non-numeric characters; if False, passwords do not have to contain non-numeric characters.

password.must.have.numeric=

Modifiable Field	**password.must.have.numeric**
Field Description	Determines whether passwords must contain numeric characters.
Possible Values	True/False, 1/0
Value Definition	If True, passwords must contain numeric characters; if False, passwords do not have to contain numeric characters.

password.must.have.non.alphanumeric=

Modifiable Field	**password.must.have.non.alphanumeric**
Field Description	Determines whether passwords must contain non-alphanumeric characters.
Possible Values	True/False, 1/0
Value Definition	If True, passwords must contain non-alphanumeric characters; if False, passwords do not have to contain non-alphanumeric characters.

password.min.length=

Modifiable Field	**password.min.length**

Field Description	Minimum length of a password.
Possible Values	User-defined
Value Definition	User-defined integer

`password.max.length=`

Modifiable Field	**password.max.length**
Field Description	Maximum length of a password.
Possible Values	User-defined
Value Definition	User-defined integer

`password.max.matching.sequential.chars=`

Modifiable Field	**password.max.matching.sequential.chars**
Field Description	Maximum number of sequential password characters that can match.
Possible Values	User-defined
Value Definition	User-defined integer

`password.max.previous.chars=`

Modifiable Field	**password.max.previous.chars**
Field Description	Maximum number of sequential password characters that can be reused in a new password.
Possible Values	User-defined
Value Definition	User-defined integer

Locking user accounts

To prevent anyone trying to guess a username and password combination, you can lock users accounts after a number of unsuccessful log on attempts. When an account is locked with a time period enabled, when the time period expires, a user can log on again with the correct password. However if an incorrect password is entered another time, the account is locked again after a single attempt. If the account is locked and a user attempts to log on during the lockout period, the expiry time will start from the last attempt, even when the attempt was made during a locked out phase. This is for security reasons, so that an administrator can see if an attempt is being made to hack an account; the failed count is increasing and the last time of failure recorded. You can use the following properties to lock user accounts, set a period of time for the lock and specify machines that the locked account can be used on.

`account.lockout=`

Modifiable Field	**account.lockout**
Field Description	Lock a user account after a consecutive number failed logons. Set to 0 to disable this function, this is the default value.
Possible Values	user defined
Value Definition	User-defined. integer.

`account.lockout.timeout=`

Modifiable Field	**account.lockout.timeout**
Field Description	If user account is locked due to consecutive failed logons, re-enable the account after this time. The period can be MIN,HOUR,DAY,MONTH. **Note:** This is only valid when **account.lockout** is enabled.
Possible Values	User-defined
Value Definition	User-defined. MIN,HOUR,DAY,MONTH. For example, set to 5MIN means the account is locked for 5 minutes, set to 2DAY, account is locked for 2 days. **Note:** If left blank the account is locked until manually set.

`account.lockout.allowlogonfrom=`

Modifiable Field	**account.lockout.allowlogonfrom**
Field Description	You can use this property to permit users to log on from this host even if their account is locked due to consecutive failed logons. If your account has been locked, you can log on to the IBM Endpoint Manager for Remote Control Server from the machine or machines whose IP addresses are listed here.`For example : 192.0.2.1;192.0.2.2;` **Note:** You must end each host name with ;
Possible Values	User-defined
Value Definition	User-defined list of IP addresses separated by a semi colon and ending the list with a semi-colon.

Examples of usage:

account.lockout = 0

account.lockout.timeout = X

The account is not locked after unsuccessful log on attempts because:

account.lockout=0

account.lockout = 3

account.lockout.timeout =

After three successive failed logons for an account, the account is locked, and requires a reset via the database or the server UI using an administrator account. This is a manual reset because **account.lockout.timeout** is not assigned a value.

account.lockout = 3

account.lockout.timeout = 1HOUR

After three successive failed logons for an account, the account is locked for a duration of 1hour, but could be reset via the database or the serverUI using an administrator account.

account.lockout = 3

account.lockout.timeout =

account.lockout.allowlogonfrom=1.1.1.1;

After three successive failed logons for an account, the account is locked, and requires a reset via the database or the server UI using an administrator account, or the user can logon from a machine with the IP address set in **account.lockout.allowlogonfrom** and the lockout is ignored.

When a user account has been locked, you can unlock the account using the **Unlock locked userid** menu item. See Chapter 4, "Unlocking user accounts," on page 17.

When a user uses the forgotten password on the logon page, a password is emailed to the registered user for the account. However if the account is locked, it remains locked. This is a security precaution to prevent an attacker having unlimited attempts to guess a password. You can use the property **account.lockout.reset.onemailpassword** to automatically unlock an account in this scenario.

account.lockout.reset.on.emailpassword=

Modifiable Field	**account.lockout.reset.on.emailpassword**
Field Description	Determines whether a locked account is reset when the user selects the forgotten password check box on the logon screen.
Possible Values	True / False
Value Definition	**True** The locked account is reset when the password reset email is received from the administrator. **False** The locked account is not reset when the forgotten password request is received **Note:** As this works in conjunction with the forgotten password feature, email must be enabled in the system.

Chapter 3. Accessing the IBM Endpoint Manager for Remote Control Server Web Interface

After you install the IBM Endpoint Manager for Remote Control Server software and the IBM Endpoint Manager for Remote Control Target software, you can logon to the server application. For more information about installing and configuring the server and target software, see the *IBM Endpoint Manager for Remote Control Installation Guide*.

Logging on to the IBM Endpoint Manager for Remote Control server

To use the IBM Endpoint Manager for Remote Control Server, log on to the server user interface.

1. In a web browser type `http://SERVERNAME/trc`.

   SERVERNAME: This is the name of your IBM Endpoint Manager for Remote Control Server. If you do not have this name, contact your IBM Endpoint Manager for Remote Control System Administrator.
2. Enter a valid ID and password. Invalid or missing IDs and passwords generate an error message.

   If you are an Administrator, and this is your first time logging on, the default Admin ID is `admin` and password is `password`. After you log on for the first time, you must change your password.

   Password rules are set in the `trc.properties` file in the set of variables starting with **`password.`** For more information about password rules, see the *IBM Endpoint Manager for Remote Control Administrator's Guide*.
3. Click **Logon**.

The IBM Endpoint Manager for Remote Control Server UI is displayed.

Getting a temporary logon password

If you forget your password, you can use the forgotten password option on the server logon screen.

The temporary password is sent to you in an email. This function is available when email has been set up and enabled in the system. You can enable email functions at installation or by editing the `trc.properties` file. For more information, see the IBM Endpoint Manager for Remote Control Installation Guide and the IBM Endpoint Manager for Remote Control Administrator's Guide.

Note: If email **AND** LDAP are enabled, the forgotten password option is not displayed.

To obtain a temporary password, complete the following steps on the logon screen:

1. Enter your ID.
2. Click **Forgotten password**.
3. Click **Logon**. A message is displayed: `A new password has been sent to your registered email address`
4. Logon with your ID and temporary password.

   The Edit details screen is displayed where you can change your password.

5. Type and confirm your new password.
6. Click **Submit**.

Your new password is saved. When email is enabled, you can contact the System Administrator using the link on the logon screen.

Setting up email

To use the email function, a mail server must be installed and set up. By editing the **trc.properties** file, you can enable the email function by editing the following variables:

email.enabled
Set to true to enable email function.

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

smtp.authentication
Set to true if you want the SMTP server to authenticate with the smtp ID and password. Set to false if no authentication is required.

smtp.userid
User IDfor the SMTP server.

smtp.password
Password for the SMTP server.

Logging off from the IBM Endpoint Manager for Remote Control server

To log off from the IBM Endpoint Manager for Remote Control server UI, select **Sign Out**. The welcome screen is displayed.

Chapter 4. Unlocking user accounts

When a user account is locked you can unlock the account by using the **Unlock locked userid** feature.

When a user logs on to the IBM Endpoint Manager for Remote Control server with an incorrect password, their user account is locked if the number of failed logon attempts exceeds the value assigned to the **account.lockout** property in the trc.properties file. For more information about this property, see "trc.properties" on page 172.

To unlock the user account for one or more users, complete the following steps:

1. Choose the appropriate method to unlock users.
   a. To unlock users using the search utility.
      - Click **Users** > **Search**
      - The Search User screen is displayed
      - Enter the user information to be used in the search
      - Click **Submit**
      - Select the required user and go to step 2

   b. To unlock users using the All Users report
      - Click **Users** > **All users**.
      - The list of all defined users is displayed.
      - Select the required users.
2. Choose the appropriate action to unlock the users.
   - Click **Users** > **Unlock locked userid**.
   - Select **Unlock locked userid** from the Action list on the left.

The user account for the selected users is unlocked and they are able to make another logon attempt.

The following additional user information is also displayed on the Change details screen when you are editing user details, if the **account.lockout** property in the trc.properties file is enabled. For more information about editing user details, see "Modifying user details" on page 34.

Last failed logon
: Shows the date and time of the last failed logon attempt by this user.

Failed logons
: Shows the number of failed logons since the last successful logon or since the user's account was unlocked by an administrator.

Account locked
: Displays Yes or No depending on whether the user's account has been locked because they have reached the limit of consecutive failed logons defined by the **account.lockout** property in the trc.properties file.

Chapter 5. Managing targets and target groups

In the IBM Endpoint Manager for Remote Control system, targets are endpoints that you install the target software on. The target software identifies the computers to the IBM Endpoint Manager for Remote Control Server to receive connection requests, and pass information to and from the server. For more information about installing the target software, see the *IBM Endpoint Manager for Remote Control Installation Guide*.

The targets periodically report back to the IBM Endpoint Manager for Remote Control Server to let the server know that they are still active and, in particular, when their state changes. For example, when a user logs on, when a remote control session is taking place or when the system powers on or shuts down.

When a target is first installed and made known to the server it is automatically assigned to the default target group and given a default set of policies. You can decide which set of policies and permissions must be assigned to the target by making it a member of any relevant target groups. Target groups are created and assigned specific permissions that are combined with user group permissions to determine what the target users can do during remote control sessions.

Note: Only a user with Administrator authority sees the **Target Groups** menu.

Managing Targets

The following actions are available for Administrators to use on targets. For more information about the features that all users can use on targets, see the *IBM Endpoint Manager for Remote Control Console User's Guide*

Delete Target
Use this feature to delete one or more targets from the IBM Endpoint Manager for Remote Control Server

Manage Group Membership
Use this feature to add a target to a target group.

Deleting a target

You can remove targets from the IBM Endpoint Manager for Remote Control Server by using the **Delete target** option.

- If the target is still active and it has the IBM Endpoint Manager for Remote Control Target service running, it can report back to the server again and it's details are uploaded to the server, to be displayed in the All Targets list
- If it does report back, any policies or permissions that were set previously are reset and it is no longer a member of any previously assigned target groups

Removing the target software or stopping the **IBM Endpoint Manager for Remote Control - Target** service on the target prevents it from uploading details again.

To delete one or more targets complete the following steps:

1. Choose the appropriate method to delete targets:
   a. To delete a target by searching for targets, complete the following steps:
      1) Click **Targets** > **Search**

2) In the search field, enter information about the required target.
   `For example : serial number, computer name, model number, IP address`
3) Click **Submit**.
4) Select the required targets from the list and go to step 2

b. To delete a target using the All Targets report, complete the following steps:
1) Click **Targets** > **All targets**.
2) The list of all defined targets is displayed.
3) Select the required targets.

2. Choose the appropriate action to delete the target.
   - From the **Targets** menu select **Delete target**.
   - Select **Delete target** from the Actions list on the left.
3. On the **Confirm deletion screen** click **Submit**.

The targets are deleted. Use the **`delete.target.auth`** property in the `trc.properties` file to change the user authority required to carry out this action. For more information about this property, see Chapter 21, “Editing the properties files,” on page 171.

Assigning targets to target groups

When targets are registered in the server, they can then be assigned to target groups. The policies and permissions that are set for the groups are used to determine what the target members can or cannot do during a remote control session.

You can use the **Manage group membership** feature to add targets to target groups thus making them members of the selected groups. This action must be performed after a new target is made known to the server. For more information about creating target groups, see “Creating target groups” on page 22. For more information about how policies and permissions are granted for remote control sessions, see Chapter 8, “How policies are determined for a remote control session,” on page 63.

You can also assign targets to target groups by creating target membership rules. The rules can be used to automatically assign targets to specific groups when they contact the IBM Endpoint Manager for Remote Control server. For more information about target membership rules, see “Using rules to define target membership” on page 125.

Assigning a target to target groups

After a target has registered with the IBM Endpoint Manager for Remote Control Server you can assign it to one or more target groups. When the target takes part in a remote control session, the policies and permissions that are defined for these groups are considered when the final session policies are derived. For more information about how policies are set for a session, see Chapter 8, “How policies are determined for a remote control session,” on page 63.

To add a target to one or more target groups, complete the following steps:

1. Choose the appropriate step to select a target:
   a. Select by using the search utility
      1) Click **Targets** > **Search**
      2) In the search field, type in some specific or non-specific information about the targets.

```
For example :  serial number, computer name, model number, IP address
```

3) Click **Submit**
4) Select a target and go to step 2

b. Select by using the All targets report
   1) Click **Targets** >**All targets**. The list of all defined targets is displayed.
   2) Select a target.

2. Choose the appropriate way to select Manage Group Membership
   - Select **Targets** > **Manage Group Membership**.
   - Select **Manage Group Membership** from the Actions list on the left.

   The manage group membership screen is displayed listing all defined target groups and sub groups.
3. From the group list, select the target groups that the target will become a member of. Any groups with a + sign can be expanded to select sub groups also.

   Note: A target can be a member of multiple target Groups.
   To create target groups, see "Creating target groups" on page 22
4. Click **Submit**.

The target is now a member of the selected target groups.

Assigning multiple targets to target groups

You can assign multiple targets to target groups and also change their current group membership.

For example, targets used by the one department might need to be in the same target group. You can select all of these targets and assign them to the relevant target group or groups at the same time, which is more efficient than assigning each target individually.

Assign multiple targets to target groups by using one of the following options that can be used when you define the group tree hierarchy.

replace
The selected targets become members of the group or groups that you select within manage group membership. Their membership to any other groups is replaced by the target groups that are selected here.

For example: Target1 and target2 are members of targetgroup1 and targetgroup2. Select these targets from the target list and then select **Manage Group Membership**. From the list of groups that are displayed, select targetgroup3 and the replace option. Target1 and target2 are no longer members of targetgroup1 or targetgroup2 and are only members of targetgroup3.

add The selected targets are now also members of the group or groups that you select within manage group membership.

For example: In the example that is used in the replace option, if targetgroup3 is selected with the add option, target1 and target2 are now members of targetgroup1, targetgroup2, and targetgroup3.

delete The selected targets are removed from the groups that you select within manage group membership.

For example: Target1 and target2 are members of targetgroup1 and targetgroup2. Select these targets from the target list and then select **Manage Group Membership**. Select targetgroup2 from the group list in manage group membership along with the delete option. Target1 and target2 are still members of targetgroup1 but are no longer members of targetgroup2.

To assign multiple targets to one or more target groups, complete the following steps:

1. Choose the appropriate method for selecting a target
   a. Select by using the search utility
      - Select **Targets** > **Search**.
      - Type in some relevant information for retrieving the target data.
      - Click **Submit**.
      - Select the targets and then go to step 2.

      You can click **Reset** to clear the value that is entered in the search field.
   b. Select by using the All targets report.
      - Click **Targets** > **All targets**.
      - Select the relevant targets from the list.
2. Choose the appropriate way to select **Manage Group Membership**
   - Click **Targets** > **Manage Group Membership**.
   - Select **Manage Group Membership** from the Actions list on the left.

   The Manage User Group Membership screen is displayed listing all defined target groups and sub groups.
3. From the group list, select the relevant target groups. Any groups with a + sign can be expanded to select sub groups also.
4. Select one of the following options:
   - **replace current group membership**
   - **add to current group membership**
   - **delete from current group membership**
5. Click **Submit**.

The group membership for the multiple selected targets is defined by the option that is selected in step 4.

Creating target groups

Use target groups to assign similar policies and permissions to multiple targets. The policies are effective during remote control sessions.

For more information about starting remote control sessions, see the *IBM Endpoint Manager for Remote Control Installation Guide*. When a new target is defined in the IBM Endpoint Manager for Remote Control Server, it automatically becomes a member of the default target group, however the Administrator must assign the target to relevant target groups.

A target can be a member of multiple groups. Policies and permissions are defined for a target group when it is created. A permissions link **must** be created between the target group and a user group. The policies and permissions that are defined in the permission link and any other links that are defined in the group hierarchy, are

used to derive the set of policies for the session. For more information about deriving session policies, see Chapter 8, "How policies are determined for a remote control session," on page 63.

To create target groups, complete the following steps:

1. Click **Target Groups** > **New Target group**. The Edit Target Group screen is displayed. Use the screen to define the target group name and select the policies and permissions that are required for the target group.
2. Type in a name for the target group, for example, testtargets.
3. Type in an optional description for the target group.
4. For **Heartbeat interval**, type in the number of minutes that the target members of this group wait before they contact the IBM Endpoint Manager for Remote Control Server.
5. Use **Lock target on disconnect** to determine whether the target computers that belong to this target group are locked automatically when a remote control session ends.

   Set to Yes
   The target is locked when a remote control session with it ends.

   Set to No
   The target is not locked when a remote control session with it ends.
6. Select the value for **Automatically reset the console after a Remote Desktop console session:**

Value	Description
Never	Do not apply the workaround.
At session start	Reset the Windows session when a remote control session is started. **Note:** The Windows session takes a couple of minutes to initialize and the controller user sees a blank desktop until the initialization is complete.
After console is logged out	Reset the Windows session when the Remote Desktop user logs out.

   For more information about this attribute, see "Gray screen on a Windows 2003 system" on page 311.

   Note: The attribute is not set to any value by default.
7. Select the permission settings for the target group. The settings are classed as the standard or normal set for the group. On initial display, the screen shows the default values for the permissions that you can accept or change to your own requirements

   The Permission settings for the group can be defined in the following ways:
   - To **accept the given default** permission settings, click **Submit**.
   - To **assign an already defined set** of standard or normal permissions, select the template name from the pull-down
     – The Policy list is populated with the values saved for the selected permission set.
     – Click **Submit**.
   - To **define a new standard set** of permissions complete the following steps
     a. Click **Edit Settings**, the policy values are now available for selection.

b. For each Policy in the list select the required permission or enter a value

   Note: For more information about server policies, see Chapter 7, "Server session policies," on page 47.

   Yes The policy is valid for members of this target group and therefore its value is considered when the permissions are combining in Manage Permissions.

   No The policy is not valid for members of this target group but its value is also considered when the permissions are combined in Manage Permissions.

   Not Set
   No value is set and therefore it is not considered when the permissions are combined in Manage Permissions because this option is overridden by all others. For more information about how permissions are assigned, see Chapter 8, "How policies are determined for a remote control session," on page 63.

c. The new permissions set can be saved in the following ways:
   - **Save existing template**

     Select this option to save the changes to the template name that is displayed in the template list.
   - **Save as new template named**

     Select this option to save the changes to a new template.

d. Click **Submit**.

Viewing Target Groups

When target groups have been created, you can view a list of all defined groups. To view all target groups click **Target Groups** > **All target groups**.

The list of all defined Target Groups is displayed.

Managing Target Groups

When Target Groups have been created, there are various actions you can perform from the All Target Groups report.

Viewing the members of a target group
View a list of targets belonging to the selected group.

Deleting target groups
Delete the selected target groups.

Changing the details for a target group.
Edit the selected target groups details.

Removing members from a target group.

- Remove one or more selected members from a target group
- Remove All members from the selected target group

Setting permissions for a target group.
Define a relationship between a selected user group and target group that will determine what permissions they have during a remote control session.

Assigning target groups to other target groups.
Create a group hierarchy so that target groups can be made members of other target groups

Searching for target groups.
Search for a target group.

Viewing the members of a target group

You can see what targets have been assigned to a target group by using the List Members function.

To list all members of a selected target group, complete the following steps :

1. Choose the appropriate method for selecting all target groups
   a. Select using the search utility
      - Follow the steps in"Searching for target groups" on page 29 then return to here
      - Select the required target group then go to step 2
   b. Select using the All Target groups report
      - Click **Target groups** > **All target groups**.
      - The list of all defined target groups is displayed.
      - Select the required target group.
2. Choose the appropriate way to select List Members.
   - Select **Target Groups** > **List Members**
   - Select **List members** from the Action list on the left

The list of members for the selected target group is displayed, showing any target groups as well as targets that are members of the selected group.

Note:

1. Click **Cancel** from the List Members screen to return to the previously displayed screen

Deleting a target group

You can remove target groups that are no longer required by using the Delete target group function.

To delete one or more target groups, complete the following steps :

1. Choose the appropriate method for selecting the groups.
   a. Delete using the search utility
      - Follow the steps in "Searching for target groups" on page 29 to display the required target groups.
      - Select the required target groups then go to step 2
   b. Delete using the All Target groups report.
      - Click **Target groups** > **All Target groups**.
      - The list of all defined target groups is displayed.
      - Select the required target groups.
2. Choose the appropriate method for deleting the groups.
   - Select **Target Groups** > **Delete Group**.
   - Select**Delete Group** from the Action list on the left.

3. On the **Confirm deletion screen** click **Submit** .

The target groups are deleted.

Note: Click **Cancel** on the Confirm Deletion screen to return to the previously displayed screen and the target groups are not deleted.

Changing the details for a target group

After you have created a target group you can change the details or policies and values for the group by using the Edit Group function.

Note: It is important to note that if the policy values are changed for a group, the new policies will only be valid for this group when any **NEW** permissions links, between this target group and a user group, are created in manage permissions. For creating permissions links, see Chapter 8, "How policies are determined for a remote control session," on page 63. Any existing links already defined in manage permissions for this target group, will keep the policy values that were set for the group when the link was created.

To edit a target groups details, complete the following steps :

1. Choose the appropriate method for selecting the group.
   a. Select using the search utility
      - Follow the steps in "Searching for target groups" on page 29 for displaying the required groups.
      - Select the required Target Group then go to step 2.
   b. Select using the All Target groups report
      - Click **Target groups** > **All target groups**.
      - The list of all defined target groups is displayed.
      - Select the required target group.
2. Choose the appropriate method for selecting Edit Group.
   - Click **Target Groups** > **Edit Group**.
   - Select **Edit Group** from the Action list on the left.

   The Edit Target Group screen is displayed. For details of the requirements for this screen see "Creating target groups" on page 22.
3. Change the required information.
4. Click **Submit** .

The updated groups details are saved.

Note:

1. Click **Cancel** to return to the previously displayed screen.

Removing members from a target group

When targets or target groups have been assigned to target groups you can remove them from the group.

Removing members from a target group can be done in two ways

- Remove one member from a Target Group
- Remove All members from a Target group

Removing one member from a target group

To remove one member from a target group, complete the following steps :

1. To select the target that you want to remove from the target group, Choose the appropriate method for : -
   a. Select using the search utility.
      - Click **Targets** > **Search**
      - In the search field, type in some specific or non-specific information about the required target

        `for example : serial number, computer name, model number, IP address`
      - Click **Submit**.
      - Select the required target then go to step 2.
   b. Select using the All targets report
      - Click **Targets** > **All targets**.
      - The list of all defined targets is displayed.
      - Select the required target.
2. Choose the appropriate method for selecting Manage Group Membership.
   - Click **Targets** > **Manage Group Membership**.
   - Select **Manage Group Membership** from the Action list on the left.
3. Deselect the target group that you want to remove the target from.
4. Click **Submit**.

The target is no longer a member of the selected target group.

Note:

1. Click **Cancel** to return to the previously displayed screen and the target is still be a member of the selected target Group.
2. The above steps remove a target from a target group, the same steps would apply for removing a target group from a target group.

Note: You can confirm the removal by performing List Members on the selected target group. see “Viewing the members of a target group” on page 25. The selected target, is not displayed in the list.

Removing all members from a target group

To remove all members from a target Group, complete the following steps :

1. Choose the appropriate method for selecting the target group.
   a. Select using the search utility.
      - Follow the steps in “Searching for target groups” on page 29 to display the required target group.
      - Select the target group then go to step 2.
   b. Select using the All target groups report
      - Click **Target groups** > **All target groups**
      - The list of all defined target groups is displayed.
      - Select the required target group.
2. Choose the appropriate method for removing the members.
   - Select **Target Groups** > **Remove all members**.
   - Select **Remove all members** from the Action list on the left.
3. Press **Submit** to confirm.

All members are removed from the selected target group.

Note: You can confirm the removal by performing List Members on the selected target group. see "Viewing the members of a target group" on page 25. The members list should be empty.

Assigning target groups to other target groups.

Use the Manage Group Membership function to assign target groups to other target groups thus creating a group hierarchy. Target groups are assigned the permissions and policies of the direct target groups they are a member of and these are known as their standard or normal set of permissions. For more details of how policies and permissions are granted via the Policy Engine, see Chapter 8, "How policies are determined for a remote control session," on page 63.

To add target groups to target groups complete the following steps :

1. Choose the appropriate method for displaying the target groups.
   a. Select using the search utility
      1) To Search for a target group follow steps in "Searching for target groups" on page 29 to display the target groups.
      2) Select the required target group then go to step 2.
   b. Select using the All Target Groups report
      1) Click **Target Groups** > **All Target Groups**.
      2) The list of all defined target groups is displayed.
      3) Select the required target group.
2. Choose the appropriate method for selecting Manage Group Membership.
   - Click **Target Groups** > **Manage Group Membership**.
   - Select **Manage Group Membership** from the Actions list on the left.

   The manage Group Membership screen is displayed listing all defined target groups and sub groups.
3. From the group list select the required target groups that the selected target group should become a member of.

   Note:

   a. The group hierarchy can be created with target groups being members of target groups therefore some target groups in the list may have a plus sign in front of them which can be expanded. You can expand it to show the target group members of this target group. For details of how the group hierarchy is used, when determining the policies and permissions that are assigned when a remote control session is requested, see Chapter 8, "How policies are determined for a remote control session," on page 63
   b. A target group can be a member of multiple target groups. For creating target groups see "Creating target groups" on page 22
   c. You can assign multiple target groups to other target groups at the same time, see "Assigning multiple targets to target groups" on page 21 and follow this procedure selecting multiple target groups.
4. Click **Submit**.

The target group becomes a member of the selected target groups.

Note:

1. Click **Cancel** to return to the previously displayed screen and the target group is not assigned to the selected target groups.

Setting permissions for a target group

Use the manage permissions action to create a permissions link between a user group and a target group. This link defines the policies and permissions that are granted in a remote control session between user and target members of these groups. For details of this function and how the policies and permissions are determined for a remote control session, see Chapter 8, "How policies are determined for a remote control session," on page 63.

Searching for target groups

You can use the Search utility to access specific target groups or find a target group using non specific information. To search for a target group, complete the following steps :

1. Click **Target Groups** > **Search**. The Search Target Group screen is displayed.

   The input field is used to enter the target group information that is used in the search, this can be all or part of the target group name or description associated with the target group.

   - If the target group name is known, type this into the Search Target groups field for the quickest search.
   - If part of the name or description is known, for example if Test is part of the name, type this in.

2. Click **Submit**.

- If any matching target groups are found, the following information is displayed
  - If the target group name was entered, the details for that target group is displayed.
  - If non specific information was entered, a list of any target groups with this information as part of their details is displayed.

    Note: The information entered is not case sensitive - Test will also match on test
- If no matching target groups are found, a message is displayed and the target group list is blank.

Note:

1. Click **Reset** on the Search screen to clear values or return to previous values on the input screen.
2. Click **Cancel** on the Search screen to return to the previously displayed screen.
3. If nothing is entered in the input field and Submit is clicked, the list of all target groups is displayed.

Chapter 6. Managing users and user groups

IBM Endpoint Manager for Remote Control Server is designed to accommodate three types of user authorities: user, super user and administrator. A variety of IBM Endpoint Manager for Remote Control Server functions can be carried out by each user account type, with the administrator having the most comprehensive privileges.

User account authorities and the functions available to each account

Three types of user accounts can be created in the IBM Endpoint Manager for Remote Control server UI. The user accounts are user, super user, and administrator. The administrator account has the most authority. Administrators can do more advanced tasks. All types of authority can take part in remote control sessions, taking over and controlling target systems and are known as controller users. A user with administrator authority can also carry out Server admin functions and is known as a Server Admin User.

The following table illustrates each user account and highlights the authority that is given to each account.

User Account	Types of functions
User	The most limited account. A user with user authority can do the following actions: • Log on to the web application. • View all targets available for control. • Create or view lists of favorite targets. • Start a remote control session. • View target status or information. • View their own user and group details. • View information for – Sessions that they started. For example, session history, session details, recording details, audit logs. – Defined groups. – Recently accessed targets. • Search for targets.
SuperUser (User+)	Can do the same tasks as a user and also more advanced functions, such as generating specialized reports. A user with SuperUser authority can do the following extra actions: • Create and run various reports about users, sessions, targets, and server. However, a SuperUser is limited to viewing their own user details only. They are also limited to viewing the session details only for sessions that they started.

User Account	Types of functions
Administrator (User +, Super User+)	Can do the same tasks as a user and super user and also more advanced functions. Unlike the user and super user, they are not limited to just viewing their own details but can view details for all users. Also, responsible for maintaining and modifying user and target groups and for managing permissions that are granted to those groups. A user with administrator authority can do the following extra actions: • Edit and delete targets. • Create, delete, and manage users. • Create, delete, and manage user groups. • Create, delete, and manage target groups. • Create and run various reports on users, sessions, targets, and server. • Various types of data importing. For example, from LDAP or by using import templates • Property file editing. • Search for targets and users. • View the application log and server status.

Creating user accounts

To create a new user, complete the following steps:

1. Click **Users** > **New** The **Add User** screen is displayed.
2. Type in the relevant information for the new user.

   Note: The fields marked with a star are mandatory fields.

   User ID
   Type in a unique ID for the user.

   Email address
   Type in a valid email address for the user.

   Forename
   Type in a given name for the user.

   Surname
   Type in a surname for the user.

   Password
   Type in a unique password that conforms to your defined password rules and then retype the password for confirmation. Password rules are defined in the `trc.properties` file. For details, see "trc.properties" on page 172.
3. From the Authority list, select the authority level to assign to the new user. For more information about user account authorities, see "User account authorities and the functions available to each account" on page 31.
4. Select the groups that the new user is a member of.
5. Click **Submit**.

Note:

1. Click **Reset** to clear or change back to previous values any changes made to the input screen.

2. Click **Cancel** to return to the previous screen and the user is not created.

Viewing user accounts

When user accounts have been created, you can view the list of all user accounts.

To view all user accounts click **Users** > **All Users** .

The ***All Users*** screen is displayed listing all users defined in the system.

Managing user accounts

When user accounts have been created, you can manage these accounts and carry out various actions on them. These include the following actions.

Setting user account privileges
Edit a user details and change their user authority.

Modifying user details
Edit a users details.

Removing users
Deleting user accounts.

Unlocking user accounts
Unlocking user accounts that have been locked due to too many incorrect logon attempts.

Viewing a list of previous sessions established by a user
Viewing the session history list for a specific user.

Searching for users
Searching for one or multiple users.

Setting user account privileges

As an administrator you can set the authority for other user accounts. The types of privileges given to a user depends on the types of operations the user needs to accomplish. For information about the types of user accounts and the functions associated with each account, see "User account authorities and the functions available to each account" on page 31.

To set the authority level of a user account, complete the following steps :

1. Choose the appropriate method for displaying the user.
   a. To select the user using the search utility
      - Follow the steps in "Searching for users" on page 36 to display the required users.
      - Select the user then go to step 2

   b. To select the user using the All User report
      - Click **Users** > **All users**
      - The list of all defined users is displayed
      - Select the required user.
2. Choose the appropriate method for selecting Edit User.
   - Click **Users** > **Edit User**
   - Select **Edit User** from the Action list on the left

   The **Change Details** screen is displayed.

3. From the Authority pull down, select the authority level to assign to the account.
4. Click **Submit**.

Note:

1. Click **Reset** to clear or change back to previous values, any changes made to the input screen
2. Click **Cancel** to return to the previously displayed screen

Modifying user details

After a user has been created you can modify the users details. You can do this by selecting the user from the All Users Report or by using the search utility, then using the Edit user function to make the required changes. If there are many users defined in the system, using the search utility will provide a quicker route to the required user.

To modify a users details, complete the following steps :

1. Choose the appropriate method for displaying the user.
   a. To modify using the search utility
      - Follow the steps in "Searching for users" on page 36 to display the required user.
      - Select the user then go to step 2
   b. To modify using the All User report
      - Click **Users** > **All users**.
      - The list of all defined users is displayed.
      - Select the required user.
2. Choose the appropriate method for selecting Edit User.
   - Click **Users** > **Edit User**.
   - Select **Edit User** from the Action list on the left.

   The Edit User screen is displayed.
3. Change the relevant information For details of the requirements for the Edit Details screen, see "Creating user accounts" on page 32. The following additional user information is also displayed if the **account.lockout** property in the trc.properties file is enabled.

   Last failed logon
   Shows the date and time of the last failed logon attempt by this user.

   Failed logons
   Shows the number of failed logon attempts made by the user.

   Note: If this user account has been locked previously due to the number of allowed failed logon attempts being exceeded, the number shown for failed logons denotes the number of failed attempts since the last time the account was unlocked.

   Account locked
   Displays Yes or No depending on whether the users account has been locked because they have reached the limit of consecutive failed logons defined by the **account.lockout** property in the trc.properties file.

   Note: The User ID is unique and therefore cannot be changed.

4. Click **Submit**

Note:

1. Click **Reset** to clear or change back to previous values any changes made to the input screen
2. Click **Cancel** to return to the previously displayed screen

Removing users

After users have been created you can remove them if they are no longer required. Use the Delete user function to remove them. If there are many users defined in the system, using the search utility will provide a quicker route to the required users.

To remove one or more users, complete the following steps :

1. Choose the appropriate method for displaying the users.
   a. To remove users using the search utility
      - Follow the steps in "Searching for users" on page 36 to display the required users.
      - Select the users then go to step 2
   b. To remove users using the All Users report
      - Click **Users** > **All users**.
      - The list of all defined users is displayed.
      - Select the required users.
2. Choose the appropriate method for deleting the users.
   - Click **Users** > **Delete User**.
   - Select **Delete User** from the Action list on the left.
3. On the **Confirm deletion screen** click **Submit** .

The users are deleted.

Note: Click Cancel on the Confirm deletion screen to return to the previously displayed screen and the users are not deleted.

Unlocking user accounts

When a user logs on to IBM Endpoint Manager for Remote Control with an incorrect password their user account is locked if the number of failed logon attempts exceeds the value assigned to the **account.lockout** property in the `trc.properties` file. For more details of this property, see "trc.properties" on page 172. Once the user account is locked you can unlock the account by using the **Unlock locked userid** function.

To unlock the user account for one or more users, complete the following steps :

1. Choose the appropriate method for displaying the users.
   a. To unlock users using the search utility
      - Follow the steps in "Searching for users" on page 36 for diaplying the required users.
      - Select the required user then go to step 2 on page 36
   b. To unlock users using the All Users report
      - Click **Users** > **All users**.
      - The list of all defined users is displayed.

- Select the required users.

2. Choose the appropriate method for unlocking the user account.
   - Click **Users** > **Unlock locked userid**.
   - Select **Unlock locked userid** from the Action list on the left.

The user account for the selected users are unlocked and they are able make a new logon attempt.

Viewing a list of previous sessions established by a user

You can view a list of all previous sessions that one or more selected users has taken part in using the Session history function.

To view a list of previously established sessions by specific users, complete the following steps :

1. Choose the appropriate method for displaying the users.
   a. To select a user using the search utility
      - Follow the steps in "Searching for users" to display the required users.
      - Select the required user then go to step 2.
   b. To select a user or users using the All Users report
      - Click **Users** > **All users**.
      - The list of all defined users is displayed.
      - Select the required users.
2. Choose the appropriate method for viewing the session history.
   - Click **Users** > **Session history**.
   - Select **Session history** from the Action list on the left.

The Session History screen is displayed listing the sessions that have been started by the selected users, with the most recent session first in the list.

Searching for users

You can use search for users and view a summary list in the search results. To search for a user, complete the following steps.

1. Click **Users** > **Search**.
2. The Search User screen is displayed
3. The input field is used to enter the user information to be used in the search.
   - Type the users's email address in the **Search Users** field for the quickest search.
   - You can type all or part of the name or any other detail that is known.
4. Click **Submit**.

- Any users that match the search criteria are shown. To view the details for any of the users, click their name in the search results.
  – If the email address was entered, the summary details for that user are shown.
  – If non-specific information was entered, a list of any users with this information as part of their details is displayed. For example, if you typed Scot, a list of users with Scot somewhere in their details is listed.

```
Users with Forename - Scot
           Email - ascot@example.com
```

Note: The information that is entered is not case-sensitive. Scot can also match with scot.

- If no matching users are found, a message is displayed and the user list is blank

Note:

1. Click **Reset** on the Search screen to clear or change back to previous values, any changes that are made to the input screen
2. Click **Cancel** on the Search screen to return to the previous screen.

Creating user groups

You can create groups of users in IBM Endpoint Manager for Remote Control Server. User groups are used for grouping together users who will have the same permissions and access during a IBM Endpoint Manager for Remote Control , remote control session. For details of establishing and performing remote control sessions, see the IBM Endpoint Manager for Remote Control Controller User's Guide .

When a new user is defined in IBM Endpoint Manager for Remote Control Server they automatically become a member of the DefaultGroup. You can also assign the user to other user groups.

Note:

1. A user can be a member of multiple groups.
2. It is important to note that, although policies and permissions are defined for the user group when it is created, this is not the set of policies that is applied in a remote control session between members of this user group and members of a target group. A permissions link **MUST** be created between the user group and a target group and it is the policies and permissions defined in this link, as well as any other links defined in the group hierarchy, that are used to derive the set of policies for the session. For more details, see Chapter 8, “How policies are determined for a remote control session,” on page 63.

To create a user group complete the following steps :

1. Click **User Groups** > **New User group** The **Edit User Group** screen is displayed. This screen is used to define the user group name and select the policies and permissions required for the user group.
2. Type in a name for the user group.
3. Type in an optional description for the user group.
4. Select the required permission settings for the user group. These settings are classed as the standard or normal set for the group. The default or shipped values for the permissions are displayed and you can accept or change these to your own requirements.

   You can define the Permission settings for a group in one of three ways.

   a. To **accept the given default** permission settings click **Submit**.
   b. To **assign an already defined set** of standard or normal permissions, select the template name from the pull down.
      - The Policy list is populated with the values saved for the selected permission set.
      - Click **Submit**.
   c. To **define a new standard set** of permissions :
      1) Click **Edit Settings**, the policy values are now available for selection.

2) For each Policy in the list select the required permission or enter a value.

   Note: For definitions and default and possible values for these policies, seeChapter 7, “Server session policies,” on page 47.

   Yes This policy is valid for members of this user group and therefore its value is considered when combining the permissions in Manage Permissions.

   No This policy will not be valid for members of this user group but its value will also be considered when combining the permissions in Manage Permissions.

   Not Set
   No value is set and therefore it is not considered when combining the permissions in Manage Permissions as this option is overridden by all others. For details of how permissions are assigned, see Chapter 8, “How policies are determined for a remote control session,” on page 63.

3) The new permissions set can be saved in one of two ways
   - **Save existing template**

     Select this option if you want to save the changes made to the template name that is displayed in the template list.
   - **Save as new template named**

     Select this option if you want to save the changes made to a new template. Enter a name for the new template.

4) Click **Submit**.

Note:

1) Click **Cancel** to return to the previously displayed screen and the user group is not created.

Assigning users to groups

When user groups have been created, you can add users to these groups. This can be done in a number of ways.

- Assigning the user to a group when the user account is being created.
- Selecting one or more users then using the Manage Group Membership action.

Assigning at user account creation

When you are creating a new user, a list of all user groups is displayed on the Add user screen and you can select the groups that the new user has to be made a member of. For more details of creating users, see “Creating user accounts” on page 32.

Assigning one user to one or more user groups

To add a user to one or more user groups complete the following steps :

1. Choose the appropriate method for displaying the user.
   a. Select using the search utility.
      - Follow the steps in “Searching for users” on page 36 to display the required user.
      - Select the user then go to step 2 on page 39.

b. Select using the All Users report
   - Click **Users** > **All users**.
   - The list of all defined users is displayed.
   - Select the required user.

2. Choose the appropriate method for selecting **Manage Group Membership**.
   - From the Users menu select **Manage Group Membership.**
   - Select **Manage Group Membership** from the Actions list on the left.

   The **Manage User Group Membership** screen is displayed displaying all defined user groups and sub groups.
3. From the group list select the required user groups that the user has to be assigned to. Any groups with a + sign can be expanded to select sub groups also.
4. Click **Submit**.

The user is a member of the selected groups.

Note:

1. Click **Cancel** to return to the previously displayed screen.

Assigning multiple users to user groups

As well as assigning one user to one or more user groups you can also assign multiple users to user groups.

```
Users working in the same department may need to be in the same user
group. You can select all of these users together then assign them to
the relevant user group or groups at once, which is more efficient and
less time consuming than assigning each user individually.
```

Do this by using one of the three following options when defining the group tree hierarchy.

replace
The selected users become members of the groups you select within manage group membership. Their membership to any other groups is replaced by the user groups that are selected here.

```
For example:  user1 and user2 are members of usergroup1 and usergroup2.
 Select the users from the user list and then select manage group
 membership is selected. From the list of groups that are displayed,
 select usergroup3 and the replace option. user1 and user2 are no longer
 members of usergroup1 or usergroup2 and are only members of usergroup3.
```

add The selected users are now also members of the groups that you select within manage group membership.

```
For example:  in the example used in the replace option, if usergroup3
 is selected with the add option, user1 and user2 are now
members of usergroup1, usergroup2 and usergroup3.
```

delete The selected users are removed from the groups that you select within manage group membership.

```
For example: user1 and user2 are members of usergroup1 and usergroup2.
Selected these users from the user list, then select manage group
membership is selected. usergroup2 is selected from the group list
within manage group membership along with the delete option. user1
and user2 are still members of usergroup1 but are no longer members
of usergroup2.
```

To assign multiple users to one or more user groups complete the following steps :

1. Choose the appropriate method for selecting multiple users
   a. Select using the search utility
      - Select **Users** > **Search**.
      - Type in some relevant information for retrieving the user data.
      - Click **Submit**.
      - Select the required users then go to step 2.

      Note:
      1) Click **Reset** to clear the value entered into the search field.
      2) Click **Cancel** to return to the previously displayed screen and the search is not performed.

   b. Select using the All users report.
      - Click **Users** > **All users**.
      - Select the required users from the list.
2. Choose the appropriate method for selecting **Manage Group Membership**
   - Click **Users** > **Manage Group Membership**.
   - Select **Manage Group Membership** from the Actions list on the left.

   The Manage User Group Membership screen is displayed listing all defined user groups and sub groups.
3. From the group list select the required user groups. Any groups with a + sign can be expanded to select sub groups also.
4. Select one of the following options :-
   - **replace full group membership**
   - **add to current group membership**
   - **delete from current group membership**
5. Click **Submit**.

The group membership for the multiple users is defined by the option selected in step 4.

Viewing user groups

When user groups have been created you can view a list of all groups.

To view all user groups click **User Groups** > **All User groups**.

The All User Groups screen is displayed.

Managing user groups

When user groups have been created, you can manage these groups and carry out various actions on them.

Viewing the members of a user group
View a list of Users belonging to the selected Group

Deleting user groups
Delete the selected user Groups

Changing the details for a user group.
Edit the selected user groups details

Removing members from a user group.

- Remove one or more selected members from a user group.
- Remove All members from the selected user group.

Setting permissions for a user group.
Define a relationship between a selected user group and target group to determine the permissions they have during a remote control session.

Assigning user groups to other user groups.
Create a group hierarchy by assigning user groups to other user groups.

Searching for user groups.
Search for user groups

Viewing the members of a user group

Use the List Members function to view a list of users and users groups that are members of a specific user group.

To list all members of a selected user group, complete the following steps :

1. Choose the appropriate method for displaying the user group
   a. Select using the search utility.
      - Follow the steps in "Searching for user groups" on page 45 to display the user group.
      - Select the required user group then go to step 2

   b. Select using the All User Groups report
      - Click **User groups** > **All User Groups**.
      - The list of all defined user groups is displayed.
      - Select the required user group.
2. Choose the appropriate method for listing the group members.
   - Click **User Groups** > **List Members**
   - Select **List members** from the Action list on the left.

The list of members for the selected user group is displayed showing any user groups as well as users that are members of the selected group.

Note:

1. Click **Cancel** from the List Members screen to return to the previously displayed screen.

Deleting user groups

To delete one or more user groups, complete the following steps :

1. Choose the appropriate method for displaying the user groups.
   a. Delete using the search utility.
      - Follow the steps in "Searching for user groups" on page 45 to display the user groups.
      - Select the required user groups then go to step 2

   b. Delete using the All User groups report
      - Click **User groups** > **All user groups**.
      - The list of all defined user groups is displayed.
      - Select the required user groups.
2. Choose the appropriate method for deleting the user groups.
   - Click **User Groups** > **Delete User group**.

- Select **Delete User group** from the Action list on the left.

3. On the Confirm deletion screen click **Submit** .

The user groups are deleted.

Note: Click **Cancel** on the Confirm Deletion screen to return the application to the previously displayed screen and the user groups are not deleted.

Changing the details for a user group

You can use the Edit Group function to edit the details or policies and values for the selected user group.

Note: It is important to note that if the policy values are changed for a group, the new policies will only be valid for this group when any **NEW** permissions links, between this user group and a target group, are created in manage permissions. For creating permissions links, see Chapter 8, "How policies are determined for a remote control session," on page 63. Any existing links already defined in manage permissions for this user group, will keep the policy values that were set for the group when the link was created.

To edit a user groups details, complete the following steps :

1. Choose the appropriate method for selecting the user group.
   a. Select using the search utility.
      - Follow the steps in "Searching for user groups" on page 45 to display the user group.
      - Select the required user group then go to step 2

   b. Select using the All User groups report.
      - Click **User groups** > **All user groups**.
      - The list of all defined user groups is displayed.
      - Select the required user group.

2. Choose the appropriate method for editing the group.
   - From the **User Groups** > **Edit Group**.
   - Select**Edit Group** from the Action list on the left.

   The Edit User Group screen is displayed. For details of the requirements for this screen see "Creating user groups" on page 37.

3. Change the required information.
4. Click **Submit** .

Note:

1. Click **Cancel** to return to the previously displayed screen

Removing members from a user group

When users or user groups have been assigned to user groups you can also remove them from the group.

Removing members from a user group can be done in two ways

- Remove one member from a user group.
- Remove all members from a user group.

Removing one member from a user group

To remove one member from a user group, complete the following steps :

1. Choose the appropriate method for selecting a user.
   a. Select using the search utility (may provide a quicker route)
      1) Follow the steps in "Searching for users" on page 36 to display the user.
      2) Select the required user then go to step 2.
   b. Select using the All User report
      1) Click **Users** > **All users**.
      2) The list of all defined users is displayed.
      3) Select the required user.
2. Choose the appropriate method for selecting **Manage Group Membership**.
   - Click **Users** > **Manage Group Membership**.
   - Select **Manage Group Membership** from the Action list on the left.
3. Deselect the user group that you want to remove the user from.
4. Click **Submit**

The user is no longer a member of the selected user group.

Note:

1. Click **Cancel** to return to the previously displayed screen and the user remains a member of the selected user group.

Note: Use the List Members function on the selected user group to confirm the removal. For more details, see "Viewing the members of a user group" on page 41.

Remove all members from a user group

To remove all members from a user group, complete the following steps :

1. Choose the appropriate method for selecting a user group :
   a. Select using the search utility
      - Follow the steps in "Searching for user groups" on page 45 to display the user groups.
      - Select the required user group then go to step 2
   b. Select using the All User groups report
      - Click **User groups** > **All user groups**.
      - The list of all defined user groups is displayed.
      - Select the required user group.
2. Choose the appropriate method for removing all members.
   - Click **User Groups** > **Remove all members**.
   - Select **Remove all members** from the Action list on the left
3. Press **Submit** to confirm.

All members are removed from the selected user group.

Note: Use the List Members function on the selected user group to confirm the removal. For more details, see "Viewing the members of a user group" on page 41.

Assigning user groups to other user groups

Use the **Manage Group Membership** function to make user groups members of other user groups to create a group hierarchy. User groups are assigned the

permissions and policies of the user groups they are a member of and these are known as the standard or normal set of permissions. For more details of how policies and permissions are granted, see Chapter 8, “How policies are determined for a remote control session,” on page 63.

To add user groups to user groups complete the following steps :

1. Choose the appropriate method for displaying the user group.
   a. Select using the search utility.
      1) To search for a user group follow steps in item “Searching for user groups” on page 45 to display the group.
      2) Select the required user group then go to step 2
   b. Select using the All User Groups report.
      1) Click **User Groups** > **All User Groups**.
      2) The list of all defined user groups is displayed.
      3) Select the required user group.
2. Choose the appropriate method for selecting Manage Group Membership.
   - Select **User Groups** > **Manage Group Membership**.
   - Select **Manage Group Membership** from the Actions list on the left.

   The Manage Group Membership screen is displayed listing all defined user groups and sub groups.
3. From the group list select the required user groups that the selected user groups will become a member of.

   Note:

   a. A group hierarchy can be created with user groups being members of user groups. Some user groups in the list might have a plus sign next to their name. Click the group names to show its user group members. For details of how the group hierarchy is used when determining the policies and permissions that are assigned when a remote control session is requested, see Chapter 8, “How policies are determined for a remote control session,” on page 63.
   b. A user group can be a member of multiple user groups. For creating user groups, see “Creating user groups” on page 37.
   c. Multiple user groups can be assigned to user groups at the same time.
4. Click **Submit**.

The user group is now a member of the selected user groups.

Note:

1. Click **Cancel** on the Manage Group Membership screen to return to the previously displayed screen. The user group is not assigned to the selected user groups.

Setting permissions for a user group

Use the Manage Permissions function to create a permissions link between a user group and a target group. This link is used to define the policies and permissions that are granted in a remote control session between user and target members of these groups. For details of this function and how the policies and permissions are determined for a remote control session, seeChapter 8, “How policies are determined for a remote control session,” on page 63.

Searching for user groups

You can use the Search utility to find specific user groups or find a user group using non specific information. To search for a user group, complete the following steps :

1. Click **User Groups** > **Search**. The Search User Group screen is displayed.

   Enter the user group information to be used in the search, this can be all or part of the user group name or description associated with the user group.

   - If the user group name is known, type this into the Search User groups field for the quickest search
   - If part of the name or description is known, for example if Test is part of the name, type this in

2. Click **Submit**

- If any matching user groups are found, the following is displayed
  - If the user group name was entered, the details for that target group is displayed
  - If non specific information was entered, a list of any user groups with this information as part of their details is displayed.

    Note: The information entered is not case sensitive - Test will also match on test
- If no matching user groups are found, a message is displayed and the user group list is blank

Note:

1. Click **Reset** on the Search screen to change the input screen values back to their previous values.
2. Click **Cancel** on the Search screen to return to the previously displayed screen.
3. If nothing is entered in the input field and Submit is clicked, the list of all user Groups is displayed

Chapter 7. Server session policies

You can configure the following session policies on the IBM Endpoint Manager for Remote Control Server to determine what actions and features are available during a remote control session. The policies can be configured initially when you create a user or target group. However, the permission links set up between the user and target groups determine what policies and permissions are finally derived for the session.

For more information about groups and policies, see the following sections.

- "Creating user groups" on page 37
- "Creating target groups" on page 22
- Chapter 8, "How policies are determined for a remote control session," on page 63

Policy list definitions

Security policies

Reboot

To send a restart request to the target computer so that it can be restarted remotely. Determines whether **Reboot** is available as a session mode option on the start session screen. For more information about session types, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes

Reboot is shown as an option on the start session screen.

Set to No

Reboot is not shown as an option on the start session screen.

Allow multiple Controllers

To enable collaboration so that multiple controllers can join a session. Determines the availability of the collaboration option on the controller window. For more information about collaboration sessions that involve multiple participants, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes

The collaboration icon is available for selection in the controller window.

Set to No

The collaboration icon is not active in the controller window.

Allow local recording

To make and save a local recording of the session in the controlling system. Determines the availability of the record option on the controller window. For more information about recording sessions, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes

The record option is available for selection in the controller window.

Set to No

The record option is not active in the controller window.

Set target locked

Determines whether the local input and display is locked for all sessions. Therefore, the target user cannot use the mouse or keyboard on the target while in a remote control session.

Set to Yes

The target screen is blanked out when the session is started, preventing the target user from interacting with the screen while in the session. The target desktop is still visible to the controller user in the controller window.

Set to No

The target screen is not blanked out when the session is started and the target user is able to interact with the screen.

Allow input lock

Determines whether the 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.

Set to Yes

The Enable Privacy option is available in the **Perform Action in target** menu in the controller window. For more details of the controller window functions, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to No

The Enable Privacy option is not available in the **Perform Action in target** menu in the controller window.

Connect at Logon

Determines whether a session can be started when no users are logged on at the target.

Set to Yes

Session is established with the target.

Set to No

Session is not established and a message is displayed.

Use Encryption

Determines whether to encrypt the data that is being transmitted.

Disable Panic Key

Determines whether the Pause Break key can be used by the target user to automatically end the remote control session.

Set to Yes

The target user cannot use the Pause Break key to automatically end the remote control session.

Set to No

The target user can use the Pause Break key to automatically end the remote control session.

Enable On-screen Session Notification

Determines whether a semi-transparent overlay is shown on the target computer to indicate that a remote control session is in progress. Use this policy when privacy is a concern so that the target user is clearly notified when somebody is remotely viewing or controlling their computer.

Set to Yes

The semi-transparent overlay is shown on the target screen with

the text **IBM Endpoint Manager for Remote Control**. The type of remote control session that is in progress is also displayed. The overlay does not intercept keyboard or mouse actions, therefore the user is still able to interact with their screen.

Set to No
The overlay is not shown on the target computer.

Note: This policy is only supported on targets that have a Windows operating system installed.

Allow input lock with visible screen
This property works along with **Allow input lock** and on its own. Use **Allow input lock with visible screen** to lock the target users mouse and keyboard during a remote control session.

Set to Yes

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.

Set to No

The lock target input menu item is not enabled in the **Perform action in target** menu in the controller window.

Note: If Enable Privacy is selected, during a session, the remote user input is automatically locked. It is not possible to enable privacy without also locking the input.

Display screen on locked target
Works along with **Set target locked**, which you can use to enable privacy mode at session startup. You can use **`Display screen on locked target`** to determine whether the target user can view their screen or not during a remote control session, when privacy mode is enabled.

Set to Yes

In privacy mode, the target screen is visible to the target user during the session, but their mouse and keyboard control is locked.

Set to No

In privacy mode, the target screen is not visible to the target user and the privacy bitmap is displayed during the session. The target users mouse and keyboard input is also disabled.

Note: For **`Display screen on locked target`** to take effect set **`Set target locked`** to Yes.

Denied Program Execution List
To specify a list of programs that a controller user cannot run on the target during an active session with the target. These programs must be entered as a comma-separated list. The following points must be noted.

Note:

1. This feature works only on the following operating systems
   - Windows 2000, all editions
   - Windows XP, 32-bit editions only

- Windows Server 2003, 32-bit editions only

2. The programs can be entered with or without a path defined.

   ```
   For example
   c:\notepad.exe or notepad.exe are both acceptable.
   ```

3. Any program with a space in its name must be enclosed in double quotation marks.

   ```
   my prog.exe should be entered as "my prog.exe"
   ```

4. If you enter any of the IBM Endpoint Manager for Remote Control specific programs in the list, for example `trc_dsp`, `trc_base` or `trc_gui`, they are ignored.
5. If any of the programs that are listed are already running on the target when the session is started, they continue to run. However, any new instances of the program are not started.

Inactivity timeout

Number of seconds to wait until the connection ends if there is no session activity. Set this value to 0 to disable the timer so that the session does not end automatically. The minimum timeout value is 60 seconds. Therefore, a value >0 and <60 times out automatically at 60 seconds and values >60 timeout when the value is reached. The default value is 0.

Note: Set the value to 0 for sessions that do not involve sending or receiving information from the controller to the target. For example in Monitor sessions.

Auditing

Force session recording

All sessions are recorded and the session recordings are uploaded and saved to the server.

Set to Yes

A recording of the session is saved to the server when the session ends. A link for playing the recording is also available on the session details screen.

Set to No

No recording is stored and therefore no link is available on the session details screen.

Local Audit

Use to create a log of auditable events that take place during the remote control session. The log is created on both the controller and target computer.

Set to Yes

The `trcaudit` log file is created and stored on the controller computer in the home directory of the currently logged on user.

The log can be viewed on a Windows target computer by using the event viewer. To access the Application Event Viewer click **Start** > **Control Panel** > **Administrative Tools** > **Event Viewer** > **Application**. On a Linux target, the events are stored in the messages file that is in the `/var/log` directory.

Set to No

No log is created or stored on the controller or target computer.

Force session audit

A log of auditable events is automatically stored on the server. Determines the visibility of these events on the session details screen.

Set to Yes

Controller and target events that took place during the session are displayed on the session details screen.

Set to No

Controller and target events are not displayed on the session details screen.

Keep session recording in the target system

Determines whether a copy of the session recording that was done on the target and successfully uploaded to the IBM Endpoint Manager for Remote Control Server is also saved on the target system. The location of the saved recording is determined by the location that is set in the target property **RecordingDir**.

Note: This policy is only valid if **Record the session in the target system** is set to Yes.

Set to Yes

If **Record the session in the target system** is set to Yes and the session recording is successfully uploaded to the IBM Endpoint Manager for Remote Control Server, a copy of the recording is also saved on the target system.

Set to No

If **Record the session in the target system** is set to Yes and the session is recorded, a copy of the recording is not saved on the target system.

Record the session in the target system

Determines whether the session recording is done on the target system instead of the controller, when the **Force session recording** policy is also set to Yes.

Set to Yes

The session is recorded on the target and uploaded to the IBM Endpoint Manager for Remote Control Server.

Note: If **Force session recording** is set to **No**, session recording is not performed.

Set to No

The session is recorded on the controller and uploaded to the IBM Endpoint Manager for Remote Control Server.

Control

Enable true color

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**.

Set to Yes

The target desktop is displayed in true color 24-bit mode at the start of the session.

Set to No
The target desktop is displayed in 8-bit color mode at the start of the session. This value is the default value.

Allow registry key lookup
Determines the availability of the Enter key item in the **Registry keys** menu on the controller window, during a guidance and active session.

Set to Yes
The **Enter key** option is available in the **Registry keys** menu. Use the Enter key option to enter a registry key and lookup the value that is defined for it on the target. For more information about the **Registry keys** menu, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to No
The Enter key option is not available and the controller user cannot find out the values of the targets registry keys.

View registry key list
Determines the availability of the defined registry keys list in the **Registry keys** menu on the controller window.

Set to Yes
The list of up to 10 registry keys, which can be defined in the `trc.properties` file, is visible in the **Registry keys** menu. The controller user can select one to view the value for it on the target. For more information about editing the properties files, see Chapter 21, “Editing the properties files,” on page 171.

Note: If you set this policy to Yes, you must make sure that you define registry keys in the `trc.properties` file. Otherwise, if you click the menu item, nothing is shown.

Set to No
The defined list of registry keys is not visible in the **Registry keys** menu.

Enable user acceptance for system information
Use this policy to display the user acceptance window on the target computer when the controller user selects to view the target system information.

Set to Yes
When the controller user clicks 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. If the target user clicks accept, the target system information is displayed in a separate window on the controller system. If they click refuse, a message is displayed on the controller and the system information is not displayed.

Set to No
The target system information is displayed automatically when the controller user clicks the system information icon.

Enable user acceptance for file transfers
Use this policy to display the user acceptance window on the target computer when the controller user wants to transfer a file from the target to the controller system.

Set to Yes

The acceptance window is displayed in the following two cases. The target user must 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 accept the request.
- If the controller user selects **send file to controller** from the **Actions** menu in the target window

Set to No

The acceptance window is not displayed and files are transferred automatically from the target to the controller system when requested.

Enable user acceptance for mode changes

Use this policy to display the user acceptance window on the target computer when the controller user selects a different session mode.

Set to Yes

The user acceptance window is displayed each time the controller user selects a new session mode. The target user must accept or refuse the request.

Set to No

The user acceptance window is not displayed and the session mode is changed automatically.

Enable user acceptance for incoming connections

Use this policy to display the user acceptance window on the target computer when a remote control session is requested. The target user must accept or refuse the session.

Note: This policy works along with **`Acceptance Grace Time`** and **`Acceptance timeout action`**.

Set to Yes

The acceptance window is displayed and the target user has the number of seconds defined for **`Acceptance Grace time`** to accept or refuse the session.

Note:

1. The target user can also select a different session mode on the User Acceptance window.
2. The target user can hide any running applications by choosing the **Hide applications** option on the acceptance window. For more information about hiding applications, see the IBM Endpoint Manager for Remote Control Controller User's Guide.
3. When set to Yes, the Acceptance Grace time must be > 0 to give the target user time to accept or refuse the session

Accept

The session is established.

Refuse

The session is not started and a message is displayed.

Set to No
The session is started automatically and the User Acceptance window is not displayed on the target.

Run post-session script

Determines whether a user-defined script is run after the remote control session finishes.

Set to Yes
When a remote control session ends, the user-defined script is run. The following must be done to set up the script (see Run pre-session script for details of defining scripts).

The script must be given the following name.

```
post_script. {ext}
```

Where {ext} is **.cmd** on a Windowssystem and **.sh** in UNIX or Linux systems.

The script must be placed in the following directory on the target.

Windows systems
```
\%SYSTEMROOT%\scripts
```

Where *SYSTEMROOT* is the relevant Windows operating system directory.

UNIX or Linux systems
```
/etc/scripts
```

Note: This directory must be owned by root and have the permissions 700 so that root can read, write or execute. All other users must have no permissions, otherwise the script will not run and it fails. The success or failure of the execution of this script is logged by the target into the audit log.

Set to No
No script is run after the session.

Run pre-session script

Determines whether a user-defined script is run before the remote control session starts. The script is run just after the session is allowed but before the controller user has access to the target. This policy is connected to **Pre-script fail operation**. The outcome of running the script and the continuation of the session is determined by the value that is set for**Pre-script fail operation**.

Set to Yes
When a Remote Control Session is requested the defined script is run before the Controller user has access to the target.

Defining Pre and Post scripts

The script development is free from any constraint, except for the need to allow their unattended execution and to use exit codes that can be correctly interpreted by IBM Endpoint Manager for Remote Control. Pre-scripts and post-scripts are supported on the following operating systems.

- Windows (XP, 2003, Vista, 7)
- Linux (SLES, RHLE)

When you develop scripts, you must adhere to the following rules:

- Define the scripts as batch files on a Windows system (with extension `.cmd`) and as shell files on a Linux system (with extension `.sh`).
- On Windows systems , the scripts must be named `pre_script.cmd` and `post_script.cmd`. On Linux systems they must be named `pre_script.sh` and `post_script.sh`.
- Copy the scripts into a directory that is called `scripts` that is in the installation directory of the IBM Endpoint Manager for Remote Control target. Make sure that they are executable just by root to avoid security exposures in Linux.

  Note: This directory must be owned by root and have the permissions 700 so that root can read, write or execute. All other users must have no permissions, otherwise the script will not run and it fails. The success or failure of the execution of this script is logged by the target into the audit log.
- The pre-script and post-scripts are run with system privileges and without validation to protect them from unauthorized access.

  Note: The installer creates the script directory with access just for administrators and **`localsystem`** on a Windows system and for read/write/execute just for root on a Linux system.
- Ensure that the scripts end within 3 minutes. If they run for longer, they cannot return a valid execution code. The administrator at the controller is notified that the timeout elapsed and an error occurred. The execution code indicates whether the script did run.
- Define a non-negative (greater than or equal to 0) exit code for the script to indicate that the script ran with success and a negative exit code to indicate that it ran with errors. Whenever an error occurs a message is reported to the controller. The exit code is shown and session fails to start.

Environment Variables

You can use the following environment variables in the pre-script and post-script.

RC_TIVOLI_ADMIN_NAME= Tivoli_administrator_name
Where Tivoli_administrator_name specifies the Tivoli® administrator name on the controller as provided by the server.

RC_TIVOLI_ADMIN_LOGIN = Tivoli_administrator_name
Where Tivoli_administrator_name specifies the Tivoli administrator name on the controller as provided by the server.

RC_ACTION= action
Where action specifies the following actions:

0 No actions

1 Remote Control (Active, Guidance or Monitor)

2 File Transfer

3 Chat

4 Reboot

RC_GRACE_PERIOD= duration
Where duration specifies the number of seconds to wait for the target user to respond before an activity starts or times out.

RC_PROCEED_IF_TIMEOUT= timeout
Where timeout determines whether to start a session if the target user does not respond within the grace period. Possible values are:

1 Starts the session if the grace period times out.

0 Cancels the session if the grace period times out.

RC_STARTUP_STATE = startup_state
Where startup_state specifies the initial state of a Remote Control action. Possible values are:

0 The action is started in monitor state (Monitor or Guidance).

1 The action is started in active state (Active).

RC_CHANGE_STATE= change_state
Where change_state determines whether the target user can change the state during a Remote Control session. Possible values are:

0 Not enabled

1 Enabled (user can change from Active to Monitor/Guidance or vice versa).

Set to No
No script is run before the session.

Allow clipboard transfer
Determines the availability of the **clipboard transfer** icon in the controller session window. For more information about this feature, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes

The clipboard transfer icon is available for use in the controller window. The controller user can transfer the clipboard content between the controller and the target.

Set to No

The clipboard transfer icon is not available for use in the controller window.

Allow session handover
The master controller in a collaboration session can use this feature to hand over control of the session to a new controller. Determines the availability of the **Handover** option on the collaboration control panel. For more information about the hand over function, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes

The **Handover** option is displayed in the collaboration control panel.

Set to No

The **Handover** option is not displayed in the collaboration control panel.

Enable user acceptance for collaboration requests

Use this policy to display the user acceptance window on the target computer when another controller requests to join a collaboration session. For more information about joining a collaboration session, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes

The user acceptance window is displayed on the target computer after the master controller accepts to share the session for collaboration. The target users response determines whether the additional controller is allowed to join the session.

Accept

The additional controller joins the collaboration session.

Refuse

A refusal message is displayed on the controller and the additional controller cannot join the collaboration session.

Timeout

If the target user does not respond to the user acceptance within the time defined in **Acceptance Grace Time** a refusal message is displayed to the additional controller. The additional controller does not join the collaboration session.

Set to No

The user acceptance window is not displayed on the target machine. After the master controller accepts to share the session for collaboration, the additional controller joins the session.

Stop screen updates when screen saver is active

Stops the target from sending screen updates when it detects that the screen saver is active.

Set to Yes

While the screen saver is active on the target system, the target stops transmitting screen updates. A simulated screen saver is displayed on the controller computer so that the controller user knows that a screen saver is active on the remote screen. The controller user can close the screen saver by pressing a key or moving the mouse.

Set to No

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.

Enable user acceptance for local recording

Use this feature to display the user acceptance window when a controller user clicks the record icon on the controller window. The target user can accept or refuse the request to make a local recording of the remote control session.

Set to Yes

When the controller user clicks the record icon on the controller window, a message dialog is displayed. If the target user clicks **Accept**, the controller

user can select a directory to save the recording to. If the target user clicks **Refuse**, a recording refused message is displayed to the controller.

Note: After the target user accepts the request for recording, if the controller user stops and restarts local recording, the acceptance window is not displayed.

Set to No

When the controller user clicks the record icon on the controller window, the message window is not displayed. The controller user can select a directory to save the recording to.

Hide windows

Determines whether the **Hide windows** check box is displayed on the user acceptance window when **Enable user acceptance for incoming connections** is also set to Yes.

Set to Yes

The **Hide windows** check box is displayed on the user acceptance window.

Set to No

The **Hide windows** checkbox is not displayed on the user acceptance window.

Remove desktop background

Determines whether a desktop background image can be removed from view during a remote control session.

Set to Yes

The desktop background image on the target is not be visible during a remote control session.

Set to No

The desktop background image on the target is visible during a remote control session.

Lock color depth

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**.

Set to Yes

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.

Set to No

The initial color depth can be changed during the session.

Pre/post - script fail operation

Action to take if the pre-script or post-script execution fails. A positive value or 0 is considered a successful run of the pre-script or post-session script. A negative value, script that is not found or not finished running within 3 minutes is considered a failure.

Abort If the pre-script or post-script run is a fail, the session does not continue.

Proceed

If the pre-script or post-script run is a fail, the session continues.

Acceptance timeout action

Action to take if the user acceptance window timeout lapses. The target user did not click accept or refuse within the number of seconds defined for **Acceptance Grace time**.

Abort Session is not established. The default value is Abort.

Proceed
Session is established.

Acceptance Grace Time
Sets the number of seconds to wait for the target user to respond before a session starts or times out. Used along with **Enable User Acceptance for incoming connections**.

Note: If **Enable user acceptance for incoming connections** is set to Yes, Acceptance Grace Time must be set to a value >0 to give the target user time to respond.

Configuration

File Transfer
Determines whether File Transfer is available as a session mode on the start session window so that files can be sent or received during the session. For more information about File Transfer session mode, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes
File Transfer is available as a session mode in the start session window.

Set to No
File Transfer is not available as a session mode in the start session window.

Allow chat in session
Determines whether chat functions are available while in a remote control session and the also the availability of the chat icon in the controller window. For details of the Chat function, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes
Chat icon is available for selection in the controller window.

Set to No
Chat icon is disabled in the controller window.

Active Determines whether the target system can take part in active sessions. Also determines whether Active is available as a session mode on the start session window. For more information about the Active session mode, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes
Active is available as a session mode in the start session window.

Set to No
Active is not available as a session mode in the start session window.

Guidance
Determines whether the target system can take part in guidance sessions. Also determines whether Guidance is available as a session mode on the

start session window. For more information about the Guidance session mode, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes
Guidance is available for selection as a session mode in the start session window.

Set to No
Guidance is not available for selection as a session mode in the start session window.

Monitor
Determines whether the target system can take part in monitor sessions. Also determines whether Monitor is available as a session mode on the start session window. For more information about the Monitor session mode, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes
Monitor is available for selection as a session mode in the start session window.

Set to No
Monitor is not available for selection as a session mode in the start session window.

Chat Determines whether the target system can take part in chat only sessions. Also determines whether Chat is available as a session mode on the start session window. For more information about the Chat session mode, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to Yes
Chat is available as a session mode in the start session window.

Set to No
Chat is not available as a session mode in the start session window.

File Transfer Actions
Determines the actions that can be carried out on a file during a File Transfer session. If no value is set, the file transfer action is determined by the **default.rc_def_ft_actions** property in the `trc.properties` file.

Set to Send
You can transfer files only to the target during a File Transfer session.

Set to Pull
You can transfer files only from the target during a File Transfer session.

Set to Both
You can transfer files to and from the target during a File Transfer session.

Allow file transfer in session
Controls the transfer of files while in an Active session. Its value determines the availability of the **Send file** / **Pull file** options in the **File Transfer menu** within the Controller window. For more information about transferring files, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Set to NONE
The Send file and Pull file options are not available for selection. No file transfers can be initiated.

Set to BOTH
The Send file and Pull file options are available. Files can be transferred to the target and transferred from the target. This value is the default value.

Set to PULL
Only the Pull file option is available. Files can be transferred only from the target.

Set to SEND
Only the Send file option is available. Files can be transferred only to the target.

Policy List Values

Table 1. Policy acceptable and default values.

Policy	Possible Values - Bold (shipped default)	Default value
Reboot	**yes** | **no**	**yes**
Allow multiple controllers	yes | no	yes
Allow local recording	yes | no	yes
Set target locked	yes | no	no
Allow input lock	yes | no	yes
Connect at logon	yes | no	yes
Use encryption	yes | no	yes
Disable Panic Key	yes | no	no
Enable on-screen session notification	yes | no	no
Allow input lock with visible screen	yes | no	no
Display screen on locked target	yes | no	no
Denied Program Execution List	blank	blank
Inactivity timeout	number of seconds	0
Force session recording	yes | no	no
Local audit	yes | no	yes
Force session audit	yes | no (live audit on server)	yes
Keep session recording in the target system	yes | no	no
Record the session in the target system	yes | no	yes
Enable true color	yes | no	no
Allow registry key lookup	yes | no	no
View registry key list	yes | no	no

Table 1. Policy acceptable and default values. (continued)

Policy	Possible Values - Bold (shipped default)	Default value
Reboot	**yes | no**	**yes**
Enable user acceptance for system information	yes | no	no
Enable user acceptance for file transfers	yes | no	no
Enable user acceptance for mode changes	yes | no	no
Enable user acceptance for incoming connections	yes | no	no
Run post-session script	yes | no	no
Run pre-session script	yes | no	no
Allow clipboard transfer	yes | no	yes
Allow session handover	yes | no	yes
Enable user acceptance for collaboration requests	yes | no	no
Stop screen updates when screen saver is active	yes | no	no
Enable user acceptance for local recording	yes | no	no
Hide windows	yes | no	no
Remove desktop background	yes | no	no
Lock color depth	yes | no	no
Pre / post -script fail operation	abort | proceed	abort
Acceptance timeout action	abort | proceed	abort
Acceptance Grace Time	number of seconds	45
File transfer	yes | no	yes
Allow chat in session	yes | no	yes
Active	yes | no	yes
Guidance	yes | no	yes
Monitor	yes | no	yes
Chat	yes | no	yes
File transfer actions	pull | send | both	both
Allow file transfer in session	none | pull | send | both	both

Chapter 8. How policies are determined for a remote control session

When a remote control session is requested, a number of factors have to be considered when determining what permissions and policies are applied to the session. The policies and permissions for the various entities involved in the session are considered. These entities are user, user groups to which the user belongs, target, and target groups to which the target belongs. These different sets of policies have to be resolved following rules of precedence. The result is a single set of policies and permissions for each session.

Users and targets are assigned to groups that have policies and permissions defined. The permissions defined in these groups are known as their standard or normal set of permissions.

Due to the group hierarchy that can be set up, users and targets can be members of groups and user groups and target groups can also be members of other groups. This means that when a remote control session is requested, the permissions sets that are defined for immediate user to target group relationships, and permissions sets defined for relationships between parent and grandparent groups are all considered when determining the policies for the session.

When all required user and target groups have been created and their membership has been defined, you should create relationships between the user and target groups. This will determine what policies and permissions are applied during a remote control session. Use the Manage Permissions function to create these links between the groups.

Note: It is important for you to set up these groups and relationships in a way that will not lead to unexpected policy values.
.

Setting the policies and permissions for a remote control session

Creating permissions links between user groups and target groups is a fundamental part of the IBM Endpoint Manager for Remote Control application. These links are used when determining what policies and permissions are considered when resolving the final set of policies to be applied to a remote control session. When a user group or target group is created, a set of permissions is defined for the group, known as the standard or normal set. Use Manage Permissions to create a permissions link to combine the standard set of policies for the user group and standard set of policies for the target group. This standard permissions link has all of the policies set to priority **0**. You can then enable or disable the relevant policies. These standard permissions can also be overridden by selecting a **1** or **5** priority value to create a new set of permissions which will only be valid for the particular user group and target group combination that is selected. This will avoid the requirement for setting up a user and target group permissions link for every relationship needed.

Note: It should be noted that after a permissions link has been created between a user group and target group, the only way to change the policies for a session between members of these two groups is to edit this link. Editing the policies,

through the Edit group function, will have no affect on the policies and permissions defined in the existing link in Manage Permissions. It will only affect the policies considered for the group when any **NEW** permissions links are created.

Values assigned for standard or normal permissions

When you select a user group and a target group to set up a permissions link, the rules governing the values applied automatically in manage permissions, are defined as follows :

Yes

1. applied when **both** user group and target group have a policy value, in their standard permissions template, set to **Yes**
2. applied if one group has a policy value in their standard permissions template set to **Yes** and the other group set to **Not Set**. Standard Yes overrides Not Set

No applied when either group has a **No** policy value set in their standard permissions template

```
For example :  user group UG1

Guidance policy set to Yes
Monitor policy set to Yes
Reboot policy set to No
```

Members of UG1 can carry out Guidance and Monitor Sessions but are not allowed to perform a Reboot of the target.

```
For example :  target group TG1

Guidance policy set to Yes
Monitor policy set to Not Set
Reboot policy set to Yes
```

Members of TG1 can accept Guidance and Monitor Sessions and are allowed to accept a Reboot request.

So using the example user and target group above, the following policy values, would be automatically applied to the standard permissions set when UG1 and TG1 are selected on the Manage Permissions screen.

UG1 ⇔TG1

Table 2. Standard Permissions

	UG1	**TG1**	**Manage Permissions set**
Guidance	Yes	Yes	Yes
Monitor	Yes	Not Set	Yes
Reboot	No	Yes	No

Giving policies a higher priority value

Use the Manage Permissions function to apply a higher priority to policy permissions, to override the standard permissions set to satisfy the specific needs of your environment at any given time. The purpose of this is to avoid the requirement of having to set up a user group and target group permissions combination for every relationship needed. Higher priority permissions override

standard permissions if multiple permissions sets are found within the group hierarchy, when the policies for a session are being determined. There are three values that can be assigned to policies.

0 This is the standard or normal value that is automatically assigned to the policies when a link is created between a user group and a target group.

1 This value can be used to override any priority 0 policies when there are multiple permissions sets to be considered for a session.

If there is a group hierarchy and one of the permissions links has a policy set to priority 0 No, this policy is set to No when a session is established. To set the policy to Yes, when a session is established, select priority 1 Yes in one of the permissions links. A priority 1 Yes overrides a priority 0 No.

5 This value will override all other priority values when there are multiple permissions sets to be considered for a session.

Creating a permissions link

After user groups and a target groups have been defined, create a link between them to define a set of policies to be considered when a remote control session is requested between the user and target members of these groups.

To create this link, complete the following steps :

Note: The procedure given here selects the target group first, it can also be performed by selecting the user group first.

1. Click **Target groups** > **All Target groups** or use the search facility. For more details, see "Searching for target groups" on page 29
2. Select the required target group. For example, DefaultTargetGroup.
3. Click **Manage Permissions**. The Manage Permissions screen is displayed.
4. Choose the appropriate method for creating the permissions link.
   - Using the Group Browser. Use this option the first time a permissions link is created.
     - Click the selector button next to user group then select the required user group from the list. For example, DefaultGroup.
     - Click the selector button.
     - Click the selector button next to target group then select the required target group from the list. For example, DefaultTargetGroup.
     - Click the selector button.
   - Using an Existing profile.
     - Select **Existing Profile**
     - Select the required user to target group link from the list.
     - Click the selector button.

   The set of permissions and their selected values, derived from the combination of standard policies defined for the selected user and target group, is displayed.
5. To activate the policies click the **Enabled** checkbox at the top of the Enabled Column to enable all of the policies or click the enabled checkbox next to each required policy. If not all of the policies are required deselect the enabled checkbox **next to each non required policy.**

   Note: It is important to note that all required policies MUST be enabled before saving the permissions link, as any policy not enabled will lose it's

current value when the permissions link is saved. You should reassign a value to the policy if it is enabled, within the permissions link, in the future.

6. Set the required priority for each enabled policy.

   0 This is the lowest priority and is automatically assigned when creating the permissions link.

   1 This value will override a priority 0 policy when the policies and permissions are being determined for a remote control session.

   5 This is the highest priority. This value will override any existing 0 and 1 priority policies when the policies and permissions are being determined for a remote control session.

7. Set or enter a value for the enabled properties. For definitions and values for the policies, see Chapter 7, "Server session policies," on page 47.

   Set to Yes
   The policy is in effect during a remote control session depending on the priority that is set for it.

   Set to No
   The policy is not in effect during a remote control session depending on the priority that is set for it.

8. If the policy set is not required to be always in effect, you can create a schedule to define when it is used. To create a schedule for the policies, go to step 9 otherwise click **Submit** and these policies are now active.

9. From the - Repeat Schedule - list, select the required options then click **Submit**

   Once Only
   Policies are only valid from the Start date and start time till the End date and end time.

   a. Type in a Start date, in the format **yyyy-mm-dd** or select the calendar icon to select the required date.
   b. Type in a Start time in the format **hh:mm:ss**.
   c. Type in an End date, in the format **yyyy-mm-dd** or select the calendar icon to select the required date.
   d. Type in an End time in the format **hh:mm:ss**.

   Daily Policies are valid every day between the selected Start time and the End time from the Start date till the End date.

   a. Type in a Start date, in the format **yyyy-mm-dd** or select the calendar icon to select the required date.
   b. Type in an End date, in the format **yyyy-mm-dd** or select the calendar icon to select the required date.
   c. Type in a Start time in the format **hh:mm:ss**.
   d. Type in an End time in the format **hh:mm:ss**.

   Weekly
   Policies are valid every week on the selected days, between the selected Start time and End time from the Start date till the End date

   a. Type in a Start date, in the format **yyyy-mm-dd** or select the calendar icon to select the required date.
   b. Type in a Start time in the format **hh:mm:ss**
   c. Type in an End date, in the format **yyyy-mm-dd** or select the calendar icon to select the required date.
   d. Type in an End time in the format **hh:mm:ss**.

e. Select the required days.

Note:

a. Click **Cancel** on the Manage Permissions screen to return to the previously displayed screen and the Permissions link is not created.

Deleting a permissions link

After you have created permissions links you can delete them by completing the following steps :

1. Click **Target groups** > **All Target groups** or use the search function to search for target groups. For more details, see "Searching for target groups" on page 29.
2. Select the required target group. For example, DefaultTargetGroup.
3. Click **Manage Permissions**.
4. Click **Existing Profile**.
5. Select the required link from the Existing Profile list.
6. Click x, to the right of the existing profiles list.
7. On the Confirm deletion screen click **Submit**.

The selected permissions link is deleted.

Note: It is important to note that it is the link between the user group and target group that is deleted, the policies and permissions that are set specifically for the user group and target group are not affected when the permissions link is deleted.

How permissions are derived

When a request for a remote control session is initiated, all of the groups to which the user and target belong to is determined. The following can be true for these groups.

- **No grandparent group** present. Any parent groups found for the user and target only have user or target members.
- **Grandparent group present**. Due to the group hierarchy created through manage group membership, any parent groups found have user, target, user group and target group members.

The next thing that is determined is what permissions links have been created between any of these group. Using the set of rules defined below, the permissions for the session are derived.

- **No grandparent group** - this can be broken into two categories

  user and target are only members of one user and target group
  the policies for the session are set from the one permissions link that is defined for their parent user group and target group combination.

  user and target are also members of other user and target group
  the policies for the session are derived from comparing the multiple permissions links that are defined for any parent user group and target group combinations.

.

- **Grandparent group present** - the policies for the session are derived from comparing the multiple permissions links that are defined for any parent user group and target group combinations **AND** any permissions links defined for any grandparent groups.

Where multiple permissions links are present within the group hierarchy, the value set for each enabled policy, within each link, is checked and the rules governing the policy permissions for the session are defined as follows :

Priority 5 No
: If a policy in any of the relevant permissions links has this value set, the value set for the session is priority 5 No. This value overrides all other values.

Priority 1 No
: This value is set for the session if are no priority 5 values set in any existing permissions links.

Priority 0 No
: This value is set for the session if there are no priority 1 or 5 values set for any of the existing permissions links.

Priority 5 Yes
: This value is set for the session if there are **no** priority 5 No values set for any of the existing permissions links. Priority 5 Yes overrides any lower priority No.

Priority 1 Yes
: This value is set for the session if there are no priority 5 values or priority 1 no values set for any of the existing permissions links.

Priority 0 Yes
: This value is set for the session if there are no higher priority values set or a priority 0 No set for any of the existing permissions links.

Setting non binary policies

The non binary policies are not handled in the same way as the binary policies.

- Denied Program Execution List
- Inactivity timeout
- Pre Script Fail Operation
- Acceptance Timeout Action
- Acceptance Grace Time
- Allow File Transfer in Session

There are no specific rules for these policies BUT the following should be noted

- If there are multiple values for these set within permissions links, within the group hierarchy, the final set of policies will inherit one of these values BUT it is not defined which one.
- More importantly, if a policy is **NOT** defined in any permissions links in the group hierarchy, default values, defined in the `trc.properties` file (see “trc.properties” on page 172) will be assigned .

  Note: If non binary policies have been enabled in the group hierarchy but no values have been assigned to them, the values defined in `trc.properties` will **NOT** be assigned, therefore it is important to note that if you enable a non binary policy you should also assign a value to it.

Permissions set examples

The following examples show how the permissions are determined for a session involving the following entities,

4 user groups U1 – U4

5 target groups T1 – T5

users X and Y

targets A and B

The following gives the actions and steps that would be required to set up the users, targets, user groups and target groups used in the examples, to show how policies and permissions are derived for a session.

1. Create the required users X and Y
   a. Click **Users** > **New**.
   b. You would then enter relevant details for user X and click **Submit**.

   The above steps would be repeated for user Y.
2. Create the required user group U1 to U4 -
   a. Click **User groups** > **New user group**.
   b. Type in U1 for the group name.
   c. Click Submit to accept the default template.

   The above steps would be repeated for group U2, U3 and U4.
3. Assign user or user group members to the user group
   - Make user X a member of group U3
     a. Click **Users** > **Search**.
     b. Type in the userid or some other relevant information for user X.
     c. Select the entry for user X then click **Manage Group Membership**.
     d. In the user group list select U3 then click **Submit**.

     Note: Make sure that U3 is the only user group that is selected.
   - Make user Y a member of group U4
     a. Click **Users**.
     b. Click **Search** then type in the userid or some other relevant information for user Y.
     c. Select the entry for user Y then click **Manage Group Membership**.
     d. In the user group list select U4 then click **Submit**.

     Note: Make sure that U4 is the only user group that is selected.
   - Make groups U3 and U4 members of U2
     a. Click **User groups**.
     b. Click **Search** then type in U.
     c. Click **Submit**
     d. Select the entries for U3 and U4 then click **Manage Group Membership**
     e. In the user group list select U2.

     Note: Make sure that U2 is the only user group that is selected.

f. Select **add to current group membership**.
g. Click **Submit**.

- Make U2 a member of U1
  a. Click **User groups**.
  b. Click **Search** then type in U2.
  c. Click **Submit**.
  d. Select the entry for U2 then click **Manage Group Membership**.
  e. In the user group list select U1 then click **Submit**.

4. Create the required target groups T1 to T5
   a. Click **Target groups** > **New target group**.
   b. Type in T1 for the group name.
   c. Click **Submit** to accept the default template.

   The above steps would be repeated for group T2, to T5.
5. After the target software has been installed on target A and B and targets have made themselves known to the server, assign target or target group members to target groups
   - Make target A a member of group T4
     a. Click **Targets**.
     b. Click **Search** then type in the serial number or some other relevant information for target A.
     c. Select the entry for target A then click **Manage Group Membership**.
     d. In the target group list select T4 then click **Submit**.

     Note: Make sure that T4 is the only target group that is selected.
   - Make target B a member of group T5
     a. Click **Targets**.
     b. Click **Search** then type in the serial number or some other relevant information for target B.
     c. Select the entry for target B then click **Manage Group Membership**.
     d. In the target group list select T5 then click **Submit**.

     Note: Make sure that T5 is the only target group that is selected.
   - Make group T4 and T5 members of T2
     a. Click **Target groups**.
     b. Click **Search** then type in T.
     c. Click **Submit**.
     d. Select the entries for T4 and T5 then click **Manage Group membership**.
     e. In the target group list select T2.

     Note: Make sure that T2 is the only target group that is selected.
     f. Select **add to current group membership**.
     g. Click **Submit**.
   - Make T2 and T3 members of T1
     a. Click **Target groups**.
     b. Click **Search** then type in T.
     c. Click **Submit**.
     d. Select the entries for T2 and T3 then click **Manage Group Membership**.

e. In the target group list select T1

Note: Make sure that T1 is the only target group that is selected.

f. Select **add to current group membership**.

g. Click **Submit**.

6. Permissions links would then be created between specific user and target group remembering to enable all required policies- We will create the links in each example below.

The following figure shows the group hierarchy that we have created.

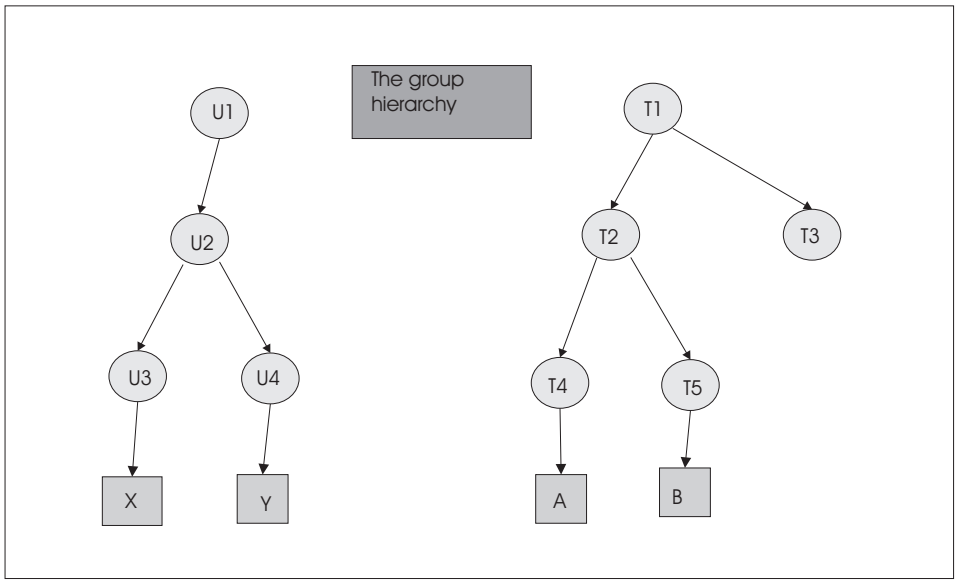

Figure 1. Group tree diagram

Example 1: - Standard priority 0 permissions

When the groups are created, a standard permissions template is defined for U1 and T1. To change any values for the group, use the **Edit group** action. In this example, edit the values for U1, set Chat to Yes and everything else to No. In group T1 Chat and Monitor are set to Yes and everything else to No.

Edit user group U1

1. Click **User groups**.
2. Select **Search**
3. Type in U1 in the input field.
4. Click **Submit**.
5. Select the entry for U1 and click **Edit group**.
6. Click **Edit Settings**.
7. Select **Yes** for Chat, everything else select **No**.
8. Select **Save as new template named** and type in **AllowChat** for the template name.
9. Click **Submit**.

Edit target group T1

1. Click **Target groups**.
2. Select **Search**.
3. Type in T1 in the input field.
4. Click **Submit**.
5. Select the entry for T1 and click **Edit group**.
6. Click **Edit Settings**.
7. Select **Yes** for Chat and Monitor, everything else select **No**.
8. Select **Save as new template named** and type in **AllowChatMonitor** for the template name.
9. Click **Submit**.

Within the Manage Permissions action when a relationship between U1 and T1 is created, because there are no higher priority permission values enabled, the set that is created for the U1 ⇔T1 combination has all enabled policies set to priority 0.

Create the Permissions link

1. Click **Target groups** > **All target groups**.
2. Select T1.
3. Click **Manage Permissions**.
4. The Manage Permissions screen is displayed.
5. Click the **Group Browser** button if not selected.
6. Click the selector button next to user group then select U1.
7. Click the selector button.
8. Click the selector button next to target group then T1.
9. Click the selector button.
10. The set of permissions and their selected values, which are derived from the combination of standard policies that are defined for U1 and T1, is displayed.
11. Click the **Enabled** check box to make the policies available.
12. Click **Submit**

The following figure shows the group hierarchy and permissions links

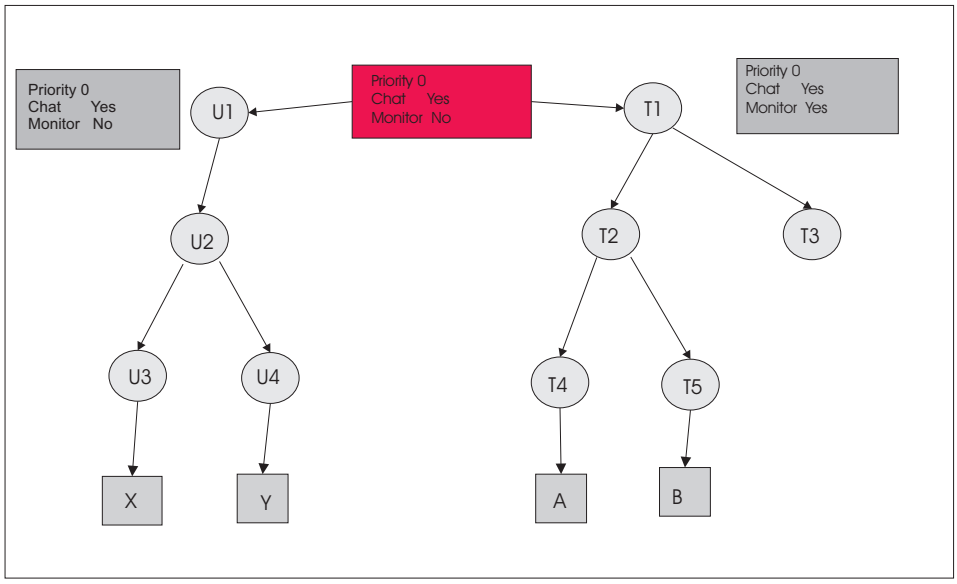

Figure 2. Standard priority 0 permissions

Determining session permissions for example 1

user X is a member of group U3, U2 and U1

user Y is a member of group U4, U2 and U1

target A is a member of group T4, T2 and T1

target B is a member of group T5, T2 and T1

Using Figure 2 and the policy engine process explained above, there are parent and grandparent groups, however there is only **one** permissions link defined in the group hierarchy between U1 and T1. It is the policies and their values within this link that are assigned for a remote control session. The resultant permissions set will allow users X and Y to only initiate Chat sessions with targets A and B.

Note: Monitor is set to No because the priority 0 No value that was set for group U1 overrides the priority 0 Yes value that was set for group T1.

Example 2: - Higher priority permissions

When group U4 and T4 were created, the default template was accepted as the standard set of permissions. Create a relationship in Manage Permissions between U4 and T4 and select a higher priority No for Chat and higher priority Yes for Monitor.

Create the Permissions link

1. Click **Target groups** > **All target groups**.
2. Select T4
3. Click **Manage Permissions**.
4. The Manage Permissions screen is displayed.
5. Click the **Group Browser** button if not selected.
6. Click the selector button next to user group then select U4 (group list must be expanded to show this).

7. Click the selector button.
8. Click the selector button next to target group then T4 (group list must be expanded to show this).
9. Click the selector button.
10. The set of permissions and their selected values, which are derived from the combination of standard policies that are defined for U4 and T4 is displayed.
11. Click the **Enabled** check box to make all of the policies available.
12. Set priority to 1 for Chat and select the value No, set priority to 1 for Monitor, and select the value Yes. Set Guidance, Active, and File transfer to No
13. Click **Submit**

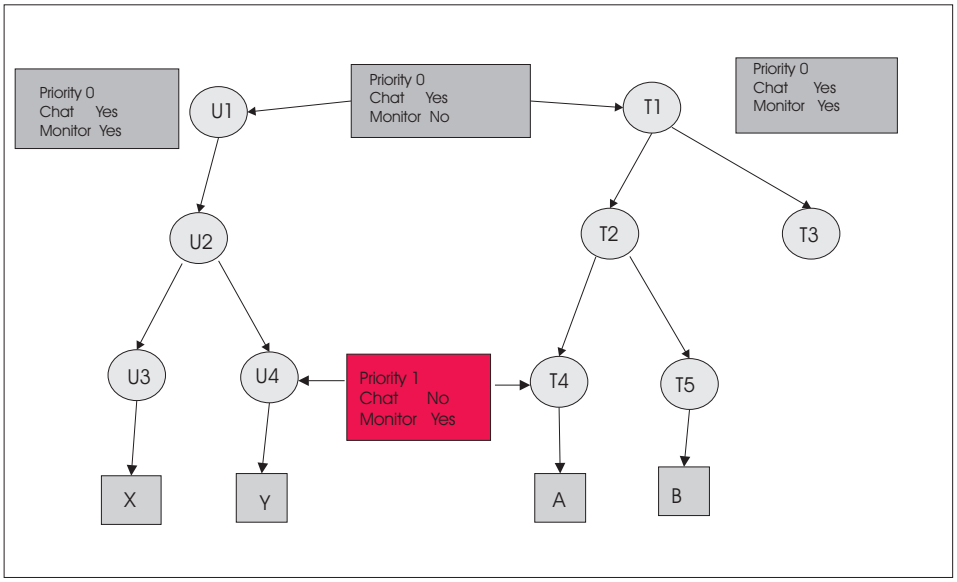

Figure 3. Higher priority permissions

Determining Permissions for example 2.

user X is a member of group U3, U2 and U1

user Y is a member of group U4, U2 and U1

target A is a member of group T4, T2 and T1

target B is a member of group T5, T2 and T1

Using Figure 3 and the policy engine process, explained above, there are parent and grandparent groups and there are multiple permissions links defined in the group hierarchy. The following permissions is applied for each example session.

Session with user X and target A
The only permissions link considered for these two entities is the one between U1 and T1 because user X is NOT a member of U4. Therefore user X can only initiate a Chat session with target A.

Session with user X and target B
A similar explanation to the one above. Only the link between U1 and T1

is considered as user X is not a member of U4 and target B is NOT a member of T4. Therefore user X can only initiate a Chat session with target B.

Session with user Y and target A
There are two permissions links to be considered this time: U1 to T1 and U4 to T4. Therefore user Y can only initiate a Monitor session with target A as the priority 1 value set in the link between U4 to T4 overrides the priority 0 value set in the link between U1 and T1.

Priority 1 No overrides priority 0 Yes

Priority 1 Yes overrides priority 0 No

Session with user Y and target B
The only permissions link considered for these two entities is the one between U1 and T1 because target B is NOT a member of T4. Therefore user Y can only initiate a Chat session with target B.

Note: The same explanation as above would be applied if the priority values set in the U4⇔T4 link had been set to 5 as priority 5 overrides 1 and 1 overrides 0.

Example 3: - Only relationship permissions are inherited

Edit the target group T2 and change the standard permission template value for Chat to No.

Edit target group T2

1. Click **Target groups** > **Search**.
2. Type in T2 in the input field.
3. Click **Submit**.
4. Select the entry for T2 and click **Edit group**.
5. Click **Edit Settings**.
6. Select **No** for everything, including Chat.
7. Select **Save as new template named** and type in `NoChat` for the template name.
8. Click **Submit**.

In Figure 4 on page 76 there are parent and grandparent groups, and there are multiple permission links defined in the group hierarchy. The following permissions are applied for each example session.

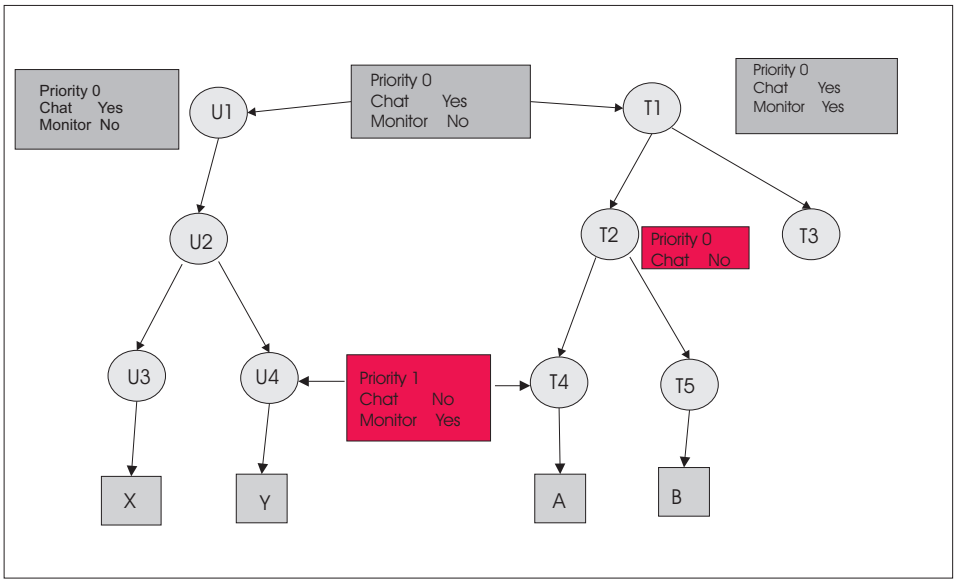

Figure 4. Only relationship permissions inherited

Determining Permissions for example 3

user X is a member of group U3, U2 and U1

user Y is a member of group U4, U2 and U1

target A is a member of group T4, T2 and T1

target B is a member of group T5, T2 and T1

Session with user X and target A

The only permissions link considered for these two entities is the one between U1 and T1 because user X is NOT a member of U4 . Therefore user X can only initiate a Chat session with target A

Priority 1 No overrides priority 0 Yes

Priority 1 Yes overrides priority 0 No

Note: The standard set for T2 has Chat set to priority 0 No which would override standard Yes, if it was a link **BUT** because we did not create a permissions link with T2 and any other group, it's values are not considered as it is only the policy values in permissions links that are inherited.

Session with user X and target B

A similar explanation to the one above. Only the link between U1 and T1 is considered as user X is not a member of U4 and target B is NOT a member of T4. Therefore user X can only initiate a Chat session with target B. Similar explanation as the T2 permissions.

Session with user Y and target A

There are two permissions links to be considered this time U1 to T1 and U4 to T4. Therefore user Y can only initiate a Monitor session with target A as the priority 1 value set in the link between U4 to T4 overrides the priority 0 value set in the link between U1 and T1. Again T2 policies and permissions are not considered as there are no permissions links set up between it and any other groups.

Session with user Y and target B

The only permissions link considered for these two entities is the one between U1 and T1 because target B is NOT a member of T4 . The value of priority 0 No in the standard set for T2 would have overridden the U1 to T1 priority 0 Yes if T2 had been linked to another group but as it is not, the value is not considered. Therefore user Y can only initiate a Chat session with target B

Example 4 - No overrides Yes when priority values are the same

Now in Manage Permissions we will create a link between group U2 and T2 with priority 0 permissions and Chat set to No.

Create the Permissions link

1. Click **Target groups** > **All target groups**.
2. Select T2.
3. Click **Manage Permissions**.
4. The Manage Permissions screen is displayed.
5. Click the **Group Browser** button if not selected.
6. Click the selector button next to user group then select U2 (group list will need to be expanded to show this).
7. Click the selector button.
8. Click the selector button next to target group then T2.
9. Click the selector button.
10. Displayed is the set of permissions and their selected values, derived from the combination of standard policies defined for U2 and T2.
11. Make the policies available by clicking the **Enabled** checkbox.
12. Set the value for Chat to `priority 0 No`, Monitor to `priority 0 Yes` and Guidance, Active and File Transfer to Yes
13. Click **Submit**

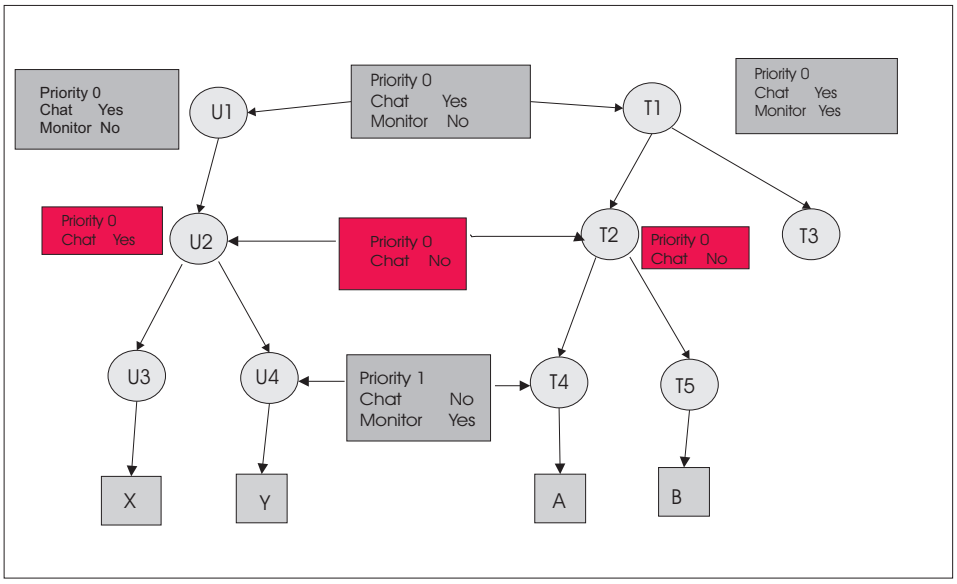

Figure 5. No overrides Yes when priority values are the same

Determining Permissions for example 4

user X is a member of group U3, U2 and U1

user Y is a member of group U4, U2 and U1

target A is a member of group T4, T2 and T1

target B is a member of group T5, T2 and T1

Using Figure 5 and the policy engine process explained above, there are parent and grandparent groups, and there are multiple permissions links defined in the group hierarchy . The following permissions is applied for each example session

Session with user X and target A

There are two permissions links to be considered for these two entities, the link between U2 and T2 and the link between U1 and T1. Both links have priority 0 permissions set, U2 ⇔ T2 has Chat set to priority 0 No and U1 ⇔ T1 has Chat set to priority 0 Yes, therefore user X cannot initiate a Chat session or a Monitor session with target A as the priority 0 No for Chat in U2 to T2 overrides the priority 0 Yes for Chat in U1 to T1.

Note: The link between U4 and T4 is not considered as user X is NOT a member of group U4.

Session with user X and target B

A similar explanation to the one above. Only the links between U2 and T2 and U1 and T1 are considered as user X is not a member of U4 and target B is NOT a member of T4. Therefore user X cannot initiate a Chat session or a Monitor session with target B.

Session with user Y and target A

There are three permissions links to be considered this time U1 to T1, U2 to T2 and U4 to T4. Therefore user Y can only initiate a Monitor session with target A as the priority 1 value set in the link between U4 to T4

override the priority 0 values set in the link between U1 and T1 for Monitor . A Chat session **cannot** be initiated because the priority 1 value of No, set for Chat in the U4 to T4 link, overrides the priority 1 No in the U2 to T2 link and the priority 0 Yes in the U1 to T1 link.

Session with user Y and target B

There are two permissions link considered for these two entities, the one between U2 and T2 and U1 and T1. Therefore user Y cannot initiate a Chat or a Monitor session with target B as the priority 0 No value for Chat in the link between U2 to T2 overrides the priority 0 Yes value for Chat in the link between U1 to T1.

Note: The link between U4 and T4 is not considered as target B is NOT a member of group T4.

Note: It should also be noted that the same explanation would have applied if the priority for Yes and No had both been 1 or 5. No will override Yes when the priority values are the same.

Example 5 - Higher priority Yes overrides lower priority No

In this example we will edit an existing link in Manage Permissions to change the value of the priority 1 link defined between U4 and T4. We will change the value of Chat from No to Yes.

Edit the Permissions link

1. Click **Target groups** > **All target group**
2. Select T4
3. Click **Manage Permissions**
4. The Manage Permissions screen is displayed
5. Click the **Existing Profile** button
6. From the pull down select the link between U4 and T4
7. Click the selector button
8. Keeping the priority 1 option selected next to Chat, select the value Yes
9. Click **Submit**

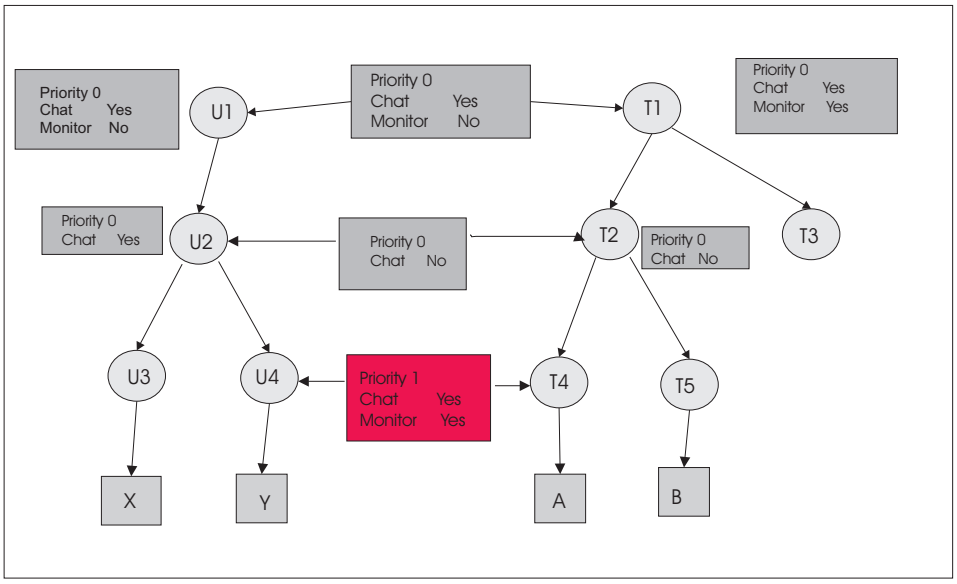

Figure 6. Higher priority Yes overrides lower priority No

Determining Permissions for example 5

user X is a member of group U3, U2 and U1

user Y is a member of group U4, U2 and U1

target A is a member of group T4, T2 and T1

target B is a member of group T5, T2 and T1

Using Figure 6 and the policy engine process explained above, there are parent and grandparent groups, and there are multiple permissions links defined in the group hierarchy. The following permissions is applied for each example session

Session with user X and target A

There are two permissions links to be considered for these two entities, the link between U2 and T2 and the link between U1 and T1. Both links have priority 0 permissions set, U2 and T2 have Chat set to No and U1 and T1 have Chat set to Yes, therefore user X cannot initiate a Chat session or a Monitor session with target A as the priority 0 No for Chat in U2 to T2 overrides the priority 0 Yes for Chat in U1 to T1.

Note: The link between U4 and T4 is not considered as user X is NOT a member of group U4.

Session with user X and target B

A similar explanation to the one above. Only the links between U2 and T2 and U1 and T1 are considered as user X is not a member of U4 and target B is NOT a member of T4. Therefore user X cannot initiate a Chat session or a Monitor session with target B.

Session with user Y and target A

There are three permissions links to be considered this time U1 to T1, U2 to T2 and U4 to T4. Therefore user Y can initiate both a Monitor session

and a Chat session with target A as the priority 1 values set in the link between U4 to T4 overrides the priority 0 values set in the link between U1 and T1.

Session with user Y and target B

There are two permissions link considered for these two entities, the one between U2 and T2 and U1 and T1. Therefore user Y can only initiate a Chat session with target B as the priority 0 No value for Chat in the link between U2 to T2 overrides the priority 0 Yes value for Chat in the link between U1 to T1.

Note: The link between U4 and T4 is not considered as target B is NOT a member of group T4.

Note: The same explanation would have applied if the priority value had been set to 5 in the U4 ⇔T4 link. Priority 5 overrides 1 and 1 overrides 0.

In summary

- Users and targets **MUST** be members of user and target groups to be able to establish Remote Control Sessions.
- Permissions links **MUST** be set up between the relevant user and target groups.
- All required policies **MUST** be enabled in the permissions links.
- If there is only one permissions link defined in the group hierarchy it is the policies and permissions defined in this link that will be assigned to the Remote Control Session.
- If there are multiple permissions links defined in the group hierarchy the final set is derived from these links using the following rules
  - Priority 5 No overrides all other values.
  - Priority 5 Yes overrides priority 0 or 1 No.
  - Priority 1 No overrides priority 0 or 1 Yes.
  - Priority 1 Yes overrides priority 0 No
  - Priority 0 No overrides priority 0 Yes
- Changing policy values via **Edit group** will **NOT** affect the policy values for the group in any **existing** permissions links, only in any **NEW** permissions links, therefore it will be of more benefit if the changes are made in the permissions links in **Manage Permissions**.

Chapter 9. Managing permission sets for temporary access to targets

When a controller user requests temporary access to a target you can action the request and define what the controller user is allowed to do during the session. Part of this process involves enabling and setting values for the policies that should be in effect during the temporary session. You can define a set of policies and permissions that can be saved and used automatically to set the temporary permissions, thus removing the need for enabling each of the required policies every time you grant a new request. This is achieved by using the **Permissions Sets** option in theIBM Endpoint Manager for Remote Control Server. For details of how to deal with a temporary access request, see Chapter 10, "Requests for temporary access to targets," on page 87.

Creating a set of permissions

You can create a set of permissions that can be saved and used to define the policies and permissions for a temporary access request session thus removing the need for setting each individual policy every time you grant a request.

To create a set of permissions complete the following steps in the IBM Endpoint Manager for Remote Control Server:

1. Click **Admin** > **New Permission Set**. The **Edit Permission Set** screen is displayed.
2. Type in a name for the permissions set in the **Set Name** field.
3. Choose the appropriate method for enabling the required policies
   - to enable every policy click Enabled at the top of the column
   - select the check box next to each required policy

   Note: It is important to enable all required policies.
4. Set the required priority for each enabled policy. The default priority value is the value that is displayed first in the list when the Edit Permission Set screen is displayed and is set by the **trc.default.request.priority** property in `trc.properties` file. For details of editing the properties files, see Chapter 21, "Editing the properties files," on page 171.

   5 This is the highest priority. This value will override any existing policies that may exist between the user and target.

   1 This value will override any existing priority 0 policies that may exist between the user and target.

   0 This is the lowest priority. Any existing permissions in effect between the user and target that are of a higher priority will override this policy therefore it is recommended to set the policy to a higher priority value if there are existing permissions.
5. Set or enter a value for the enabled properties. For definitions and values for the policies, see Chapter 7, "Server session policies," on page 47.

   Set to Yes
   The policy is in effect during the temporary session depending on the priority that is set for it.

Set to No

The policy will not be in effect during the temporary session depending on the priority that is set for it.

Note: If the priority is set to 0 or 1, an existing policy of priority 5 Yes will override this policy.

6. Click **Submit**.

You have now created a set of policies and permissions that can be selected whenever you are granting a temporary access request so that you can enable and set values for specific policies without having to manually select each one.

Viewing sets of permissions

After you have created sets of policies and permissions you can view the list of sets by using the **View Permissions Sets** option.

To view the list of permissions sets click **Admin** > **All Permission Sets**.

The View Permissions Sets screen is displayed listing all defined permissions sets.

Modifying a defined set of permissions

You can edit a set of permissions to change the following information

- The name of the set.

  Note: Duplicate names are not allowed.
- Enable or disable policies.
- Set or change priority levels.
- Set or change the policy value.

To edit a set of permissions complete the following steps :

1. Click **Admin** > **All Permission Sets**.
2. Select the required permissions set.
3. Choose the appropriate method for selecting **Edit Permissions Set**:
   - Select **Edit Permission Set** from the action list on the left.
   - click **Admin** > **Edit Permissions Set**

   The Edit Permission Set screen is displayed.
4. Make the required changes to the policies.
5. Click **Submit**

The changes made are now saved to the selected set of permissions.

Note: Click **Cancel** to leave the Edit Permission Set screen. The information for the selected set of permissions is not modified.

Deleting permission sets

You can remove one or more defined sets of permissions if they are no longer required by using the **Delete Permission Set** action.

To remove sets of permissions complete the following steps :

1. Click **Admin** > **All Permission Sets**.
2. Select the required permissions sets.
3. Choose the appropriate method for deleting the permissions set .:
   - Select **Delete Permission Set** from the action list on the left.
   - click **Admin** > **Delete Permissions Set**
4. On the Confirm Deletion screen click **Submit**.

The selected permission sets are deleted.

Note: Click **Cancel** to leave the View Permissions Sets screen and the selected permissions sets are not removed.

Chapter 10. Requests for temporary access to targets

Users can only start a remote control session with the targets that they have permission to access through their group membership and the relationships that have been set up between these groups. However, a user can request temporary access to one or more targets that they do not normally have access to. When a request for temporary access is received it is known as an outstanding access request, with a status of pending. These requests are listed in the outstanding requests list in the IBM Endpoint Manager for Remote Control Server. When you grant the request it becomes a live request, with a status of granted and is moved to the live requests list. If you refuse the request its status changes to rejected and it is removed from the outstanding list. However all requests outstanding, live or denied are also displayed in the **All access requests** list and remain there till they have either expired or are removed by the cleanup task' which runs periodically to delete expired or no longer required requests.

Note: It is important to note that the email functionality must be enabled in order for the notification process to take place. For more details, see "Setting up email" on page 16.

Handling a request for temporary access to targets

When a user creates a request for temporary access to target systems an email is sent to the administrator or a group of administrators letting them know that a request has been made.

Display the **Outstanding requests** list to view this new request and determine its outcome by performing one of the following actions

- Grant
- Deny
- Delete

Note: The recipient of the email when a request is submitted is determined by property values in the `trc.properties` file. You can create a user group and assign to it, the specific users with admin authority who should receive the email. The property **`trc.ticket.admin`** should be set to the user group name that you have created. If this property is not assigned a value it is the admin user whose email address is set in the **`email.admin`** property that will receive the email. For details of editing the properties files, see Chapter 21, "Editing the properties files," on page 171.

Giving users temporary access to target systems

You can allow users to temporarily access targets by granting a request for access. Use this option to define what the user is allowed to do during the session. This includes setting the policies and permissions that will be effective during the temporary access, providing them with any additional information that you think may be relevant and setting a date and time period that the access is valid for. Use the **show effective policies** option to check if there are already existing policies set for the user and target which should be taken into consideration when setting the policies for the temporary access to the target.

Allowing temporary access can be carried out in three ways

1. Grant an outstanding access request.
2. Grant a denied request.
3. Grant an anonymous request.

Granting an outstanding access request

When you receive an email informing you that a request for temporary access to one or more targets has been submitted you should action this by looking in the **Outstanding Access Requests** list.

To grant temporary access complete the following steps :

1. Click **Reports** > **Outstanding Access Requests**.
2. Select the required request.
3. Choose the appropriate method for viewing the request :-
   - Select **View/Edit Request** from the Actions list on the left.
   - Select **Reports** > **View/Edit Request**.

   The Manage access to targets screen is displayed showing what the user has requested in the **Requested access requirements** section.
4. Click the arrow button next to the target name at **Request Targets** to view effective policies, to check if there are any existing policies set for the user and target.

   Note: If there are existing policies set for the user and target, these should be taken into consideration when setting the policies and permissions for the temporary access.
5. Click **Cancel** to return to the Manage Access to Target screen.
6. Use the **Specify access allowed** section to set the policies and time period for the access.

   Setting the permissions effective during the session

   You can enable and set the policies and permissions that will be effective during the temporary session by using an already defined permissions set or by enabling individual policies. Choose the appropriate method for setting the policies.

   a. **Permissions Set** - Use an already defined set of permissions.
      1) Select a defined set of permissions from the list
      2) Click the arrow button next to **Permissions**, to show the policies and permissions that are set.

         Note: You can also change any of these values here.

      For details of Permissions sets, see “Creating a permission set” on page 124.

   b. **Permissions** - Manually enable each required policy.
      1) Click the arrow button next to **Permissions**.
      2) Choose the appropriate method for enabling the policies
         - to enable every policy click **Enable all** at the top of the column.

           Note: This should be selected if there are existing policies set.
         - select the check box next to each required policy

Note: It is important to enable all required policies, particularly if there are existing permissions set between the user and the target, as any existing policy that is not enabled here will not be in effect in the temporary session.

c. Set the required priority for each enabled policy. The default priority value is the value that is displayed first in the list and is set by the **trc.default.request.priority** property in `trc.properties` file. For details of editing the properties files, see "trc.properties" on page 172.

5 This is the highest priority. This value will override any existing 0 and 1 priority policies that may exist between the user and target.

1 This value will override any existing priority 0 policies that may exist between the user and target.

0 This is the lowest priority. Any existing permissions in effect between the user and target that are of a higher priority will override this policy therefore it is recommended to set the policy here to a higher priority value if there are existing permissions.

d. Set or enter a value for the enabled properties. For definitions and values for the policies, see Chapter 7, "Server session policies," on page 47.

Set to Yes
The policy is in effect during the temporary session if there are no existing permissions set up between the user and target. For existing permissions it is in effect depending on the priority that is set for it here.

Set to No
The policy will not be in effect during the temporary session if there are no existing permissions set up between the user and target. For existing permissions it will not be in effect depending on the priority that is set for it here.

Note: If the priority is set to 0 or 1, an existing policy of priority 5 Yes will override this policy.

Admin Notes®
Type in here any relevant additional information. For example to inform the user of the time that the session is valid for if it is different to the times requested.

```
for example : Session only valid today between 12:00:00 and 14:30:00.
```

Starting on

a. Select from the calendar or type the date, in the format **yyyy-mm-dd**, on which you want the access to commence.
b. Type in a time in the format **hh:mm:ss** that you want the access to commence.

Ending on

a. Select from the calendar or type the date, in the format **yyyy-mm-dd**, on which you want the access to end.
b. Type in a time in the format **hh:mm:ss**, that you want the access to end.

7. Click **Grant**.

An email is sent to the requesting user informing them that the request for temporary access has been granted and the request is saved to the Live access requests list.

Granting an already denied access request

If after denying a request for temporary access to a target it is decided that the access is allowed, you can modify the request and change the status of the request to granted. When you change the status of the request you can also define what access is allowed and when the access is allowed.

To grant an already denied request for temporary access complete the following steps :

1. Click **Reports** > **All Access Requests**.
2. Select the required request.
3. Choose the appropriate method for viewing the request :
   - Select **View/Edit request** from the Actions list on the left.
   - Select **Reports** > **View / Edit request**.
4. Go to step 6 on page 88, to complete the details for the request.

An email is sent to the requesting user informing them that the request for temporary access has been granted and the request is saved to the Live access requests list.

Granting an anonymous request

When a request for temporary access is made by a user who is not registered in the IBM Endpoint Manager for Remote Control Server it is known as an anonymous request. The user should provide details of the targets that they are requesting access to and you should search for these targets or a group of targets to determine if the temporary access should be allowed.

To accept an anonymous request for temporary access complete the following steps :

1. Click **Reports** > **Outstanding Access Requests**.
2. Select the required request.
3. Choose the appropriate method for viewing the request :
   - Select **View/Edit request** from the Actions list on the left.
   - Select **Reports** > **View / Edit request**.
4. The Manage Access to Targets screen is displayed showing that there are no targets selected.
5. Specify Access allowed - Use the justification from the user to determine the targets that are being requested.

   Choose the appropriate method to select targets.

   Select Targets

   a. Click **Select Targets**.
   b. Select one or more targets from the Search targets list.
   c. Click **Submit**. The target name is displayed next to Targets.

   Select Target Groups

   a. Click **Select Target Groups**.

b. Select one or more target groups from the Search list.
c. Click **Submit**.

   All targets that are members of the selected groups are displayed next to Targets.

6. Go to step 6 on page 88, to complete the details for the request.

An email is sent to the user informing them that their request has been granted and provides a link to the IBM Endpoint Manager for Remote Control application so that they can access the targets.

Revoking requests for temporary access to target systems

If you decide that a user should no longer be allowed to temporarily access a target after their request was granted you can update the request to refuse the access by using the **Revoke** option.

To revoke a request for temporary access to a target complete the following steps :

1. Click **Reports** > **Live Access Requests**.
2. Select the required request.
3. Choose the appropriate method for viewing the request :
   - Select **Reports** > **View/Edit request**.
   - select **View/Edit request** from the Actions list on the left.

   The Manage Access to Target screen is displayed but as the status is granted the policies and permissions that were set for the temporary access are not displayed.
4. If you require to change any of the policies for the request click the **Manage Permissions** link to view the policies that are set and complete steps 5 on page 65, to 9 on page 66 to make the required changes. If you do not require to make any changes, click **Revoke**.

   Note: If you click **Cancel** on the Manage Permissions screen any changes made to the policies will not be saved.

An email is sent to the requesting user informing them that the request for temporary access is no longer allowed and the request is removed from Live access requests list.

Denying requests for temporary access to target systems

When a request for temporary access to targets is received you can refuse the user access to the specified targets by using the **Deny** option.

To deny a request for temporary access to a target complete the following steps :

1. Click **Reports** > **Outstanding Access Requests**.
2. Select the required request.
3. Choose the appropriate method for viewing the request :
   - Select **View/Edit request** from the Actions list on the left.
   - Select **Reports** > **View/Edit request**.
4. In the **Admin Notes** field supply a reason for denying the request.
5. Click **Deny**.

An email is sent to the requesting user informing them that the request for temporary access has been rejected and the request is removed from the outstanding access requests list.

Deleting requests for temporary access to target systems

You can remove one or more requests for access that are no longer required by using the Delete option. This can be done in the following ways

- Selecting one or more requests from a list of requests.
- When viewing or editing a request.

Deleting access requests from a request list

To remove one or more requests from a list of requests complete the following steps:

1. Click **Reports** then one of the following items:
   - Outstanding Access Requests.
   - Live Access Requests.
   - All Access Requests.
2. Select the required requests.
3. Choose the appropriate method for deleting the request:
   - Select **Delete Request** from the Actions list on the left.
   - Select **Reports** > **Delete Request**.
4. On the Confirm Deletion screen click **Submit**.

The selected requests are removed from the IBM Endpoint Manager for Remote Control database.

Note: Click **Cancel** on the Confirm Deletion screen to return to the previously displayed screen and the requests are not removed.

Deleting access requests while editing

To remove a request when viewing or editing it complete the following steps :

1. Click **Reports** then **one** of the following items
   - Outstanding Access Requests.
   - Live Access Requests.
   - All Access Requests.
2. Select the required requests.
3. Choose the appropriate method for viewing the request :
   - Select **View/Edit Request** from the Actions list on the left.
   - Select **Reports** > **View/Edit Request**.
4. Click **Delete** on the Manage Access to Target screen .

The request is removed from the IBM Endpoint Manager for Remote Control database.

Viewing requests for temporary access to target systems

When requests for temporary access to targets have been submitted you can view the lists of these for reporting purposes. There are three ways to view the requests

- View outstanding access requests.
- View live access requests.

- View all access requests.

Viewing outstanding access requests

When requests for temporary access to targets are first received they are known as outstanding access requests which you should action accordingly. The status of these requests is set to pending.

To view the **Outstanding Access Requests** list click **Reports** > **Outstanding Access Requests**.

The list of all outstanding access requests is displayed.

Viewing live access requests.

When requests for temporary access to targets have been granted they are known as live access requests meaning that the temporary access is available during the specified time period. The status of these requests is set to granted.

To view the **Live Access Requests** list click **Reports** > **Live Access Requests**.

The list of all live access requests is displayed.

Viewing all access requests.

Unless a request for access has been deleted it will remain in the IBM Endpoint Manager for Remote Control database until the defined time period for it expires. Up to that point it can be set to three different states. To show all defined requests for access and their states you can use the **All access requests** option. The state of the request is listed as a number and corresponds to the following values

0 The request is pending and needs to be addressed. It is also displayed in the outstanding requests list.

1 The request has been granted. It is also displayed in the live access requests list.

2 The request has been rejected.

To view the All Access Requests list click **Reports** > **All Access Requests**.

The list of all access requests is displayed.

Chapter 11. Generating custom reports

There are two types of reports that can be generated in the IBM Endpoint Manager for Remote Control server. Common reports are reports provided with the application and are aimed at generating general information that you might need on a more regular basis. These reports can be run from the relevant menus within the IBM Endpoint Manager for Remote Control Server menu bar. Custom reports are reports that you have created or modified and generate information specific to your own environment. This section describes how to create, edit and run custom reports.

Note: Please note that a report manager is used for controlling the output of the reports. The function of this is to cache the output from the report and re display this when the report is next run for a quicker display of the results, so that the application does not need to go back and reload the data from the database. There are three properties in the `trc.properties` file that you can use to set the interval for reloading of the data from the database.

- **`report.timeout.frequency`**
- **`report.manager.frequency`**
- **`report.manager.period`**

For more details of these properties, see “trc.properties” on page 172.

It should also be noted that the **Refresh** link on the upper right of the screen can be used to reload the output of a report to show any changes in the data.

Creating a Custom Report

Custom reports are typically created by a Super User or Administrator and are useful for generating reports that specifically meet the needs of their environment. To generate a custom report a customized SQL query is run against the database and its output is displayed on screen.

Custom reports can be created in a number of ways

- By sorting, filtering or removing columns from a generated reports to meet your own requirements.
- By directly editing the SQL that is used for generating the report..

  Note: A good understanding of how to use SQL is required, to successfully complete this method.
- By creating a new report using the Edit SQL feature to build a query by adding required tables and columns. This can be done in two ways.
  - By selecting the New option in the Reports menu to create a new report
  - By using an existing report as the basis for the new report.

  For this option an understanding of SQL and the database tables and their associated columns is required . For details of the database tables, see Chapter 31, “Database table and column descriptions,” on page 283.
- By adding database tables and columns to existing reports.

Creating a report by Sorting and Filtering

You can create a custom report by sorting and filtering the columns of an already defined report. To do this generate the report that is used as the basis for your new report then perform the sort or filter option on this generated report.

To create the custom report complete the following steps :

1. Generate the report from the menus by completing the following steps:
   a. Click the menu that contains the required report. For example the **Targets** menu or **All Custom Reports**.
   b. Click the required report. For example All Targets.
2. The report that is generated can be manipulated to your requirements by doing **any or all** of the following actions :
   - **Sort, Move or delete a column**
     – Click the heading of the required column that you want to work on.
     – An icon with four arrows is displayed at the top of the column.
     – Hovering the mouse over the icon, displays the actions for the arrows. These are
       - sort up (Ascending) - click the up arrow
       - sort down (Descending) - click the down arrow
       - move the column to the left - click the left arrow
       - move the column to the right - click the right arrow
       - delete the column - click the cross in the centre

       Note: If the key column of a report is deleted it should be noted that some of the actions in the menu on the left will not be available.
     – The report is re-displayed in the order you selected.
   - **Filter a column**
     – If you click on any cell in the report the column that the cell is in is limited to the value that you selected.

       for example : If you select IBM in the Manufacturer column when All Targets are displayed, only those targets manufactured by IBM are re-displayed.
   - Repeat step 2 till you have the report to your requirements
3. To save this new report complete the following steps :
   a. Click **Reports** > **Save As Custom Report**.
   b. Change the name in the **Query name** field to one relevant for the new report.
   c. If required, change or delete the description in the **Description** field.
   d. Enter a menu name. This name is displayed in the **Custom Reports** menu.
   e. From the Groups list, select any Groups that should have access to this report.

      Note: The created report is only displayed in the Custom Reports menu of the Admin user or Super User who created the report. If a group or groups is selected in the step above, the report is also displayed in the Custom Reports menu of any Users who are members of the selected Groups.
   f. Click **Submit**.

The report is displayed and its name is displayed in the submenu of the **Custom Reports** menu.

Creating a report by editing the SQL statement

If you have some knowledge of SQL you can create a custom report by editing the SQL query used to generate an existing report. To do this complete the following steps :

1. To generate your base report, perform step 1 on page 96 Generate the base Report
2. Click **Reports** > **Save custom query**.
3. In the SQL data field, make the required changes to the SQL .
4. There are two options available now
   - To check the output of the Report go to step 5.
   - to save the Report go to step 7.
5. Click **Run Report**.
6. If the generated Report is what you require go to step 7, otherwise complete the following actions
   - Click **Reports** > **Save As Custom Report**.
   - repeat from step 3 above till the report meets your requirements.
7. Select **Reports** > **Save custom query**.
8. Change the name in the **Query name** field to one relevant for the new report.
9. If required, change or delete the description in the **Description** field.
10. Enter a menu name. This name is displayed as a menu item in the **Custom Reports** menu.
11. From the Groups list, select any Groups that should have access to this report.

    Note: The created report is displayed only in the Custom Reports menu of the Admin User (or Super User) who created the report . If a group or groups is selected in the step above, the report is also displayed in the Custom Reports menu of any users who are members of the selected Groups.
12. Click **Submit**.

Your custom report is created.

Note:

1. Click **Reset** on the Edit Custom Report and Group Access Rights screen to clear or reset any changes made to the input screen.
2. Click **Cancel** on the Edit Custom Report and Group Access Rights screen to return to the previously displayed screen and the custom report is not created.

Creating a report using Edit SQL feature

Using the Edit SQL feature you can create a query, by adding the required tables, columns and any specific search conditions, that can be run to generate your report. For details of the IBM Endpoint Manager for Remote Control database table names and columns, see Chapter 31, “Database table and column descriptions,” on page 283.

You can use the Edit SQL feature in two ways

- Selecting the New option in the Reports menu.
- Editing the SQL of an existing report.

Note:

1. **In the set of screens that are used in Edit Report, only click Submit when you have finished creating and adding things to your report, otherwise click Back to return to the main Edit Report screen to continue adding to or modifying your report.**
2. In this section we will use the Users table as an example for creating the report.

Selecting the New option in the Reports menu to create a new report

1. Click **Reports** > **New**.
2. On the screen that is displayed, on the upper right, click **Edit SQL**.
3. On the Edit Report screen to start building the query for the new report, select **Add Table.**
4. On the Add Tables screen select the required table. For example, *COMMON.USER_GROUP*. Click **Add.**.
5. Repeat from step 3 to add more tables if you require.
6. Click **Back** to return to the Edit Report screen.
7. Click **Add Column** to select the columns to be displayed in the report. The Modify Report Columns screen is displayed

   Note: The Add Column option is only applicable if more than one table has been selected for the report. If you select only one table, the list is blank and the next step is not required.
8. From the list select the a column and click **Add**.
9. Repeat from step 8 till all required columns have been added.
10. Click **Back** to return to the Edit Report screen.
11. If you want to **delete** a column complete the following steps
    a. Select **Delete Column**
    b. On the Delete Report Columns screen select the required column and click **Delete**.
    c. Repeat the above step to delete more columns. In this example click Delete till the first column in the list is **GROUP_KEY**.
    d. Click **Back** to return to the Edit Report screen.
12. If you want to re arrange the Report columns complete the following actions
    a. Select **Arrange Columns** on the Edit Report screen.
    b. On the Order Columns screen select the required column from the pull down and click < or > to move the columns to the left or the right. In this example select USER_GROUP.NAME then click the left arrow button till this column is first in the list.
    c. Repeat the previous step to re arrange more columns.
    d. Click **Back** to return to the Edit Report screen.
13. If you want to specify a condition in your query complete the following steps :
    - Click **Modify conditions** on the Edit Report screen.
    - On the **Modify Report Limits** screen choose the appropriate method to select a limit
      – Click on Quick Limits to select an already defined limit (if any have been defined) from the pull down
        - Click **add** to add this condition to your query.

- Click on **Back** to return to the Edit Report screen.

– Click on Add - to create an AND or OR condition for one of the columns in your query.

```
for example  AND USER_GROUP.NAME LIKE DefaultGroup
```

- The Modify Reports expanded screen is displayed
- Select **AND** or **OR** from the pull down.
- Select required column from the pull down.
- Select the required operator from the pull down.
- Enter the required value for the condition in the field, in the format and type that is specified on screen.
- The **Append column to query** selection can be used to select whether to display the condition column in the report. Select Yes or No.
- Click on **Add** to return to the Edit Report screen with the message

  ```
  Limit added : "AND USER_GROUP.NAME LIKE DefaultGroup"
  ```

  Which shows the limit as it will be used in the SQL query.

14. If you want to see the full SQL for the query that you have created, complete the following steps :
    a. Click **Edit SQL** on the Edit Report screen. The Edit SQL screen is displayed.
    b. Click **Update** if you make any changes.
    c. Click **Back** to return to the Edit Report screen.
15. To name your new report complete the following steps :
    a. Click **Edit Name** on the Edit Report screen.
    b. On the **Edit Name** screen type in a name for your report and click **Update**. The message `'Report was renamed '` is displayed on the screen.
    c. Click **Back** to return to the Edit Report screen.
16. **Submit** - At any time, in the sequence of events above, that you click **Submit**, the query that you have created is run and the report that this generates is displayed with the name that you defined, in **Edit Name**.
    - To Save this new Report complete the following steps :
      – Click **Reports** > **Save custom query**.
      – Change the **Query name** if required.
      – Enter a description for your report.
      – Enter a menu name. This name is displayed in the **Custom Reports** menu.
      – Select any Groups that should have access to the report.

        Note: The created report is displayed only in the Custom Reports menu of the Admin User (or Super User) who created the report . If a group or groups is selected in the step above, the report is also displayed in the Custom Reports menu of any Users who are members of the selected Groups.
      – Click **Submit**.

Note:

1. Click **Reset** on the Edit Custom Report and Group Access Rights screen to clear or reset any changes made to the input screen.
2. Click **Cancel** on the Edit Custom Report and Group Access Rights screen to return to the previously displayed screen and the Custom Report is not created.

Using an existing report as the basis for a new report

You can create a custom report using the Edit SQL feature on an existing report. To do this complete the following steps :

Generate the base report by selecting the required report from the relevant menu. For example to use the All Targets report as the base report, complete the following steps

1. Select **Targets** > **All targets**.
2. The All Targets Report is displayed.
3. Click **Edit SQL**, on the top right of the screen.
4. Follow from step 3 on page 98

Creating a report by adding tables and columns

You can create a custom report by adding database tables and columns to existing reports. For details, see "Adding a database table to a query" on page 109. After you have added the required tables and columns you can save the report.

To save the report complete the following steps:

Click **Reports** > **Save As Custom Report**.

1. Change the **Query name** if required.
2. Enter a description for your report.
3. Enter a menu name. This name is displayed as a menu item in the **Custom Reports** menu.
4. Select any Groups that should have access to this report.

   Note: The created report is displayed only in the Custom Reports menu of the Admin User (or Super User) who created the report. If a group or groups is selected in the step above, the report is also displayed in the Custom Reports menu of any users who are members of the selected groups.
5. Click **Submit**.

Running a Custom Report

Custom Reports can be run using one of the following methods.

- From the Custom reports menu
- By generating a list of Custom Reports and selecting one to run .

Choose the appropriate method for running a custom report

1. **Running a report from the Custom reports menu**
   a. Click **Reports** > **Custom Reports**. A list of Custom Report menus or available Custom Reports is displayed.
   b. Click the required Custom Report name.
2. **Running a Custom Report from the Custom Reports list.**
   a. Click **Reports** then select **All Reports**, **My Custom Reports** or **All Custom Reports**.

      Note: All Reports is the **only** option available to a **Super User**.
   b. If you selected **All Reports** , select **User Custom Reports**. If **My Custom Reports** or **All Custom Reports** was selected, select the required Report from the list.

c. From the **Reports** menu or from the Action List on the left, select **Run.**

The Custom Report is generated and it's results are displayed on the screen.

Viewing Custom Reports

Any Custom reports defined in the system can be viewed in two ways,

- By selecting the **All Custom reports** or **My Custom Reports** menu items.

  Note: This method is not available to Super Users
- By running the **User Custom Reports** report from the **All Reports** list.

To view the Custom Reports complete the procedure in step 1 or step 2 :-

1. **Viewing Custom Reports by selecting the All Custom Reports or My Custom Reports menu items**
   a. Click **Reports**.
   b. Click **All Custom Reports** to display the list of **all** defined custom reports or **My Custom Reports** to display the list of custom reports created by the currently logged on administrator.
2. **Viewing Custom Reports by running the User Custom Reports, report**
   a. Click **Reports** > **All Reports**.
   b. Select **User Custom Reports**.
   c. From the **Reports** menu or the Action list on the left, select **Run**.

The User Custom reports list is displayed listing all custom reports created by the currently logged on Super User or Administrator.

Managing custom reports

When you view a list of Custom Reports there are a number of actions available that can be performed when you select one or more custom reports from the list .

Edit Custom Report and Access
Use this action to change details about the custom report and also change the group access to this report by selecting or deselecting groups in the list.

Remove my access
Use this action to remove one or more custom reports from **your** Custom Reports menu.

Delete Custom Report
Deletes the selected custom reports.

Using the Edit Custom Report and Access feature

Use the *Edit Custom report and Access* feature to select a custom report and edit its details. The name, description and menu name can be changed although its main use would be to add or remove group access to the report or to edit the reports SQL.

To use the Edit Custom report and Access complete the following steps : -

1. Select **Reports**.
2. To generate a list of Custom reports **Click All Reports**, **My Custom Reports** or **All Custom Reports.**

Note: A Super User will only be able to generate the **All Reports** list.

3. If **All Reports** has been selected go to step4 for **My Custom Reports** or **All Custom Reports** go to step 6
4. Select **User Custom Reports**.
5. From the **Reports** menu or the Action list on the left, select **Run**.
6. Select the required report from the list.
7. Choose the appropriate method for actions: -
   - Click **Reports** > **Edit Custom Report & Access**.
   - OR select **Edit Custom Report & Access** from the actions list on the left.
8. The Edit Custom Query and Group Access Rights screen is displayed
9. Change the **Query name**, **Description** or **Menu name** if required.
10. In the SQL data field, make any required changes to the SQL .

    Note: A good understanding of how to use SQL is required to do this.
11. Select or deselect the required Groups for access.

    Note: The created report is displayed only in the custom reports menu of the Admin User (or Super User) who created the Report. If a group or groups is selected in the step above, the report is also displayed in the Custom Reports menu of any Users who are members of the selected Groups.
12. There are two options available now
    - To save the Report and finish, click **Submit**.
    - To check the output of the report go to step 13.
13. Click **Run Report**.
14. If the generated report is what you require click **Submit**, otherwise complete the following
    - From the **Reports** menu select **Save custom query**.
    - Repeat from step9 above till the report meets your requirements.

Removing your access to a report

Use the Remove My Access feature to remove one or more Custom Reports from **your** Custom Reports menu.

To perform **Remove My Access** complete the following steps : -

1. Select **Reports**.
2. To generate a list of Custom reports Click **All Reports**, **My Custom Reports** or **All Custom Reports.**

   Note: A Super User will only be able to generate the **All Reports** list.
3. If **All Reports** has been selected, select **User Custom Reports** , then select **Run** from the **Reports** menu or the Action list on the left.
4. If **My Custom Reports** or **All Custom Reports** has been selected, select the required reports from the list.
5. Choose the appropriate method for actions : -
   - Click **Reports** >**Remove My Access**.
   - OR select **Remove My Access** from the Actions list on the left

The currently logged on Super User or Administrator can no longer run the selected Custom reports from their Custom Reports menu.

This can be checked by completing the following steps :-

- Click **Reports**.
- This will result in one of two things
  1. If the custom report selected was the only custom report that the Super User or Administrator had created, Custom Reports will no longer be a menu item in the Reports menu.
  2. If the Custom Reports menu item is still present in the Reports menu
     a. Click **Custom Reports**.
     b. The selected Custom reports should not be present in the menu or any sub menus.

Note: As an Administrator has access to all Custom reports, they can still run the selected Custom reports by running them from the All Custom Reports, report.

Deleting custom reports

Use the Delete Custom Report feature to delete one or more Custom Reports.

To perform **Delete Custom Report** complete the following steps : -

1. Select **Reports**.
2. To generate a list of Custom reports Click **All Reports**, **My Custom Reports** or **All Custom Reports** .

   Note: A Super User will only be able to generate the **All Reports** list.
3. If **All Reports** has been selected go to step4 for **My Custom Reports** or **All Custom Reports** go to step 6.
4. Select **User Custom Reports**.
5. From the **Reports** menu or the Action list on the left, select **Run**.
6. Select the required reports from the list.
7. Choose the appropriate method for actions :-
   - Click **Reports** > **Delete Custom Report**.
   - OR select **Delete Custom Report** from the Actions list on the left.

The list of reports is refreshed and the selected custom reports is no longer in the list.

Chapter 12. Managing the home page for a user or group

When you log on to the IBM Endpoint Manager for Remote Control Server, the first page that is displayed is the default home page. There are a number of options you can use to set your own home page, set the home page for a user, or set the home page for a group of users. If you have a list of targets that you access regularly, you can create a favorites list and set this to be your default home page. If you want a group of users to see a list of specific targets when they log on, you can create a custom report to display these targets and set this as their default home page. The page that is displayed when a user logs on to the IBM Endpoint Manager for Remote Control Server is determined by which of the following conditions is satisfied.

1. Does the user have a default home page set?

   Yes This is the page that is displayed when the user logs on.

   No Check the users groups for a home page set.

2. Do any of the groups that the user belongs to have default a home page set?

   Yes

   - If only one group has a default home page set, this is the page that is displayed when the user logs on.
   - If more than one group has a default home page set, the home page that was most recently set for the groups is displayed.

   No the `trc.properties` file is checked.

3. If no default home page has been set by the user or for any groups that the user belongs to then the value of the **`default.homepage.method`** property in the `trc.properties` file is used.

   Note: The value of **`default.homepage.method`** is set to report by default, which displays the report defined in the **`default.query`** property. This is the **All targets** report by default. If **`default.homepage.method`** is set to search, the search targets page is displayed when the user logs on. For more details, see "trc.properties" on page 172.

From the steps above it is important to note that the default home page set by the user overrules any home page that has been set for the groups that the user belongs to. For example, user1 sets his default home page to his ***favorites*** list of targets. User1 is a member of user group testusers. You create a custom query of all targets manufactured by ***companyX*** and set this to be the default home page for user group testusers. However when user1 logs on it is his ***favourites*** list that is displayed as the home page.

Creating and setting a home page

You can use any of the standard reports that come with IBM Endpoint Manager for Remote Control and set them to the default home page or you can create your own custom report and set it to the default page.

Setting a default home page as a user

To set a default home page, complete the following steps:

- Choose the appropriate method for generating a relevant report.

– Run a standard report from any of the IBM Endpoint Manager for Remote Control Server menus
– Run a custom report that you have access to from the **Custom reports** menu.

For details of how to create and save a custom report, see "Creating a Custom Report" on page 95.

- Click **Options** > **Set Current Report as Homepage**

For example, to make the favorites report your home page:

- Click **Targets** > **Favourites**
- Click **Options** > **Set Current Report as Homepage**

Your home page is set and the following message is displayed. `Your home page has been set to report` *XXXXXXX*, where *XXXXXXX* is the name of the report that you set. For example, `Your home page has been set to report Favorites`.

When you log on to the server, the **Favourites** report is the first screen that is displayed.

Setting a home page for a group

A default home page for groups can be set by using custom reports. You can set the default home page for a group in two ways:

- By editing the access for a saved custom report.

  Note: Only Administrators have authority to edit the access for a custom report.
- When you save a custom report.

To set a default home page for a group, complete the following steps.

1. Choose the appropriate method for setting the home page
   a. By editing the access for a saved custom report.
      1) Select **Reports** > **My Custom Reports** or **Reports** > **All Custom Reports**
      2) Select the report.
      3) Select **Edit Custom Report & Access** then goto step 2.
   b. When you save a custom report.
      1) Generate the custom report. For details of the various ways that a custom report can be generated, see "Creating a Custom Report" on page 95.
      2) When you generate your report click **Reports** > **Save As Custom Report**.
2. On the Edit Custom Report and Group Access Rights screen type in a name and menu name for the report.
3. In the Group list select **Make Default Homepage** next to each group that can have this new report as their default home page.
4. Click **Submit**.

The default home page is set for the selected groups. Whenever a user who is a member of the selected groups logs on to the IBM Endpoint Manager for Remote Control Server, the saved report is displayed as their home page.

However, if the user also has a default home page set, they see their default home page instead.

Viewing the default home page list

When a user sets their own default home page or you set the default home page for a group, you can view the default home page list by completing the following steps:

1. Select **Reports** > **Default homepages**.
2. Select one of the following options:

   For user groups
   The list of defined user groups is displayed. The name of the report that is set as the default home page is shown in the **Name** field.

   For Users
   The list of users who have a default home page set is listed.

Editing the default home page for a group

You can change the default home page that is set for a group by using the **Edit Group Homepage** option. The option is available when you view the **Group home pages** report.

To edit the default home page complete the following steps:

1. Select **Reports** > **Default homepages** > **For user groups**.
2. Select one of the groups in the list.
3. From the **User groups** menu or the Action list on the left, select **Edit Group Homepage**. The Edit group default homepage page is displayed showing the list of custom reports that are defined.
4. Choose the appropriate method for selecting the home page.
   - Select **None**. The users in the group no longer have a custom report set as their home page.
   - Select one of the listed custom reports. This report is saved as the new home page for the group members.
5. Click **Submit**.

When members of the selected group logon to the server, the new default home page is displayed.

Reset the default home page

When a default home page is set for a user or a group, you can reset the default home page by using the following options.

- **Reset User Homepage**
- **Reset Group Homepage**

Resetting the default home page for a user

If a user has a default home page set, the page is displayed when the user logs on. To change the home page use**Reset User Homepage** to reset their home page. The next time that the user logs on, the home page that is set for any groups that they belong to is displayed. If the groups do not have a home page set, the default home page, as defined in `trc.properties`, is displayed.

To reset a users default home page, complete the following steps:

1. Select **Reports** > **Default homepages** > **For users** .

2. Select the users.
3. From the **Users** menu or the Action list on the left, select **Reset User Homepage**.

A message is displayed when the home page is reset.

The next time that the user logs on, the home page that is set for any groups that they belong to is displayed. If the groups do not have a home page set, the default home page, as defined in `trc.properties`, is displayed.

Resetting the default home page for a group

To reset a groups default home page, complete the following steps:

1. Click **Reports** > **Default homepages** > **For user groups**.
2. Select one of the groups in the list.
3. From the **User groups** menu or the Action list on the left, select **Edit Group Homepage**. The Edit group default homepage page is displayed showing the list of custom reports that are defined.
4. Choose the appropriate method for selecting the home page
   - Select **None**. The users in the group no longer have a custom report defined as their home page. The home page is set to the default home page as defined in the `trc.properties` file.
   - Select one of the listed custom reports. This report is saved as the new home page for the group members.
5. Click **Submit**.

The next time any of the members of the selected group logs on, the new default home page is displayed.

Chapter 13. Options menu functions

Use the options menu in the IBM Endpoint Manager for Remote Control Server to carry out actions on any reports that are produced. There are various things that can be done from this menu and this section details those options which are available to super user and admin users only. See the IBM Endpoint Manager for Remote Control Controller User's Guide for additional options which are available to all users. This section details the options you can use to add additional data to your reports by adding database tables and columns to the query that is run to generate the report data. A knowledge of the database tables is required for using this option. For details of the database tables and columns, see Chapter 31, "Database table and column descriptions," on page 283.

Note: On screens that are not in a report format, for example search screens or input screens, the Options menu is not visible in the menu bar.

Adding a database table to a query

When a report is displayed on the screen you can add additional data to it by adding one or more database tables to the query that is used to generate the data. After you have added a new table you can add one or more columns from the new table to the report.

To add a new database table complete the following steps :

1. Click **Options** > **Add Table to Report**
2. Select the required database table from the list.

A message is displayed showing that the table was successfully added. To add the required database columns to the report, see "Adding a database column to a query."

Adding a database column to a query

After you have added a database table to your report you can add one or more columns from the table to the report by selecting the **Add Column to Report** option. The report is displayed with the new columns added.

To add a new column complete the following steps :

1. Click **Options** > **Add Column to Report**
2. Select the required database table then the required column from the list.

A message is displayed showing that the column was successfully added and the report is displayed with the new columns added. To add additional columns repeat from step1

Chapter 14. Admin Menu Functions

The Admin menu in the IBM Endpoint Manager for Remote Control Server provides you with configuration and troubleshooting information. The following options are available in the menu

- **Edit properties file**
- **View Application Log**
- **Send Application Log**
- **Import Data**
- **View Current Server Status**
- **All Remote Control Gateways**
- **New Remote Control Gateway**
- **Reset Application**
- **New Permission Set**
- **All Permissions Sets**
- **Target Membership Rules**

Editing the properties file

Use the **Edit Properties Files** option to edit the various property files that are present in the system to configure IBM Endpoint Manager for Remote Control to your own requirements.

The following properties files are avialable in IBM Endpoint Manager for Remote Control

- `trc.properties`
- `log4j.properties`
- `ldap.properties`
- `common.properties`
- `appversion.properties`
- `controller.properties`
- `ondemand.properties`

For details of the variables and relevant values that are required for these files, see Chapter 21, “Editing the properties files,” on page 171.

Configuring LDAP properties using the LDAP wizard

The LDAP properties file is initially installed with default values that can be changed to your requirements. You can use the LDAP configuration utility to test the connection to your LDAP server and correctly configure your user and group search parameters. This utility can be used to change and test LDAP property values to determine the correct configuration for importing the required user and group information from your LDAP server to the IBM Endpoint Manager for Remote Control database.

Note: The utility only configures the connection, user and group search properties, for details of enabling LDAP and additional LDAP configuration parameters see the IBM Endpoint Manager for Remote Control Installation Guide.

Using the LDAP configuration utility

The LDAP configuration utility contains four sections that you can use to configure and test certain LDAP properties to determine the correct values for your requirements.

1. Connection
2. Group search
3. User search
4. Other settings

You must complete section 1 before you can access and use the remaining sections.

To access and run the utility select **Admin** > **LDAP Configuration Utility**.

The LDAP configuration utility is displayed.

Testing your LDAP connection

The first step when using the LDAP configuration utility, is to test that you can successfully connect to your LDAP server. This section must be completed and verified before you can continue using the utility. To test your LDAP connection complete the following steps :

1. Enter the connection information.

   Connection URL
   Defines the URL used to connect to your LDAP server.

   Connection Name
   This should be set to the userid defined for authenticating a read-only LDAP connection with the LDAP server. This username should contain all the rights necessary to read all the required information from the directory tree.

   Connection Password
   This should be set to the password defined for authenticating a read-only LDAP connection with the LDAP server. You can enter a plain text or an encrypted password.

   If you enter a plain text password you can encrypt this by clicking **Encrypt Password** .

   Note: When you click **Encrypt Password** , **Connection Password Encrypted** is automatically selected.

   If you enter an encrypted password you should also select **Connection Password Encrypted**.

   Connection Password Encrypted
   determines whether the password is treated as encrypted or not. If you select **Connection Password Encrypted** the password is treated as encrypted if you do not select it, the password is treated as plain text.

   Note:

   a. This is automatically selected when you click **Encrypt Password**.

b. If you have entered an encrypted password in the **Connection Password** field and deselect **Connection Password Encrypted** the password will not be decrypted, it will remain encrypted for security reasons.

Alternate URL
Defines a secondary LDAP server name. If the primary LDAP server is down you can use the alternative LDAP server for authentication.

Security Authentication
Select the required security authentication. Specifies the security level to use. If using SSL select **Simple**. If using SASL select **DIGEST-MD5**.

2. Click **Test Connection**.

Connection OK is displayed if a successful connection, to the LDAP server, is made. If a connection is not possible, **Connection Error** is displayed. Click on the question mark for more details of what is causing the error.

When you have a successful connection to your LDAP server you can then configure and test group and user search parameters.

Configuring LDAP group search parameters

The Group Search section is used to search for groups in the LDAP directory tree starting the search at the directory location defined in the **GroupBase** field, and using the search query specified in the **Group Search** field.

1. Enter the group search information. You can click the question mark next to each field for more information.

Group Base
Specify the LDAP directory that you want to start the group search from. If this is left blank the search is started from the top level element in the directory, for example `OU=location,DC=domain,DC=com`. You could refine your search by going deeper into the OU structure and selecting to start the search from within a specific organisational unit, for example an OU called Test, therefore you would set the property value as `OU=Test,OU=location,DC=domain,DC=com`. This would instruct IBM Endpoint Manager for Remote Control to look for groups matching the criteria, starting the search at the Test OU level of the directory tree (and any OUs that belong to the Test OU if Group Subtree is selected) .

Note: You can use the Browse icon to the right of the field to navigate through your directory structure and select a specific starting location.

Group Search
Specify the LDAP filter expression to be used for performing the group search. `For example (objectClass=group)`. The defined expression needs to filter the results such that only the required groups are imported to the IBM Endpoint Manager for Remote Control database. The default value is `(objectClass=group)` which means, look for users in any object that is a group within the specified groupbase. That is, import all Active Directory groups to IBM Endpoint Manager for Remote Control.

Note: When using `(objectClass=group)` it should be noted that some environments can have thousands of groups therefore it is important to create a filter which will only import the required groups. The search can therefore be further refined by using more complex queries . For

example the following values
`GroupBase=(OU=location,DC=domain,DC=com) GroupSearch=(&(objectClass=group)(name=Dep*))` would return any groups within the **location OU** whose name starts with **Dep**. For example groups with names `department1` or `deputy`.

Group Subtree
Select this if you want to recursively search the subtree of the element specified in the GroupBase attribute for groups . If not selected, only the top level is searched. Default is not selected.

Group Name
The LDAP attribute name that is used to perform a group search. This is set to **name** by default.

Group Description
The LDAP attribute name to be used to get the description for this group. This is set to **description** by default.

Group Membership Attribute
The 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.**

2. Click **Test Groups Search**. A message box is displayed with the total number of groups found as a result of the search. Click **OK**.

   Note: If there are more than 100 groups found from the search, the following message is displayed. *XX* `Groups found.(Only the first 100 are shown.)` - where *XX* is the total number of groups found.

The resulting groups are displayed in the text box on the right and this is the list of groups that will be imported from LDAP when you have LDAP synchronisation enabled. You can click the icon to the left of each group name to see a list of the LDAP attributes and values defined for the group.

When you have achieved the required group search results you can use the User search section of the utility to configure and test values for your User Search LDAP properties, by following the steps in "Configuring LDAP user search parameters" or save your current configuration by following the steps in "Saving your LDAP configuration" on page 118.

Configuring LDAP user search parameters

Use the User Search section to search for users in the LDAP database. The search starts at the directory that is defined in the **User Base** field, and uses the search query that is specified in the **User Search** field.

Note: Depending on the type of LDAP server that you install, click **Set Defaults** to load the LDAP utility with the default parameter values for your server type.

1. Enter the user search information. Click the question mark next to each field for more information.

   User Base
   Specify the LDAP directory that you want to start the user search from. If left blank, the search is started from the top-level element in the directory. For example, `OU=location,DC=domain,DC=com`. You can refine your search by going deeper into the OU structure and select to start the search from within a specific organizational unit. For example, to

start from an OU called Test, set the User Base value to `OU=Test,OU=location,DC=domain,DC=com`. The search starts at the Test OU and looks for users that match the **User Search** criteria. If **User Subtree** is selected, any OU that belongs to Test OU is also searched.

Note: Use the **Browse** icon to the right of the field to navigate through your directory structure and select a specific starting location.

User Search
Specify the LDAP filter expression to be used for the user search. `For example (objectClass=user)`. The defined expression must filter the results such that only the required users are imported to IBM Endpoint Manager for Remote Control. The default value is `(userPrincipalName={0}@MyCompany.com)`. {0} is substituted with the user ID that is used to log on to IBM Endpoint Manager for Remote Control, and *MyCompany.com* is the host name of your LDAP server. That is, look for users whose **userPrincipleName** matches any users that are found within the specified **UserBase**.

Note: Some environments have thousands of users. Therefore, it is important to create a filter that imports only the required users. To limit the users to only those users who are members of groups that are imported into IBM Endpoint Manager for Remote Control through the **GroupSearch** filter, you must select **User Must be in a Group**. If this property is not selected, the users that do not belong to any of the imported LDAP groups are automatically assigned to the **DefaultGroup** user group. The search can therefore be further refined by using more complex queries. For example, set the following values. `GroupBase=(OU=location,DC=domain,DC=com) UserSearch= (&(objectClass=user)(|(memberOf=CN=Department1,OU=GROUPS, OU=location,DC=domain,DC=com) (memberOf=CN=Department3,OU=GROUPS, OU=location,DC=domain,DC=com))(name={0}))` Define three groups, `Department1, Department2`, and `Department3`. The query authenticates and imports any users that have an **objectClass** value equal to user and that are members of the groups `Department1` OR `Department3`. Users from `Department2` cannot log on to IBM Endpoint Manager for Remote Control because they are not imported. The (&(name={0}) is added to the end to specify that the name attribute is used for logging in. This value must match whatever attribute was specified as **userid**.

User Subtree
Select this option if you want to recursively search the subtree of the element that is specified in the **UserBase** attribute for users. If not selected, only the top level is searched. The default state is not selected.

User Must be in a Group
Select this option to limit the users that are imported to only those users who are members of groups that are imported into IBM Endpoint Manager for Remote Control through the **GroupSearch** filter. The default state is not selected.

LDAP attributes
Type which user-specific LDAP attribute names must be used for importing the required user details into the corresponding IBM Endpoint Manager for Remote Control user properties.

Userid

The user ID is the LDAP attribute that contains the user ID that is chosen to be mapped to the **userid** field in IBM Endpoint Manager for Remote Control.

sAMAccountName

sAMAaccount must be set to use the userid only portion of the logon (without the UPN Suffix).

userPrincipalName

userPrincipalName must be set to force all logons to use the full User Principal Name.

Note: It is recommended to set **Userid** to the **userPrincipalName** value to ensures that the user ID that is entered is not reported as containing invalid characters. For example, an apostrophe.

User Password

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

User Email

The name of the LDAP attribute in the user's directory entry that contains the users email address.

Note: User Email must not have a null value. If your Active Directory Tree does not contain email information, a different attribute must be used. For example, it can be set to `userPrincipalName`.

Employeeid

The name of the LDAP attribute in the user's directory entry that contains the user's employee ID.

Title The name of the LDAP attribute in the user's directory entry that contains the user's title.

Forename

The name of the LDAP attribute in the user's directory entry that contains the user's given name.

Initials

The name of the LDAP attribute in the user's directory entry that contains the user's initials.

Surname

The name of the LDAP attribute in the user's directory entry that contains the user's surname.

Department

The name of the LDAP attribute in the user's directory entry that contains the user's department.

Company

The name of the LDAP attribute in the user's directory entry that contains the user's company.

Location

The name of the LDAP attribute in the user's directory entry that contains the user's location.

Floor The name of the LDAP attribute in the user's directory entry that contains the user's floor.

Address_1
The name of the LDAP attribute in the user's directory entry that contains the user's address_1 details.

Address_2
The name of the LDAP attribute in the user's directory entry that contains the user's address_2 details.

Town The name of the LDAP attribute in the user's directory entry that contains the user's town.

Country
The name of the LDAP attribute in the user's directory entry that contains the user's country.

State The name of the LDAP attribute in the user's directory entry that contains the user's state.

telephone
The name of the LDAP attribute in the user's directory entry that contains the user's telephone number.

Mobile
The name of the LDAP attribute in the user's directory entry that contains the user's mobile number.

2. Click **Test User Search** A message box is displayed with the total number of users that are found as a result of the search.
3. Click **OK**

Note: If more than 100 users are found from the search, the following message is displayed. *XX* `Users found.(Only the first 100 are shown.)` - where *XX* is the total number of users found.
The resulting users are shown in the text box and the list of users would be imported from LDAP when you have LDAP synchronization enabled. You can click the icon to the left of each user name to see a list of the LDAP attributes and values that are defined for the user. Click the icon to the right of the user name to display the IBM Endpoint Manager for Remote Control user field values. The user field values are imported into the IBM Endpoint Manager for Remote Control database.

When you achieve the required user search results, you can save your current configuration by following the steps in "Saving your LDAP configuration" on page 118.

Configuring additional LDAP settings

Use the **Other settings** section of the LDAP configuration utility to configure additional LDAP properties.

Page Size
Set this value to the page size of LDAP search retrievals. Do not set this to anything greater than the maximum page size for the LDAP server. Default is 1000.

Saving your LDAP configuration

When you have achieved your required results from the Group and User search parameters that you have entered, you can save the configuration by clicking **Save**. Your values are saved to the LDAP properties file and these are loaded into the utility the next time that you run it.

Note: If you click **Cancel** before clicking Save, the values will not be saved to the LDAP properties file.

Viewing the application log

The application log lists all server activity that takes place. The latest activities are appended to the end of the file. You can use this file to look for errors if a problem occurs.

To view the application log click **Admin** > **View Application Log**

The application log is displayed, click **CTRL + END** to reach the end of the file.

Saving the application log for exporting

If a problem occurs you can save the application log to a file by using the **Send Application Log** option. This file can then be sent to support for debug purposes.

To save the application log complete the following steps :

1. Click **Admin** > **Send Application Log**.
2. Click **Save** to save to a specific location.

The file is saved as `trc.log`.

Note: Click **open** to open the `trc.log` file in text mode.

Importing data into the database

You can use the Data Import option to import data into the IBM Endpoint Manager for Remote Control database. For details of this function, see "Import data from csv files into the IBM Endpoint Manager for Remote Control database" on page 276.

Viewing the server status

To view the current server status click **Admin** > **View Current Server Status**.

The View Current Server Status screen is displayed.

Viewing the IBM Endpoint Manager for Remote Control Gateways

When you have created IBM Endpoint Manager for Remote Control gateways you can view the list of defined gateways. For details of installing gateway support and configuring gateway connections, see Chapter 20, "Accessing targets on different networks," on page 151.

To view all defined gateways click **Admin** > **All Remote Control Gateways**.

The list of defined gateways is displayed.

Editing a IBM Endpoint Manager for Remote Control gateway

To edit the details of a IBM Endpoint Manager for Remote Control gateway complete the following steps:

1. Click **Admin** > **All Remote Control Gateways**
2. Select the required gateway.
3. From the Admin menu or the Actions list on the left, select **Edit Remote Control Gateway**.
4. Change the required details.
5. Click **Submit**.

Deleting a IBM Endpoint Manager for Remote Control gateway

To delete one or more IBM Endpoint Manager for Remote Control gateways complete the following steps:

1. Click **Admin** > **All Remote Control Gateways**
2. Select one or more gateways.
3. From the Admin menu or the Actions list on the left, select **Delete Remote Control Gateway**.
4. On the Confirm Deletion screen click **Submit**.

The gateway details are removed from the IBM Endpoint Manager for Remote Control database.

Creating a IBM Endpoint Manager for Remote Control Gateway

If you have configured your network for gateway support and have controllers that need to connect to targets using the gateway configuration, you need to provide the server with details of the machines to be contacted to establish a connection between the controllers and targets.

To add a IBM Endpoint Manager for Remote Control gateway to the server, complete the following steps :

1. Click **Admin** > **New Remote Control Gateway**.
2. Supply the required information for your gateway

   Hostname
   Enter the hostname for your gateway.

   Description
   Enter a description for your gateway. This is optional.

   IP Address
   Enter the IP address of the system being used as the gateway.

   Port Enter the port that the gateway is listening for connections on.
3. Click **Add another IP address** to enter the IP address and port if the system you are using as the gateway has multiple IP addresses.
4. Click **Submit**.

   Note: Click Cancel to go back to the previously displayed screen.

When you have created a gateway you should configure your network for gateway support using the gateway configuration file. See “Configuring the gateway support” on page 151.

Resetting the Application

When updates have been made to the properties files, use **Reset Application** to force the application to load the new values from the database.

To reset the application click **Admin** > **Reset Application**.

The current screen is displayed with the following message displayed
`Reinitialised all application objects`

Note: If at any time a system hang occurs you will need to stop and restart the IBM Endpoint Manager for Remote Control server service.

Configuring the user acceptance window

When user acceptance is enabled for remote control sessions an acceptance window is displayed on the target system when the session is requested. The target user can use this window to accept or refuse the session. This window is displayed with standard text that is shipped with the product but you can also configure this text by using the **Configure session dialog** feature to change the content of the user acceptance window to your own requirements. You can display a specific icon, set a default locale and create a specific customization for selected locales to change the window title, and display customized text if required. For each of the locales that are listed in the **Configure Target session acceptance dialog** utility there is a set of translated standard text messages but if you create a customized locale it is the customized text messages that is displayed if the following conditions are satisfied.

- For the target locale is there customized text defined? If yes, display this customized text.
- If no, is there customized text defined for the selected default locale? If yes, display this customized text.
- If no, is there standard text defined for the target locale? If yes, display this standard text.
- If no, the text is displayed in US-English.

Note: This process is applied to each of the customizable text options separately, that is the title, paragraph 1 and paragraph 2. It is possible to display both custom and standard text. For example if you select a locale to customize, type in customized text for paragraph1 and paragraph2 and leave the window title field blank. The acceptance window, for a target configured for this locale, displays the standard window title and the customized paragraph1 and paragraph2 text.

To configure the session dialog complete the following steps:

1. Select **Admin** > **Configure session dialog**.
2. On the Configure Target session acceptance dialog window enter the required information.

   General

   Select an existing icon

   Select an icon to be displayed in the acceptance window. The selected icon is previewed on the right. You can upload your own icon files by using the **File Import** feature. For more details, see "Uploading user acceptance window icons" on page 124.

Hide mode selection
Select this to hide the session mode buttons on the user acceptance window.

selected

The session mode buttons that are valid for the remote control session are not displayed on the user acceptance window.

not selected

The session mode buttons that are valid for the remote control session are displayed on the user acceptance window. This is the default value.

Default locale
Select the required default locale. The default locale indicates which language is displayed when there are no translations available for the current locale of the target system. For example, if a target is configured for France, if a customized French translation is not available and English has been selected as the default locale, English text is displayed. If you do not want to set a default locale select **No default locale**.

Customisations
Shows the number of customized locales that have been created and saved.

Locale Customisation
You can create multiple customizations by selecting a locale, entering the required values and then clicking **Save**.

Locale Select the locale that you want to set customized options for.

Load customisations
You can use the load customization selections to populate the text fields with already saved text or to clear the text fields. Select the required option.

Load built-in text

Select this to populate the fields with the standard text. You can edit this if required.

Note: When you click **Save** after populating the fields with standard text it becomes the customized text for the selected locale.

Load default customisations

Select this to populate the fields with the customized text that has been saved for the default locale. You can edit this if required.

Note: If no default locale has been set, a message is displayed stating `there is no default locale defined`.

Clear customisable fields

Select this to clear the text fields.

Title Enter the customized text that will be displayed in the acceptance window title.

Paragraph 1
Enter the customized text that will be displayed in the first paragraph of the acceptance window.

Note: This usually contains any legal text that is required.

Paragraph 2
Enter the customized text that will be displayed in the second paragraph of the acceptance window.

Note: This usually contains any additional help text that is required.

3. When you have created the required customized options click **Save**. Click **Close** to exit from the Configure Target session acceptance dialog window.

   Note:

   a. If during the customization process you select a different locale you are given the following options

      Save Click this to save the options for the current locale.

      Don't Save
      Click this to clear the text fields and keep the newly selected locale available.

      Cancel
      Click this to return to the Configure Target session acceptance dialog window with the previous locale still selected.

   b. If you leave the **Title**, **Paragraph 1** or **Paragraph 2** fields blank no customized text is saved for that option.

After you have created and saved customized options, if a remote control session with user acceptance enabled is requested, the user acceptance panel is displayed on the target with thecustomized or standard text that has been configured and saved for the target machines locale.

Configuring the user acceptance window for a peer to peer session

When you use the configure session dialog feature in the IBM Endpoint Manager for Remote Control Server UI and save customized locales, these values are saved to the database and passed to the target machine when a remote control session is requested, to be saved in the following target properties. You can configure these properties locally on the target if the target will only take part in peer to peer sessions.

Note: If you set values locally for these properties and later the target takes part in remote control sessions started from the server, the local values are overwritten with values passed from the server.

CustomConfirmTitle
Use this property to define a customized window title for the user acceptance window. When there is no translation available for the locale that the target is configured for, the default string, that is saved in CustomConfirmTitle, is displayed for the window title. If you want a customized window title for specific locales you can create multiple CustomConfirmTitle.***X*** properties, where ***X*** is the locale. For example *CustomConfirmTitle.fr*.

ConfirmExtraText
Use this property to define a customized paragraph 1 for the user acceptance window. When there is no translation available for the locale that the target is configured for, the default string, that is saved in

ConfirmExtraText, is displayed for paragraph 1. If you want a customized paragraph1 for specific locales you can create multiple ConfirmExtraText.*X* properties, where *X* is the locale. For example *ConfirmExtraText.es*.

CustomConfirmOptions
Use this property to define a customized paragraph 2 for the user acceptance window. When there is no translation available for the locale that the target is configured for, the default string, that is saved in CustomConfirmOptions, is displayed for paragraph 2. If you want a customized paragraph 2 for specific locales you can create multiple CustomConfirmOptions.*X* properties, where *X* is the locale. For example *CustomConfirmOptions.zh*.

AllowSessionModeOverride
Use this property to determine whether the session mode buttons that are valid for the session are displayed on the acceptance window.

yes

The session mode buttons that are valid for the remote control session are not displayed on the user acceptance window.

no

The session mode buttons that are valid for the remote control session are displayed on the user acceptance window.

Configuring the user acceptance window on a windows target

Configure the user acceptance window properties locally on the target if the target will only take part in peer to peer sessions. For a Windows target you can edit the target registry to set the properties.

To configure the target properties in Windows complete the following steps

1. Run **regedit.exe**
2. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Tivoli\Remote Control\Target`
3. Choose the appropriate method for configuring the properties.
   - **Set a custom default string**
     a. Right-click the relevant property and select **Modify**

        Note: For details of the properties see, "Configuring the user acceptance window for a peer to peer session" on page 122.
     b. Type in the required string and click **OK**.
   - **Create a locale specific property**
     a. Right-click the right pane and select **New** > **String Value**
     b. Type in the name for the property with the locale and **ENTER**. For example `CustomConfirmTitle.fr`.
     c. Right-click the new property and select **Modify**
     d. Type in the required string and click **OK**.
4. Restart the IBM Endpoint Manager for Remote Control target service.

   If you want to add a custom icon to the acceptance window you can rename your file to `CustomConfirmIcon.bmp` and save the file to the directory defined in the **WorkingDir** target property.

   Note: The file should be 32 by 32 pixels in size and in BMP format.

Configuring the user acceptance window in Linux

You can configure the user acceptance window properties locally on the target if the target will only take part in peer to peer sessions. For a Linux target you can edit the target configuration file to set the properties.

To configure the target properties in Linux complete the following steps

1. Edit the `/etc/ibmtrct.conf` file.
2. Choose the appropriate method for configuring the properties.
   - **Set a custom default string**

     Type in the required default string for the relevant property.
   - **Create a locale specific property**

     Add an entry for the property with the locale and the required custom string. For example **`CustomConfirmTitle.fr`** = [custom string].
3. Save the file.
4. Restart the target service.

   If you want to add a custom icon to the acceptance window you can rename your file to `CustomConfirmIcon.bmp` and save the file to the directory defined in the **`WorkingDir`** target property.

   Note: The file should be 32 by 32 pixels in size and in BMP format.

Uploading user acceptance window icons

Use the **Import File** function in the IBM Endpoint Manager for Remote Control Server UI to upload icon files that you want to display in the user acceptance window. For details of what can be configured in the user acceptance window, see "Configuring the user acceptance window" on page 120.

To upload an icon file complete the following steps :

1. Click **Admin** > **Import Data** .
2. Select **Import File**.
3. In the **Upload icon for Session Acceptance Dialog** section click **Browse** and navigate to your icon file.

   Note: Icons must be in BMP format and 32 by 32 pixels in size.
4. Click **Submit**.

The uploaded icon files are displayed in the Configure session dialog window.

Creating a permission set

Use the create permission set option to create a set of policies that can be used to set temporary permissions when a user requests temporary access to a target. For details of creating these permissions see "Creating a set of permissions" on page 83.

Viewing the permissions sets

When you have created sets of policies and permissions you can view the list of these sets by using the **All Permissions Sets** action.

To view the list click **Admin** > **All Permission Sets**.

The View Permissions Sets screen is displayed listing all defined permissions sets.

Using rules to define target membership

Targets can be manually assigned to target groups using the *Manage Group Membership* function. However you can also create rules that will automatically assign targets to target groups whenever they contact the IBM Endpoint Manager for Remote Control Server server, depending on properties that have been set in the `trc.properties` file. These rules are used to match on the target's computer name, IP address or both and assign the target to the target group that is associated with the rule. If the target satisfies more than one rule it is assigned to the groups associated with these rules. Rules can be defined using the *Target Membership Rules* function to create, view, edit, change the order of and delete rules. Properties in the `trc.properties` file will determine when these rules are applied. You can use these rules to assign a target to multiple groups by checking the target computer name and IP address against all defined rules, this will assign the target to the groups associated with all matching rules. You can also limit this by setting a rule to stop any further checking and in this case the target is assigned to the groups associated with this matching rule and any previously processed rules that matched the target details.

Defining when membership rules are applied

If you are creating rules to determine a target's group membership you should configure the properties in `trc.properties` before allowing the targets to register with the server to ensure that the group membership is correctly assigned. You can configure these properties to assign targets to groups only once, at registration time, or to completely manage the target membership based on the defined rules. The following properties can be configured to determine when the target membership rules are applied.

rc.tmr.at.registration

Determines whether the target membership rules are applied to any new targets when they first contact the IBM Endpoint Manager for Remote Controlserver. Default value is **Yes**.

Set to Yes

Whenever a new target first contacts the server its computer name and IP address is checked against any defined rules and if matches are found, the target is assigned to the target groups associated with the rules.

Set to No

Whenever a new target first contacts the server its computer name and IP address are not checked against any defined rules. You will have to perform manual group membership on the target after it has registered with the server.

rc.tmr.at.every.callhome

Determines whether the target membership rules are applied every time a target contacts the IBM Endpoint Manager for Remote Control server. Default value is **No**.

Set to Yes

Each time a target contacts the server its computer name and IP address are checked against any defined rules and if matches are found, the target is assigned to the target groups associated with the rules. In this case the target's group membership is recalculated each time it contacts the server to incorporate any changes that may have been made to the target rules since the last time it contacted the server.

Set to No

Each time a target contacts the server its computer name and IP address are not checked against any defined rules.

rc.tmr.at.triggered.callhomes

Determines whether the target membership rules are applied any time a target contacts the IBM Endpoint Manager for Remote Control server due to a change in its computer name or IP address or if the target comes online. Default value is **Yes**.

Set to Yes

Each time a target contacts the server due to a change in its configuration, or when it comes online, its computer name and IP address are checked against any defined rules and if matches are found the target is assigned to the target groups associated with the rules.

Set to No

When a target contacts the server due to a change in its configuration, or when it comes online, its computer name and IP address are not be checked against any defined rules.

rc.tmr.at.rules.change

Determines whether the target group membership is immediately recalculated for any targets affected by an addition, deletion or change to a rule. When this property is enabled, any targets whose group membership was assigned using rules will have their group membership recalculated to incorporate the rule change. Default value is **Yes**.

Set to Yes

Each time you add or delete a rule, or make a change to a rule, the target group membership, for all targets whose group membership was assigned using rules, is recalculated. During this process any target whose computer name or IP address matches those in the rule that was changed, will have their group membership changed to reflect the change in the rule.

For example:

A *rule1* assigns targets with computer name starting with *test%* to the target group *testtargets*. Target *test1* contacts the server and is assigned to target group *testtargets*. If you edit *rule1* and change the computer name condition to starting with *admin%*, target *test1* has its group membership recalculated and is longer a member of *testtargets* as it does not satisfy the new condition, that is it's computer name does not begin with admin.

Set to No

The addition, deletion or change to a rule does not affect the target group membership of any targets whose group membership was assigned using the rules.

Note: The next time one of these targets contacts the server their group membership is recalculated if **rc.tmr.at.every.callhome** = Yes or **rc.tmr.at.triggered.callhomes** =Yes (the target has come online or has changed its computer name or IP address) and the following conditions are satisfied.

- their computer name or IP address satisfies the new rule
- they are effected by the rule that was deleted
- they do not satisfy the updated rule

Note: It should be noted that group membership of targets that have been manually assigned to target groups will not be modified by target rules.

```
For example :
If an administrator assigns target1 to target group T1 using
the Manage Group Membership function, it will remain a member of
T1 until it is manually removed from the target group or until
 the group is deleted.
```

Creating rules

You can create rules which will assign targets to target groups if their computer name or IP address matches conditions set in the rules. For example, you can assign targets whose IP addresses fall into a specific range of addresses to one or more target groups when they first register with the IBM Endpoint Manager for Remote Control Server or every time they contact the server. For details of properties affecting the group assignment, see "Defining when membership rules are applied" on page 125.

To create a rule complete the following steps :

1. Click **Admin** > **Target Membership Rules**
2. Select **Create new rule**.
3. On the New Rule screen supply the information required for creating the rule.

Computer name

Enter all or part of the computer name that should be checked against the target computer name. You can use % and ? as wildcard characters to denote multiple or one character respectively.

For example :

test - any targets whose computer name is test will satisfy this rule

admin% - any targets whose computer name starts with admin will satisfy this rule.

admin?? - any target whose computer name starts with admin and then another 2 characters will satisfy this rule, for example: admin22, adminGB

IP start

Enter the IP address which is at the start of the range of IP addresses that match with this rule.

Note: IPv6 is also supported in the IP ranges.

IP end

Enter the IP address which is at the end of the range of IP addresses that match with this rule.

Stop processing

Enable this if you want the group membership assignment to stop when the target details match this rule. If there are multiple rules defined, the computer name and IP address of the target that contacts the server is checked against every defined rule, however if you enable stop processing for a rule, as soon as a targets details match this rule, the server will not check the targets details against any other rules and it is assigned to the target groups that are associated with this matching rule and any previously processed matching rules.

Comments

Can be used to enter a description for the rule or for some other information. Optional field.

Priority

You can give the rule a priority level which will determine when it is checked against the target. The priority level starts at 1 and increments by one as each new rule is created. Priority 1 is the highest priority, this rule is the first to be checked against the target.

The first rule that is created is automatically assigned a priority 1 value. When you create the next rule you have the option of selecting priority 1 or 2 for this new rule. Selecting 1 will make the new rule the first rule to be checked. Each time you create a new rule you have the option of selecting a priority level and the rules are rearranged according to their priority levels from 1 to *n*, where *n* is the number of rules that have been created.

Note:

a. If you have rules that are required to be checked you should make them a higher priority to ensure that they are checked against the target. Rules with a lower priority, those further down the list, may not be reached if you have a rule with **Stop processing** enabled near the top of the rules list.

4. Select the required groups that you want the target to be assigned to if it matches the conditions for the rule.
5. Click **Submit**.

Viewing rules

After you have created rules for assigning targets to target groups you can view the list of defined rules by completing the following steps :

1. Click **Admin** > **Target Membership Rules**
2. Select **Show rules**.

The list of defined rules is displayed. You can select these rules to edit the rules definition or delete the rules.

Checking rules

You can enter a target's IP address or computer name and use the **Simulate against rules** function to check whether the target matches with any of the defined

rules. The rules are displayed and any rules that match are highlighted. You can see from the matched rule what target groups the target would be assigned to if it contacted the server.

To check the target's details against already defined rules, complete the following steps:

1. Click **Admin** > **Target Membership Rules**
2. Select **Simulate against rules**.
3. Type in the target details that you want to search on.

   IP address
   Type in the IP address that you want to check against the rules.

   Computername
   Type in the computer name that you want to check against the rules.
4. Click **Test**

The List of rules is displayed. Any rules that match the IP address or computer name are highlighted and the word **matched** is displayed next to it. You can also see from the matched entry which target groups the target would be assigned to. If no match is found, a message is displayed.

Editing rules

After you have created rules for assigning targets to target groups, you can edit a rule to change the conditions that will determine the target's group membership by completing the following steps :

1. Click **Admin** > **Target Membership Rules**
2. Select **Show rules**.
3. Select the required rule.
4. Select **Edit rule**.
5. Change the required information and select **Submit**.

The changes to the rule is updated and is used the next time a target's information is checked against the rule.

Deleting rules

After you have created rules for assigning targets to target groups you can delete these rules if they are no longer required. However there are 3 types of deletion that can be selected which result in the following actions taking place.

1) Leave target membership and target groups unchanged
You can select this option to just delete the rule and nothing else. Any targets whose group membership was assigned using this rule will remain members of the target groups that they were assigned to.

2) Reset target membership and preserve target groups
You can select this option to delete the rule and reset the target group membership. Any targets whose group membership was assigned using this rule will no longer be members of the target groups that were associated with this rule.

3) Reset membership and delete target groups
You can select this option to delete the rule, reset the target group membership and delete the target group. Any targets whose group membership was assigned using this rule will no longer be members of the

target groups that were associated with this rule and these target groups will also be deleted from the IBM Endpoint Manager for Remote Control database.

You can delete one or more rules by completing the following steps :

1. Click **Admin** > **Target Membership Rules**
2. Select **Show rules**.
3. Select the required rules.
4. Select **Delete rules.**.
5. On the Target Membership Rules screen select the type of deletion required.
6. Click **Submit**. If you have chosen deletion type 2 or 3 above, a warning message is displayed `WARNING! Resetting target membership or deleting groups cannot be undone`. Click **Submit** to continue with the deletion of the rule.

The target membership rule is deleted from the IBM Endpoint Manager for Remote Control database and the actions associated with the selected deletion option are carried out.

Chapter 15. Remotely installing the target software

Use the *Remote Install* function to install the target software onto a target that you do not have physical access to. You can download and install the target software from the IBM Endpoint Manager for Remote Control server, configuring the target in the same way that you would in a normal installation. You require a valid operating system administrator userid and password for the target and should have administrator rights for the target system.

Note: This utility can only be used to install the target software on one target at a time, it is not intended for mass distribution of the software. In Linux only the root user is allowed to perform this function.

Prerequisites for remote target installation

Note: The use of this function in Windows 2008 R2 will be supported in a future release.

To perform the remote installation, you will also require the following information:

- Target hostname or IP address.
- The admin user ID used for logging on to the target.
- The admin password used for logging on to the target.

Windows XP prerequisites

Windows XP systems must have Simple File Sharing disabled. Simple File Sharing forces all logins to authenticate as **guest** but a guest login does not have the authorizations necessary for the remote installation utility to function. To disable Simple File Sharing, complete the following steps:

1. Using Windows Explorer click **Tools** > **Folder Options**.
2. Select the **View** tab.
3. Scroll through the list of settings until you find Use Simple File Sharing.
4. Remove the check mark next to **Use Simple File Sharing**, click **Apply** and **OK**.

Windows XP includes a built-in firewall called the Internet Connection Firewall (ICF). By default, ICF is disabled on Windows XP systems. Windows XP Service Pack 2 comes with the Windows Firewall on by default. If either firewall is enabled on a Windows XP or Vista target, it blocks attempted accesses by the remote installation utility. On XP Service Pack 2, select **File and Printer Sharing** in the Exceptions tab of the Windows Firewall configuration to allow access.

Windows 7 prerequisites

You must perform the following on Windows 7 targets.

- Configure the remote registry.
- Configure the User Account Control feature.

Configuring the remote registry

On Windows 7, the default startup type for the Remote Registry service is manual. The Remote Registry service must be running to use the IBM Endpoint Manager for Remote Control remote installation feature.

To check if the Remote Registry service is enabled and started, complete the following steps:

1. Click **Start**.
2. In the Start Search box, type **services.msc**. Press **ENTER**.
3. When Microsoft Management Console starts, in the console pane, ensure that the service status is: started. If not, right-click **Remote Registry**, and click **Start**.

   To avoid problems with the manual startup, set the Remote Registry service startup type to automatic. If you want to automatically start the service after the server boot complete the following steps:

   a. Right-click **Remote Registry** and select **Properties**.
   b. In the Startup type option, choose **Automatic**.
   c. Click **Apply** and **OK** When the system starts up, Remote Registry automatically starts.
4. Turn off password protected sharing.
   a. Click **Control Panel** > **Networking and Internet** > **Network and Sharing Center**.
   b. Click **Change Advanced Sharing settings**
   c. Click the down arrow that is next to Password protected sharing.
   d. Click **Turn off password protected sharing**.
   e. Click **Apply** and exit the control panel.

Configuring User Account Control features for remote target installation

The User Account Control feature in Windows 7 requires users to perform several steps before the remote installation utility can communicate with Windows 7 targets. If you have a domain user account, ensure that the controller and the target machine are both members of a Windows domain. You can select the File and Printer Sharing box and the remote registry box in the Exceptions tab of the Windows Firewall configuration to allow access if the firewall is enabled. If you are a member of a local administrators group and you use a local user account, complete the steps below to be able to perform administrative tasks on the target machine:

1. Enable the built-in Administrator account and use it to connect.
   a. Open the Windows Control Panel.
   b. Click **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options**.
   c. Double-click Accounts: Administrator account status and select enable.
2. Disable User Account Control if a different Administrator user account is to be used to connect to the Windows 7 target. To disable User Account Control complete the following steps:
   a. Open the Windows Control Panel.
   b. Click **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options**.
   c. Double-click **User Account Control: Run all administrators in Admin Approval Mode** and select disable. Changing this setting requires a system reboot.
3. Disable User Account Control when you administer a workstation with a local user account (Security Account Manager user account). Otherwise, you cannot connect as a full administrator and cannot perform administrative tasks. To disable User Account Control, complete the following steps:

a. Click **Start** > **Run**, type **regedit**, and press **ENTER**.
b. Locate and click the following registry subkey: `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
c. If the **LocalAccountTokenFilterPolicy** registry entry does not exist, complete the following steps:
   1) On the Edit menu, point to New, and then click DWORD Value.
   2) Type **LocalAccountTokenFilterPolicy**, and press **ENTER**.
a. Right-click **LocalAccountTokenFilterPolicy,** and click **Modify**.
b. In the **Value data** box, type 1. Click **OK**
c. Restart your computer.

Alternatively, you can modify the registry entry manually by typing the following command:

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
 /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

Windows Server 2008

On Windows Server 2008 shares must be shared for the Guest or Everyone accounts, and password protected sharing must be disabled. To disable password protected sharing on Windows Server 2008, complete the following steps:

1. Click **Control Panel** > **Networking and Sharing Centre**.
2. Click the down arrow that is next to Password protected sharing.
3. Click **Turn off password protected sharing**.
4. Click **Apply** and exit the control panel.

Additionally, on Windows Server 2008 you might need to disable User Account Control if your account is not a domain user account. For more information about disabling User Account Control, see “Configuring user account control” on page 134. You can select the File and Printer Sharing box and the remote registry box in the Exceptions tab of the Windows Firewall configuration to allow access if the firewall is enabled.

Windows Vista pre requisites

Before remotely installing the IBM Endpoint Manager for Remote Control software on a Windows Vista target there are certain pre requisites that should be carried out.

- Disable password protected sharing
- Configure user account control.

Disabling password protected sharing

Password protected sharing must be disabled as a pre requisite for remotely installing the IBM Endpoint Manager for Remote Control target on a Windows Vista system.

To disable password protected sharing on Windows Vista systems, perform the following steps:

1. Click **Control Panel** > **Networking and Internet** > **Sharing and Discovery**.
2. Click the down arrow that is next to Password protected sharing.
3. Click **Turn off password protected sharing**.
4. Click **Apply** and exit the control panel.

Configuring user account control

The new User Account Control feature in Windows Vista requires users to perform several steps before the remote install utility can communicate with Vista targets.

If you have a domain user account, ensure that the controller and the target machine are both members of a Windows domain. If you are a member of a local administrators group and you use a local user account, complete the three steps below to be able to perform administrative tasks on the target machine:

1. Enable the built-in Administrator account and use it to connect.
   a. Open the Windows Control Panel.
   b. Click **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options**.
   c. Double-click on **Accounts: Administrator account status** and select enable.
2. Disable User Account Control if a different Administrator user account is to be used to connect to the Vista target. To disable User Account Control complete the following steps :-
   a. Open the Windows Control Panel.
   b. Click **Administrative Tools** > **Local Security Policy** > **Security Settings** > **Local Policies** > **Security Options**.
   c. Double-click **User Account Control: Run all administrators in Admin Approval Mode** and select disable. Changing this setting requires a system reboot.
3. Disable User Account Control when you administer a workstation with a local user account (Security Account Manager user account). Otherwise, you will not connect as a full administrator and will not be able to perform administrative tasks. To disable User Account Control complete the following steps:-
   a. Click **Start**, click **Run**, type `regedit`, and press **ENTER**.
   b. Locate and then click the following registry subkey:

      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Policies\System
   c. If the **`LocalAccountTokenFilterPolicy`** registry entry does not exist, follow these steps:
      1) On the Edit menu, point to New, and then click DWORD Value.
      2) Type `LocalAccountTokenFilterPolicy`, and press **ENTER**.
   d. Right-click **LocalAccountTokenFilterPolicy,** and click **Modify**.
   e. In the **Value data** box, type 1. Click **OK**.
   f. Restart your computer.

   Alternatively, you can modify the registry entry manually by typing the following command :

```
cmd /c reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
 /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f
```

UNIX and Linux targets

To remotely install the IBM Endpoint Manager for Remote Control target software on a Linux or Unix machine, you must ensure SSH is installed and enabled on any target you want to access using SSH protocol. OpenSSH 3.71 or higher, contains security enhancements not available in earlier releases.

Connections cannot be established with any UNIX targets that have all remote access protocols, rsh, rexec, or SSH disabled.

In all UNIX environments except Solaris, the Bourne shell (sh) is used as the target shell. On Solaris targets, the Korn shell (ksh) is used instead due to problems encountered with sh.

To communicate with Linux and other SSH targets using password authentication, you must edit the file `/etc/ssh/sshd_config file` on target machines and set:

PasswordAuthentication yes

(the default is 'no')

After changing this setting, stop and restart the SSH daemon using the following commands:

```
/etc/init.d/sshd stop

/etc/init.d/sshd start
```

To use SFTP for file transfers, in addition to calling **SSHProtocol.setUSESFTP(true)**, make sure that the SFTP server is enabled on the target machine.

Note: The location of the sftp-server is OS dependent. It is typically found in the following locations:

- Solaris: `/usr/lib/ssh/sftp-server`
- Linux: `/usr/libexec/openssh/sftp-server`
- HP-UX: `/opt/ssh/libexec/sftp-server`
- AIX®: `/usr/sbin/sftp-server`

The sshd_config file contains a line similar to the one below. Make sure that the line that enables the sftp-server subsystem is not commented out, and that it points to the OS-specific location of the sftp-server subsystem.

For example:

Subsystem sftp /one_of/the_paths/shown_above

IPv6 support for remote target installation

When you are performing remote target installations over IPv6 networks and cannot connect to the target machine you can perform some configuration steps to resolve this.

To use the remote installation feature to install Windows targets over IPv6, the server must be able to resolve the IPv6 address of the host. If that does not happen, the connection fails.

Note:

1. The host name cannot contain any colon characters because these characters are not supported by the Server Message Block (SMB) protocol. If there is a need to use the IPv6 address directly, you might try converting the IPv6 address to the ipv6-literal namespace format. For example, `the IPv6 address: 2001:4898:2b:4:bdb1:1c0:a5d8:438e might work when converted to: 2001-4898-2b-4-bdb1-1c0-a5d8-438e.ipv6-literal.net.`

2. Windows XP 32 bit does not support the SMB protocol over IPv6, and due to this limitation, performing a remote installation will fail if you attempt to connect to Windows XP 32 bit over IPv6.

If you encounter problems with IPv6 connection, complete the following steps:

1. Verify whether a port is blocked using the following command: **telnet <IPv6 address> 445**. If the connection to the host cannot be opened, it means that the port is blocked. When this happens, complete the following steps:
   a. Start the Registry Editor (regedt32.exe).
   b. Locate the following key in the Windows registry:
      `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Smb\Parameters`
   c. Add the following entries to the registry key:
      DWORD key **IPv6Protection**
      Add with hex value 00000014 (0x00000014).
      DWORD key **IPv6EnableOutboundGlobal**
      Add with hex value 1 (0x1).
   d. Reboot your computer for the changes to take effect.
2. Verify if the shared disks can be accessed by issuing the command **net use * \\<IPv6 host_domain_name>\c$**
   If the command returns an error and you cannot connect to the shared drive c$, it means that the disk cannot be accessed.
   When this happens, follow the steps below to use the IPv6 protocol
   a. Start the Registry Editor (regedt32.exe).
   b. Locate the following key in the Windows registry:
      `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters`
   c. Add the following entries to the registry key
      DWORD key **DisableStrictNameChecking**
      Add with value 1 (decimal) to enable file sharing.
   d. Reboot your computer for the changes to take effect.

Installing the target software remotely

To use the remote installation feature, you must have the following information.

- Target host name or IP address.
- The admin user ID that is used for logging on to the target.
- The admin password that is used for logging on to the target.

To remotely install the target software, complete the following steps:

1. Click **Tools** > **Remote Install**
2. Enter the information on the Remote Install screen.

   Platform Type
   Select the operating system that is running on the target.

   Target Host
   Enter the host name or IP address of the target.

   Target User Name
   Enter a valid administrator user ID that can be used to log on to the target operating system.

Note: If you chose Linux as the operating system, the user name is automatically set to root and cannot be changed.

Target Password
Enter a valid administrator password that can be used to log on to the target operating system.

Advanced Options
Use the advanced options to carry out some additional configuration. You can accept the values that are shown or change them to the relevant values for your environment.

Server Protocol
Specify the protocol that the server uses. Enter `http` or `https` for secure connections. Default is http.

Server Host
Specify the host name or IP address of the server that you want the target to contact.

Server Port
Specify the port that the server is listening on.

Server Context
Specify the server context. This value is used with the values entered in **Server Protocol** and **Server Host** for creating the URL that the target uses to contact the server.

For example, Server Protocol = https, Server Host = trcserver.com, and Server Context = /trc.

The target uses the following URL to contact the server.

```
http://trcserver.com/trc
```

Target Group
Specify the target group that you want this target to be assigned to. Default is **DefaultTargetGroup**.

Target Listening Port
Specify the port that the target listens for remote control connections on. Default is 888.

Installation Folder
Specify the installation path for the target files if you do not want to install the target in the default installation directory.

Temporary Folder
Specify a path to a folder where temporary installation files are stored during the installation.

Allow P2P
Select to enable peer to peer mode so that peer to peer sessions can be carried out regardless of the server state. For details of peer to peer mode, see IBM Endpoint Manager for Remote Control Installation Guide.

Allow P2P failover
Select to enable peer to peer mode so that peer to peer sessions can be carried out only if the server is down or unreachable. For details of peer to peer mode, see IBM Endpoint Manager for Remote Control Installation Guide.

Enable FIPS compliance
Select to enable FIPS compliance on the target. For more information about enabling FIPS compliance, see IBM Endpoint Manager for Remote Control Installation Guide.

Enable NIST SP800-131A compliance
Select to enable NIST SP800-131A compliance on the target. For more information about enabling NIST compliance, see the IBM Endpoint Manager for Remote Control Installation Guide.

Proxy Options
Select **Use Proxy** to use a proxy server and enter the proxy information.

Proxy Host
Specify the host name or IP address of the proxy server.

Proxy Port
Specify the port for the proxy server.

Proxy User
Specify a valid user ID that can be used to log on to the proxy server.

Proxy Password
Specify a valid password that can be used to log on to the proxy server.

3. Click **Next**.

   Note: Click **Reset** to clear all fields or set them back to their previous values.
4. The Remote Install summary screen is displayed with your chosen values. You can select one of the following options:
   - Click **Back** to go back and change any values.

     Note: If you are using a proxy, you must re enter the target user password and the proxy password.
   - Click **Install** to install the target software.

   As the installation progresses, **Complete** is displayed at each stage. If there is a problem during any part of the installation, a message is displayed. Click **OK** to return to the Remote Install screen to change values.
5. When the installation finishes, click **OK**.

The target software is installed on the target. You can verify the installation by running the **All targets** report to see whether the target is listed.

Note: You can click **Refresh** if the target details are not displayed in the list.

Viewing remote installation history

After you have remotely installed the target software on a target machine the results of the installation are saved to the server. You can view these results by running the **Remote Install History** report.

To view the **Remote Install History** click **Tools** > **Remote Install History**

The **Remote Installations** report is displayed . This report contains all of the remote installations attempted, those that were successful and those which failed.

Deleting remote installation history

After you have remotely installed the target software on a target machine the results of the installation are saved to the server. You can delete these results by running the **Remote Install History** report then selecting the required entry.

To delete a remote installation entry complete the following steps :

1. Click **Tools** > **Remote Install History**.
2. Select one or more entry.
3. Select **Delete entry**.
4. On the Confirm deletion screen click **Submit**.

The selected entries are removed from the database.

Chapter 16. Ensuring targets are registered correctly

When targets contact the server they send configuration details that are checked against the target details in the IBM Endpoint Manager for Remote Control database to see if the target has contacted the server before. If no match is found a new hardware key is generated and a new target entry is created in the database. In most cases this matching process is successful if the details supplied by the target are unique. However in cases where targets do not have unique identifying data, or the target configuration has changed, it can be more difficult to ensure the correct registration of the target. You can configure properties in the `trc.properties` file for multiple matching options to avoid new entries being created for existing targets or multiple targets being matched to the same entry.

`match.computername.only`
Match on computer name only.

`match.guid.only`
Match on GUID only

Perfect or Best Match with change notifications
There is no specific property to set for perfect match, this option is used if the **`match.computername.only`** and **`match.guid.only`** properties are set to false. Best match can be enabled using the **`match.allow.data.changes`** property. This is the default configuration.

Finding a perfect or best match for a target

The perfect match option is enabled by default in IBM Endpoint Manager for Remote Control and is used to try to find a perfect match for a target, where 4 criteria are used to find a match. The criteria are Virtual Product Data (VPD), UUID, MAC_ADDRESS and COMPUTERNAME and a perfect match is defined as finding a target in the database where all 4 criteria are matched successfully. However if any of these values changes for a target there are two further properties that can be used to try to find a match.

- **`match.change.notification`** - can be used if any of the criteria values change for the target.
- **`match allow.data.changes`** - can be used if only one of the criteria values has changed for the target. This is defined as a best match.

match.change.notification

True This is the default value. The target saves its details locally to a file called `tgt_info.proprties`. This file is located in the targets working directory which is defined by the **`WorkingDir`** property in the target registry. When the target contacts the server it sends its old details and its new details and the old details are used to try to find a perfect match for the 4 criteria.

0 matches
If no match is found a new hardware key is generated and a new target entry is created in the database.

1 match
If a match is found the details of the matched database entry are updated.

> 1 match found
If more than one match is found the first match is used. This scenario is very unlikely to be found.

False The old target details are not sent to the server and the new changed details are used to try to find a match. However if only one of the 4 criteria has changed and the **match.allow.data.changes** property is set to true then a best match is looked for.

match.allow.data.changes
This property is used to try to find a best match for a target in the database.

True This is the default value. When set to true, a best match is successful if all but 1 of the 4 criteria match an already registered target.

0 matches
If no match is found a new hardware key is generated and a new target entry is created in the database.

1 match
If a match is found the details of the matched database entry are updated.

> 1 match found
If more than one match is found create a new hardware key

False If the perfect match process is enabled and no match is found for all 4 of the target criteria, the best match option is not considered and depending on the value of **match.change.notifications**, if no match is found then a new target entry is created in the database.

Matching on computer name

Configure this matching option to use the target's computer name to try to find a match in the database. Use this method only if you have control over the naming of the targets and your environment uses targets that always have unique computer names. To use this method, enable the following property in the `trc.properties` file.

match.computername.only

True When a target contacts the server, its computer name is used to try to find a match in the database. One of the following three results can be achieved.

0 matches
If no match is found, a new hardware key is generated and a new target entry is created in the database.

Note: However, if the target has already registered and no match is found because its computer name has changed, the **match.change.notifications** property can also be used. If **match.change.notifications** is set to true, the target can send the old computer name and the new computer name to try to find a match.

1 match

If a match is found, the details of the matched database entry are updated.

> 1 match found

If more than one match is found, the other three criteria that are used in the perfect match process are checked against the database. They are checked to see whether a perfect match or best match can be found. This scenario might occur if the database was previously used in an older version of IBM Endpoint Manager for Remote Control. It can also occur if the database was previously used with a different matching algorithm and there were different computers with the same computer name registered.

False This value is the default value. When a target contacts the server, its computer name is not used to try to find a match in the database.

Matching on GUID

Configure this matching option to use the target's Globally Unique Identifier (GUID) to try to find a match in the database. The GUID is created by the target software.

Note: When using this method you must not clone any machines in your environment after the target software has been installed without first deleting the file called `TGT_INFO.PROPERTIES` which can be found in the target's data folder. Failure to delete the file before cloning will result in many assets matching with one database entry.

match.guid.only

True When a target contacts the server its GUID is used to try to find a match in the database. If a match is found the details of the matched database entry are updated. If no match is found a new hardware key is generated and a new target entry is created in the database.

0 matches

If no match is found a new hardware key is generated and a new target entry is created in the database.

1 match

If a match is found the details of the matched database entry are updated.

> 1 match found

If more than one match is found the other 3 criteria used in the perfect match option are then checked against the database to see if a perfect match or best match can be found. If none can be found, the entry for the first match that was found is updated.

False When a target contacts the server its GUID is not used to try to find a match in the database.

Chapter 17. Recording the session on the target

When the **Force session recording** policy is set to Yes a remote control session is automatically recorded and uploaded to the server at the end of the session. This recording is done on the controller by default. The session handover function, when in collaboration mode, has the implication that a session recording performed by a controller might not contain the full remote control session if session handover has taken place. To ensure that a full session recording can be maintained, two server policies can be configured to record the session in the target instead of the controller and save the recording to the target system after it has been successfully uploaded to the server. For details of the handover feature, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

Record the session in the target system
Determines whether the recording of the session should be done on the target system instead of the controller, when the **Force session recording** policy is set to Yes.

Keep session recording in the target system
Determines whether a copy of the session recording, that was done on the target and successfully uploaded to the IBM Endpoint Manager for Remote Control server is also saved to the target system.

For more details of these policies, see Chapter 7, “Server session policies,” on page 47.

Note: When the target cannot contact the server to upload the recording it keeps it in a queue. It later tries to contact the server and if successful it sends a list of the session ID's corresponding to the recordings to the server. The server checks each ID against the session history and if it does not find a session history for a particular ID it will report this to the target. If **Keep recording in target** is set to NO the target will delete the recording. If the property is set to Yes the target removes the recording from the queue but still keeps the recording on it's own disk. The following scenarios could cause the server not to find the IDs.

- The IBM Endpoint Manager for Remote Control Server was restored from a previous backup or the server was reinstalled with a clean database and no record of the Session ID exists in the database.
- The target was configured to connect to a different server . For example it was pointing to Server1 and now it is redirected to Server2 but this server has no matching Session ID for the recording.

Chapter 18. Set up for exporting recordings

A remote control session can be recorded and saved to the IBM Endpoint Manager for Remote Control Server. This recording can then be exported and saved to a local system at a later date. For example, to be used for education or training purposes. To enable the exporting function you must complete the follow the setup steps relevant to the operating system you have installed the IBM Endpoint Manager for Remote Control Server on.

Setting up a Windows server for exporting recordings

To enable the recording exporting function on an IBM Endpoint Manager for Remote Control Windows server complete the following steps

1. Download and run the Java Media Framework (JMF) Performance Pack for Windows installer from the following site

   `http://java.sun.com/javase/technologies/desktop/media/jmf/2.1.1/download.html`
2. Download and install the Xvid codec from **www.xvid.org**
3. Stop the **IBM Endpoint Manager for Remote Control** server service.
4. Copy the file `jmf.jar` from the JMF installation directory to the `WEB-INF\lib` directory within the IBM Endpoint Manager for Remote Control Server installation directory
5. Start the **IBM Endpoint Manager for Remote Control** server service.

Note: It is important to note that the `jmf.jar` file should be copied again into the `WEB-INF\lib`, directory whenever the IBM Endpoint Manager for Remote Control Server is updated, otherwise the exporting function is disabled.

Setting up a Linux server for exporting recordings

To enable the recording exporting function on an IBM Endpoint Manager for Remote Control Linux server complete the following steps

1. Download and run the Java Media Framework (JMF) Performance Pack for Linux installer from the following site

   `http://java.sun.com/javase/technologies/desktop/media/jmf/2.1.1/download.html`
2. Download and install MPlayer with support for the XviD codec. Depending on the Linux distribution you are using you might be able to install this using the regular package repositories if you are using SuSe Linux. If you are using RedHat Linux go to http://www.mplayerhq.hu .
3. Edit the `video.properties` file to ensure that the full path to the `encode.sh` file is set up correctly. This file is in the `WEB-INF/rc/encode.sh` directory. You need to expand the relative path to an absolute path where the application was deployed by WAS

   ```
   for example :
    /opt/IBM/WebSphere/AppServer61/profiles/installedApplications
        /trc.ear/trc.war/WEB-INF/rc/encode.sh.
   ```
4. Stop the IBM Endpoint Manager for Remote Control Server service by using the following command

   `/etc/init.d/trcserver stop`

5. Copy the file `jmf.jar` from the JMF installation directory to the `WEB-INF/lib` directory within the IBM Endpoint Manager for Remote Control Server installation directory
6. Start the IBM Endpoint Manager for Remote Control Server service by using the following command

   /etc/init.d/trcserver start

Note: It is important to note that the `jmf.jar` file should be copied again into the `WEB-INF/lib` directory, whenever the IBM Endpoint Manager for Remote Control Server is updated otherwise the exporting function is disabled.

Chapter 19. Audit log distribution

The audit log distribution feature runs a task which regularly creates a log file on the server. This file contains session information for all sessions that have been established. This feature is enabled and controlled by using the following properties in the `trc.properties` file. For details of editing this property file, see "trc.properties" on page 172.

task.logdistribution.enabled
Set to true or false.

True the log is created and written to the server.

False the log is not created.

task.logdistibution.path
Defines the location that the log file is written to on the server. This path is created if it does not exist.

task.logdistribution.file
Defines the start of the log file name which is then appended with a timestamp.

When the feature is enabled, the task is run and the file is created on the server with a name in the following format,

XXX`timestamp`.`log`

where *XXX* is the value that has been set for **`task.logdistribution.file`**.

timestamp is the time in milliseconds.

When the log is created each entry identifies the session, target and user, and a message of what action was carried out.

```
for example : sessionkey=8, target=TIVTEST1, user=Admin
              January 26, 2013 9:15:28 AM GMT
              Session Connection Attempt by Default Administrator
                  @192.0.2.0[00:11:25:f7:b2:1e]
```

Note: Each time the task runs it includes the log data created since the last task execution.

Chapter 20. Accessing targets on different networks

If you have targets, controllers and severs on different networks that cannot directly contact each other you can install and configure gateway support. After installing, you can configure your network to enable connections to be established. For details of installing the gateway support see the IBM Endpoint Manager for Remote Control Installation Guide.

The IBM Endpoint Manager for Remote Control gateway supports different types of connections

Inbound connections
configure these connections for the gateway to accept connections from endpoints, controllers, and other gateways.

Gateway connections
configure a gateway to establish a permanent connection with another gateway.

Endpoint connections
configure the gateway to locate endpoints from which a request has been received.

Tunnel Connections
used to facilitate TCP connections to the IBM Endpoint Manager for Remote Control server from the target

The gateway administrator defines the connections that are required for each gateway, in the configuration file.

Configuring the gateway support

After the gateway support is installed it should be configured using the gateway configuration file, `trc_gateway.properties`, which is in a Java properties file format. This file is located 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` on Windows Vista and later.

Linux systems
/etc

Define the connections that are required in the gateway configuration file. The gateway configuration file has a similar format to a Java properties file.

- The gateway supports multiple instances of each connection type
- The configuration directives for each connection have a user defined prefix.

You can define four types of connections depending on the setup of your environment.

- Inbound connections

- Gateway connections
- Endpoint connections
- Tunnel connections

The following optional parameters can be used to further configure your gateway.

FIPSCompliance
Set the value of this parameter to Yes to use a FIPS certified cryptographic provider for all cryptographic functions. Default value is No.

SP800131ACompliance
Set the value of this parameter to Yes to enforce NIST SP800-131A compliant algorithms and key strengths for all cryptographic functions. Default value is No.

Configuring inbound connections

Configure Inbound connections for the gateway to accept connections from endpoints, controllers, and other gateways. You can configure multiple inbound connections and you must define a prefix for each connection parameter so that the gateway finds all required settings for each connection.

```
for example
 Inbound.1.ConnectionType
finance.network.ConnectionType
Connection.for.subnet.192.0.2.0.ConnectionType
```

Note:

1. Do not prefix with # or !. These characters are reserved for comments in properties files.
2. If you want to include spaces in the prefix, you must escape them with \

```
for example :  my connection.ConnectionType
 should be defined as my\connection.ConnectionType
```

Inbound connections are configured by using the following parameters:

ConnectionType
Defines the type of connection. Must be set to `Inbound`. For example: **`inbound.1.ConnectionType=Inbound`**

PortToListen
Defines the TCP port that gateways and endpoints must use to connect to this gateway. The port for listening for inbound connections. *Required* parameter.

BindTo
This parameter is optional and can be configured to accept incoming connections on specific network interfaces. Defines the IP address that is used to create connections with. For example: **`inbound.1.BindTo=192.0.2.1`** Default is 0.0.0.0. *Optional* parameter.

AllowGateways
Determines whether other gateways can connect to this connection. This parameter is optional.

True Gateways are permitted to connect to this connection. This value is the default value.

False Gateways are not permitted to connect to this connection.

AllowEndpoints
Determines whether other endpoints can connect to this connection. This parameter is optional.

True Endpoints are permitted to connect to this connection. This value is the default value.

False Endpoints are not permitted to connect to this connection.

RetryDelay
Defines the time in seconds between attempts to establish the control connection. This parameter is optional. Default is 45 seconds.

Passphrase
If required, the gateway can be configured to request a secret passphrase from the remote gateway to be used for authentication. This parameter is optional.

Configuring gateway connections

Gateway connections are used to configure a gateway to establish a permanent control connection with another gateway. You can configure multiple gateway connections and should define a prefix for each connection parameter so that the gateway can find all required settings for each connection. If a gateway connection is down or cannot be reached it will try to get connected as it should be a permanent connection.

```
for example
 Gateway.1.ConnectionType
 G2.ConnectionType
```

See the Notes in "Configuring inbound connections" on page 152 for rules for defining prefixes.

Gateway connections are configured using the following parameters:

ConnectionType
Defines the type of connection. Must be set to `Gateway`. For example: **`gateway.1.ConnectionType=Gateway`**

DestinationAddress
Defines the IP address of the remote gateway that the connection is being made to. The gateway with this address must configured to accept inbound connections. This parameter is required.

DestinationPort
Defines the TCP port that the other gateway is listening on. This parameter is required.

BindTo
This parameter is optional. Use this parameter to configure the gateway to establish the outgoing gateway connection from a specific network interface. For example if a firewall on the network is configured to allow only 1 of the gateway's interfaces through. Defines the IP address of the network interface through which the connections will be made. For example: **`gateway.1.BindTo=192.168.74.1`** Default is 0.0.0.0.

SourcePort
Defines the port that the outgoing gateway connections are using. This parameter is optional. Default is 0.

RetryDelay
Defines the time in seconds between attempts to establish the control connection. This parameter is optional. Default is 45 seconds.

KeepAlive
Defines the time in seconds between keepalive requests. This parameter is optional. Default is 900.

Timeout
The time, in seconds, to wait before a connection attempt is considered to have timed out. Default is 90.

Passphrase
Defines a secret passphrase if the remote gateway requires it for authentication.

Configuring endpoint connections

Endpoint connections configure the gateway to locate other endpoints from which a request has been received. These connections are only needed on the gateways where the targets that you want to connect to are. You must define a prefix for each connection parameter so that the gateway can find all required settings for each connection.

Note: It should be noted that intermediate gateways that merely connect two separate gateways should not have any endpoint connections configured as this would increase network traffic unnecessarily.

Endpoint connections are configured using the following parameters:

ConnectionType
Defines the type of connection. Must be set to `Endpoint`. For example:
`endpoint.1.ConnectionType=Endpoint`

SubnetAddress
Defines the IP address of a subnet that can be connected to, either directly or indirectly. You must define an endpoint connection for each required subnet. This way, the gateway will automatically filter out attempts to endpoints that it cannot reach . This parameter is optional.

Note: The default is 0.0.0.0/0.0.0.0 which specifies that the gateway will attempt to connect to any endpoint.

SubnetMask
Defines the subnet mask of a subnet that can be connected to, either directly or indirectly. If you do not specify this the gateway will try to connect to any target, therefore by specifying specific values you can define what addresses to look at so that it is optimized. This parameter is optional. Default is 0.0.0.0

BindTo
Defines the IP address of the network interface through which the connections is made. If required, the gateway can be configured to connect to the endpoints from a specific port and interface only. This may be required if the endpoints have a desktop firewall that only allows the gateways to connect to them. For example:
`endpoint.1.BindTo=192.168.74.1` This parameter is optional. Default is 0.0.0.0

SourcePort
Defines the port that outgoing connections are made from. This parameter is optional. Default is 0.

Timeout
The time, in seconds, after which an endpoint connection is considered to have timed out. This parameter is optional. Default is 45 seconds.

Configuring tunnel connections

Tunnel connections provide a way for targets to connect to the server when there is no other way to connect to each other. You can define multiple tunnel connections. The gateway supports two types of connection, one for each end of a tunnel. The gateway will support tunnels to multiple destinations. For example, if you have a single site with multiple instances of IBM Endpoint Manager for Remote Control to support multiple customers. You should define a prefix for each connection parameter so that the gateway can find all required settings for each connection.

Tunnel Connections are configured using the following parameters :

ConnectionType
defines the type of connection. For example :
`tunnel.1.ConnectionType=InboundTunnel`

InboundTunnel
An inbound tunnel connection is used to configure a gateway to listen for incoming connections from endpoints that want to connect to the server.

OutboundTunnel
An outbound tunnel connection, is used to connect the tunnel to the destination, for example the IBM Endpoint Manager for Remote Control server.

The above connection types use the following parameters.

Inbound connections

TunnelID
The TunnelID is used to associate an inbound connection with the correct outbound connections. The default value is TRCSERVER. For example : `tunnel.1.TunnelID = TRCSERVER`. This parameter is optional.

PortToListen
Defines the TCP port that the target should use to connect to the tunnel connection. This parameter is required.

BindTo
Defines the IP address used to create the connection. This parameter is **optional.**

RetryDelay
Defines the time in seconds to wait before listening for new connections. This parameter is **optional**.

Outbound connections

TunnelID
The TunnelID is used to associate an inbound connection with the correct outbound connections. The default value is

TRCSERVER. For example : `tunnel.1.TunnelID = TRCSERVER`. This parameter is optional.

BindTo
Defines the IP address used to create the connection. This parameter is **optional.**

Destination Address
Defines the IP address of the IBM Endpoint Manager for Remote Control Server that the tunnel connection is being made to. This parameter is required.

DestinationPort
Defines the TCP port that the IBM Endpoint Manager for Remote Control Server is listening on. This parameter is required.

Timeout
Defines the time in seconds to wait before a connection attempt is considered to have timed out. This parameter is **optional**.

Configuring the targets to use tunnel connections

For targets that need to contact a IBM Endpoint Manager for Remote Control Server on a different network you can modify the **ProxyURL** target property so that a connection to the server can be made using a tunnel connection.

Configuring a Windows target to use tunnel connections

To modify the **ProxyURL** property on a Windows target complete the following steps :

1. Run the **regedit** command at a command prompt window.
2. In the windows registry navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Tivoli\Remote Control\Target`
3. Right-click the **ProxyURL** entry and click **Modify**.
4. Type in `trcgw://gatewayaddress:port` into the Value data field and click **OK**. where *gatewayaddress* is the IP address or hostname of the gateway that the target will connect to for using the tunnel connection and *port* is the port that the target should connect to for using the tunnel connection.
5. Restart the target service.

Configuring a Linux target to use tunnel connections

To modify the **ProxyURL** property on a Linux target complete the following steps :

1. Edit the `ibmtrct.conf` file and modify the **ProxyURL** entry by setting it to `trcgw://gatewayaddress:port`. where *gatewayaddress* is the IP address or hostname of the gateway that the target will connect to for using the tunnel connection and *port* is the port that the target should connect to for using the tunnel connection.
2. Save the file.
3. Restart the target service.

Configuring gateways in IPv6 networks

Configuring inbound connections

When an inbound connection is defined in the gateway configuration file it can listen by default for incoming connections from any IPv4 address and would be configured as follows

prefix.ConnectionType=Inbound

prefix.PotToListen=8881

prefix2.ConnectionType=InboundTunnel

prefix2.PortToListen=8882

Previously to create an inbound connection for IPv6, the connection would have had to be bound to the IPv6 ANY address which is 0:0:0:0:0:0:0:0 or in compressed notation ::. as follows:

prefix.ConnectionType = Inbound

prefix.PotToListen=8881

prefix.BindTo= \::

Note: As the colon can be used as a separator in properties files, it should be escaped with a backslash character to indicate that it is part of the value and not the separator.

To configure an inbound connection for incoming connections from IPv6 addresses you can now use *Inbound6* or *InboundTunnel6* instead.

prefix.ConnectionType = Inbound6

prefix.PortToListen = 8881

prefix2.ConnectionType = InboundTunnel6

prefix2.PortToListen = 8882

Note: If you want the gateway to listen for both IPv4 and IPv6 incoming connections you should define an inbound and an inbound6 connection type entry in the gateway configuration file.

Configuring endpoint connections

To specify an IP subnet in IPv4, you should specify the subnet address and the subnet mask.

prefix.ConnectionType = Endpoint

prefix.SubnetAddress = 198.51.100.0

prefix.SubnetMask = 255.255.255.0

As IPv6 addresses are much longer than IPv4 addresses, the subnet mask notation is not used for IPv6. Both IPv4 and IPv6 support Classless Inter-Domain Routing (CIDR) notation, which specifies the length of the subnet prefix after the subnet address.

prefix.ConnectionType = Endpoint

prefix.Subnet = 198.51.100.0/24

prefix2.ConnectionType = Endpoint

prefix2.Subnet = 2001:db8:d005:ee::/64

Note: The gateway does not support IPv6 subnets with the SubnetAddress / SubnetMask notation.

When an endpoint connection is defined in the gateway, by default it tries to locate all endpoints with any IPv4 address.

prefix.ConnectionType = Endpoint

Previously to configure an endpoint connection for IPv6 the default Subnet would have had to be overwritten.

prefix.ConnectionType = Endpoint

prefix.Subnet = \::/0

To configure an endpoint connection that tries to locate all endpoints with IPv6 addresses, you can now use *Endpoint6* instead.

prefix.ConnectionType = Endpoint6

Gateway setup example

The following example illustrates a gateway and tunnel connection setup. There are three networks present, a secure network, a DMZ network and an unsecure network. Firewalls are installed to control traffic between the secure network and the DMZ as well as the DMZ and the unsecure network. The security policy in force does not allow network connections to be initiated from the unsecure network to the DMZ or from the DMZ to the secure network. Network connections from the secure to the DMZ and from the DMZ to the unsecure network are allowed for particular ports. The IBM Endpoint Manager for Remote Control Server component is installed on a server attached to the secure network and controller machines are also present on the secure network. Applications run on servers that are attached to the unsecure network and these servers are unattended. The IBM Endpoint Manager for Remote Control target is installed on these systems to provide remote access for maintenance and support. No connections can be initiated from the unsecure network to the DMZ or from the DMZ to the secure network, therefore a chain of proxy servers cannot be used. The proxy server on the unsecure network is unable to connect to the proxy server on the DMZ to forward incoming HTTP requests. The solution for this scenario is to install a gateway in each of the networks.

IBM Endpoint Manager for Remote Control components present

Table 3. IBM Endpoint Manager for Remote Control components present on network

Network name	Server	Controller	Target
Secure network	**Yes**	**Yes**	No
DMZ	No	No	No
Unsecure network	No	No	**Yes**

Networks

Table 4. Networks

Network name	Subnet address	Netmask
Secure network	10.1.0.0	255.255.255.0
DMZ	10.2.0.0	255.255.255.0
Unsecure network	10.3.0.0	255.255.255.0

Machines

Table 5. Machines

Hostname	IP address	Roles
SERVER	10.1.0.2	remote control server on port 80
GATEWAYA	10.1.0.254	remote control gateway on port 8881
GATEWAYB	10.2.0.254	remote control gateway on port 8881
GATEWAYC	10.3.0.254	remote control gateway on port 8881
TARGET	10.1.0.3	remote control target on port 888

Firewall

Table 6. Firewall

Source	DestinationPort	Port	Description
10.1.0.254/ 255.255.255.255	10.2.0.254/ 255.255.255.255	8881	Allow GATEWAYA to connect to GATEWAYB
10.2.0.254/ 255.255.255.255	10.3.0.254/ 255.255.255.255	8881	Allow GATEWAYB to connect to GATEWAYC

Gateway setup

- Gateway support is installed on machine GATEWAYA in the secure network. A IBM Endpoint Manager for Remote Control gateway named GATEWAYA is also installed because there are controllers present on the secure network that need to connect to the targets on the unsecure network.

  To install the gateway support see the IBM Endpoint Manager for Remote Control Installation Guide.

To create the gateway complete the following steps on the IBM Endpoint Manager for Remote Control Server :

1. Click **Admin** > **New Remote Control Gateway**.
2. On the Add Remote Control Gateway screen enter the required details
   - **Hostname** - GATEWAYA
   - **Description** - (optional)
   - **IP address** - 10.1.0.254
   - **Port** - 8881
3. Click **Submit**.

- Gateway support is installed on machine GATEWAYB in the DMZ network.

  To install the gateway support see IBM Endpoint Manager for Remote Control Installation Guide.
- Gateway support is installed on machine GATEWAYC in the unsecure network.

  To install the gateway support see IBM Endpoint Manager for Remote Control Installation Guide.
- GATEWAYA is configured with a gateway control connection to GATEWAYB.
- GATEWAYB is configured with a gateway control connection to GATEWAYC.
- Gateway A is configured with an outbound tunnel connection to the IBM Endpoint Manager for Remote Control server.
- Gateway C is configured with an inbound tunnel connection on port 8880.
- The targets in the unsecure network are configured to connect via the inbound tunnel connection on GATEWAYC.

Gateway configuration

GATEWAYA configuration file

Inbound.1.ConnectionType= Inbound

Inbound.1.PortToListen = 8881

Gateway.A.ConnectionType=Gateway

Gateway.A.DestinationAddress = 10.2.0.254 - GATEWAYA will connect to GATEWAYB

Gateway.A.DestinationPort = 8881

Gateway.A.RetryDelay = 15

Gateway.A.KeepAlive = 900

OutboundTunnel.1.ConnectionType=OutboundTunnel

OutboundTunnel.1.DestinationAddress = 10.1.0.2 - connection to the IBM Endpoint Manager for Remote Control server

OutboundTunnel.1.DestinationPort = 80

GATEWAYB configuration file

Inbound.1.ConnectionType= Inbound

Inbound.1.PortToListen = 8881

Gateway.B.ConnectionType=Gateway

Gateway.B.DestinationAddress = 10.3.0.254 - GATEWAYB will connect to GATEWAYC

Gateway.B.DestinationPort = 80

Gateway.B.RetryDelay = 15

Gateway.B.KeepAlive = 900

GATEWAYC configuration file

Inbound.1.ConnectionType= Inbound

Inbound.1.PortToListen = 8881

InboundTunnel.1.ConnectionType=InboundTunnel

InboundTunnel.1.PortToListen = 8880- the port that the target should use to connect to the tunnel connection

Endpoint.1.ConnectionType=Endpoint

Endpoint.1.SubnetAddress= 10.3.0.0 - the network address of the unsecure network that the target is connected to.

Endpoint.1.SubnetMask= 255.255.255.0

When a target requires an HTTP or HTTPS connection with the IBM Endpoint Manager for Remote Control Server, it first connects to port 8880 on GATEWAYC. GATEWAYC accepts this connection and immediately creates a tunnel to GATEWAYA, via GATEWAYB. GATEWAYA then connects to the IBM Endpoint Manager for Remote Control Server and acknowledges the connection to GATEWAYC via GATEWAYB. When the tunnel is established, gateways C and A start reading any data from their respective connections and forwarding it to each other via the tunnel as well as writing any traffic received from the tunnel to this connection. The result is that the target and the server can communicate while being unaware that the traffic is being tunneled. When either party shuts down their end of the connection, the tunnel is torn down and the other connection is also shut down.

Keeping track of connection requests

An area of memory known as the **`Request Pool`** is used to keep track of requests. The connection requests are kept in the pool until the pool is full and the oldest requests are recycled. This is done to prevent requests from looping around in the gateway network undetected.

The following parameters can be used to configure the request pool :

Note: Configuration of the request pool is optional.

RequestPool.Size
The amount of memory, in kilobytes, to reserve for the request pool. The default is 2048 or 2 megabytes.

RequestPool.MinimumTTL
The minimum time, in minutes, before a request can be recycled. The default is 5 minutes.

Note: Each request requires 32 bytes of memory. The gateway can handle more than 200 requests per second with the default settings.

Logging gateway activity

When the gateway support is installed, a log file is created in the following directories :

Windows systems
`Documents and Settings\All Users\ Application Data\IBM\Tivoli\Remote Control\Gateway` on Windows 2000, Windows XP, and Windows 2003 operating systems

`\ProgramData\IBM\Tivoli\Remote Control\Gateway` on Windows Vista operating system and later.

Linux systems
`/var/opt/ibm/trc/gateway`

The name of the log file is `TRCGATEWAY-`*`hostname-suffix`*`.log` where *hostname* denotes the computer name or host name of the system hosting the gateway and *suffix* denotes the date and time, depending on which rotation and rollover settings are being used. For more details, see "Managing Gateway logs." For example, for a system hosting the gateway with host name `mygateway-1` and the following settings in the configuration file,

LogRotation = Weekly

LogRollover = Daily

the log file could be named `TRCGATEWAY-mygateway-1-THU-18H.log`

Managing Gateway logs

The gateway component recognizes two additional configuration keywords, which are contained in the gateway configuration file. You can use these keywords to configure log rotation and to specify the maximum period for which log files are retained.

LogRotation
controls the period after which an older log file is overwritten. Log rotation can be disabled.

Table 7. LogRotation settings

LogRotation	Description	Suffix for hourly rollover	Suffix for daily rollover
Daily	Overwrite log files after one day	00H to 23H	Not valid
Weekly	Overwrite log files after one week.	Mon-00H to Sun-23H	Mon - Sun

Table 7. LogRotation settings (continued)

LogRotation	Description	Suffix for hourly rollover	Suffix for daily rollover
Monthly	Overwrite log files after one month.	01-00H to 31-23H	01 to 31
Disabled	LogRotation is disabled	YYYY-MM-DD-hh	YYYY-MM-DD

LogRollover
controls the period after which a new log file is started. This period has to be smaller than the **LogRotation** period, therefore not all combinations are valid. **LogRollover** cannot be disabled.

Table 8. LogRollover settings

LogRollover	Description	Comments
Hourly	Start a new log file on the hour.	Recommended for busy gateways or when using log levels higher than 2.
Daily	Start a new log file every day.	Default setting.

Configuration file example

When the configuration file is created it provides examples of the required configuration parameters which you can use to create a configuration file to satisfy your network requirements. The following file is an example of the file when it is installed.

```
# Licensed Materials - Property of IBM

# 5725-C43

# US Government Users Restricted Rights - Use, duplication or disclosure

# Copyright International Business Machines Corp. 2008, 2013. All Rights Reserved

# restricted by GSA ADP Schedule Contract with IBM Corp.

# Please refer to the Administrator's Guide for instructions regarding this

# Configuration file for IBM Endpoint Manager for Remote Control Gateway

# configuration file.

# Logging levels

#

# 0 no logging

#1 error

# 2 informational (default)
```

```
# 4 debug information (only by request from IBM)
# LogLevel = 2
# Log rotation and rollover
LogRotation = Weekly
LogRollover = Daily
# LogRotation Rotate between log files (Daily, Weekly, Monthly, Disabled)
# LogRollover Switch log files (Hourly, Daily)
#
# Defaults
# LogRotation Weekly
# LogRollover Daily
# Use a FIPS certified cryptographic provider for all cryptographic functions
FIPSCompliance = No
# Request Pool
# The gateway stores session requests that it is processing in the request
# pool. The request pool uses a fixed amount of memory.
# Size of the request pool (kilobytes)
# Each request needs 32 bytes
# RequestPool.Size = 2048
# Time before a request from the pool can be re-used, in minutes
# RequestPool.MinimumTTL = 5
# Defaults
#
# RequestPool.Size 2048
# RequestPool.MinimumTTL 5
# Inbound Connections
# Connections to accept incoming connections from endpoints and gateways
# Inbound.1.ConnectionType = Inbound
```

```
# Inbound.1.PortToListen = 8881
# Inbound.PortToListen TCP port that gateways and endpoints should
# use to connect to this gateway (required)
# Inbound.BindTo Accept incoming connections on the
# specified IP address only (optional)
# Inbound.RetryDelay Time, in seconds, between attempts to
# listen for incoming connections (optional)
# Inbound.Passphrase Secret passphrase that remote gateways are
# required to authenticate with (optional)
# Inbound.1.AllowGateways Allow gateways to connect to this connection
# (yes/no or true/false) (optional)
# Inbound.1.AllowEndpoints Allow endpoints to connect to this connection
# Defaults
# (yes/no or true/false) (optional)
#
# Inbound.BindTo 0.0.0.0
# Inbound.RetryDelay 45
# Inbound.AllowGateways yes
# Inbound.AllowEndpoints yes
# Examples
# Inbound.2.ConnectionType = Inbound
# Inbound.2.PortToListen = 8881
# Inbound.2.BindTo = 192.168.74.254
# Inbound.2.Passphrase = qagumczw0krbmyajcjOkehnrryuTv1zxyevdckcwsrk}bjfi
# Inbound.2.AllowGateways = true
# Inbound.2.AllowEndpoints = false
# Inbound.3.ConnectionType = Inbound
# Inbound.3.PortToListen = 8881
```

```
# Inbound.3.BindTo = 192.168.75.254
# Inbound.4.ConnectionType = Inbound
# Inbound.4.PortToListen = 8881
# Inbound.4.BindTo = 192.168.76.254
# Inbound.4.RetryDelay = 30
# Gateway Connections
# Outgoing control connections to neighbour gateways
# Gateway.1.ConnectionType = Gateway
# Gateway.1.DestinationAddress = 192.168.77.254
# Gateway.1.DestinationPort = 8881
# Gateway.DestinationAddress IP address of the remote gateway
# Gateway.DestinationPort TCP port of the remote gateway
# Gateway.BindTo Force outgoing connections from the
# specified IP address only (optional)
# Gateway.SourcePort Force outgoing connections from the
# specified port only (optional)
# Gateway.RetryDelay Time, in seconds, between attempts to
# connect to the remote gateway (optional)
# Gateway.KeepAlive Time, in seconds, between keepalive
# requests (optional)
# Gateway.Timeout Time, in seconds, before a connection
# attempt is considered to have timed
# out (optional)
# Gateway.Passphrase Secret passphrase if the remote gateway
# requires authentication
# Defaults
#
# Gateway.BindTo 0.0.0.0
```

```
# Gateway.SourcePort 0

# Gateway.RetryDelay 45

# Gateway.KeepAlive 900

# Gateway.Timeout 90

# Examples

# Gateway.2.ConnectionType = Gateway

# Gateway.2.DestinationAddress = 192.168.78.254

# Gateway.2.DestinationPort = 8881

# Gateway.2.BindTo = 192.168.74.254

# Gateway.2.SourcePort = 8882

# Gateway.2.RetryDelay = 90

# Gateway.2.KeepAlive = 180

# Gateway.2.Timeout = 30

# Endpoint connections

# Configures the gateways to try to find an endpoint when a session request

# is received

# Endpoint.1.ConnectionType = Endpoint

# Endpoint.SubnetAddress The network address for the subnet that

# this connection can reach (optional)

# Endpoint.SubnetMask The network mask for the subnet that this

# connection can reach (optional)

# Endpoint.BindTo Force outgoing connections from the

# specified IP address only (optional)

# Endpoint.SourcePort Force outgoing connections from the

# specified port only (optional)

# Endpoint.Timeout Time, in seconds, before a connection

# attempt is considered to have timed

# out (optional)
```

```
# Defaults

#

# Endpoint.SubnetAddress 0.0.0.0

# Endpoint.SubnetMask 0.0.0.0

# Endpoint.BindTo 0.0.0.0

# Endpoint.SourcePort 0

# Endpoint.Timeout 45

# Examples

# Endpoint.2.ConnectionType = Endpoint

# Endpoint.2.SubnetAddress = 192.168.79.0

# Endpoint.2.SubnetMask = 255.255.255.0

# Endpoint.3.ConnectionType = Endpoint

# Endpoint.3.SubnetAddress = 192.168.80.0

# Endpoint.3.SubnetMask = 255.255.255.0

# Endpoint.4.ConnectionType = Endpoint

# Endpoint.4.BindTo = 192.168.74.254

# Endpoint.4.SourcePort = 8882

# Tunnel connections

# Tunnel connections are used to provide connections to the TRC server for the
endpoints

# when they cannot reach the server directly or via an http proxy.

# Setting up a tunnel requires two types of connections. On the gateways that can
reach

# the server, an outbound tunnel connection needs to be configured. On the
gateways that

# the endpoints can reach, an inbound tunnel is required. When an endpoint
connects to the

# inbound tunnel port, the gateway will locate one of the corresponding outbound
tunnels

# through the gateway control network. The outbound tunnel then connects to the
server to
```

```
# complete the tunnel. At that point, the gateways will forward all traffic between
the

# endpoint and the server through the tunnel.

# Outbound tunnel connection

# OutboundTunnel.1.ConnectionType = OutboundTunnel

# OutboundTunnel.1.DestinationAddress IP address of the server (required)

# OutboundTunnel.1.DestinationPort TCP port of the server (optional)

# OutboundTunnel.1.TunnelID ID to relate inbound and outbound

# tunnels to each other (optional)

# OutboundTunnel.1.BindTo Force outgoing connections from the

# specified IP address (optional)

# OutboundTunnel.1.Timeout Time, in seconds, before a connection

# attempt is considered to have timed

# out (optional).

# Defaults

#

# DestinationPort 80

# TunnelID TRCSERVER

# BindTo 0.0.0.0

# Timeout 90

#

# Examples

# OutboundTunnel.2.ConnectionType = OutboundTunnel

# OutboundTunnel.2.DestinationAddress = 192.168.81.52

# OutboundTunnel.3.ConnectionType = OutboundTunnel

# OutboundTunnel.3.DestinationAddress = 192.168.81.52

# OutboundTunnel.3.DestinationPort = 443

# Inbound tunnel connection

# InboundTunnel.1.ConnectionType = InboundTunnel
```

```
# InboundTunnel.1.PortToListen TCP port that endpoints should use to
# connect to the tunnel (required)
# InboundTunnel.1.TunnelID ID to relate inbound and outbound
# tunnels to each other (optional)
# InboundTunnel.1.BindTo Accept incoming connections on the
# specified IP address only (optional)
# InboundTunnel.1.RetryDelay Time, in seconds, between attempts to
# listen for incoming connections (optional)
# Defaults
#
# TunnelID TRCSERVER
# BindTo 0.0.0.0
# RetryDelay 45
```

Chapter 21. Editing the properties files

You can use the properties files in IBM Endpoint Manager for Remote Control to customize your environment, configure LDAP, set debug options, and set controller and on-demand target properties. The files can be edited in the IBM Endpoint Manager for Remote Control Server UI.

The following properties files are available.

- `trc.properties`
- `log4j.properties`
- `ldap.properties`
- `common.properties`
- `appversion.properties`
- `controller.properties`
- `ondemand.properties`

For more information about modifying the `log4j.properties` file, see **http://logging.apache.org/log4j/docs/**

To edit the properties files in the IBM Endpoint Manager for Remote Control Server UI, complete the following steps.

1. Click **Admin** > **Edit properties file**. The Edit Properties File panel is displayed.
2. Select the relevant file from the list.
3. Make the changes and click **Submit**.
4. For the new property values to take effect click **Admin** > **Reset Application**.

As there is a short delay while the file is rewritten, you must not make any immediate changes until the application is reset.

Note: To manually edit the properties files, locate them on the server and edit them. If you edit the files manually, you must reset the server application by selecting **Admin** > **Reset Application** for the new values to be displayed when you edit the file in the UI.

The properties 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 directory that the IBM Endpoint Manager for Remote Control Server is installed.

```
For example,
C:\Program Files\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 directory that the IBM Endpoint Manager for Remote Control Server is installed.

```
For example:
/opt/IBM/Tivoli/TRC/server/wlp/usr/servers/trcserver/apps/TRCAPP.ear
/trc.war/WEB-INF/classes
```

Template of field information

A table-style template has been applied to each of the properties files in the following sections. This template includes the following items:

- Category Description
- Modifiable Field
- Field Description
- Possible Values
- Value Definition

Category Description: There are several different categories within the file. Each category focuses on a particular function carried out by the IBM Endpoint Manager for Remote Control program. These categories are the same as those configured in the installation.

Modifiable Field	The field contains one or more parameters used to accomplish a specific task within the category.
Field Description	The field is used to describe precisely what function the field parameter is performing.
Possible Values	This field identifies all of the possible values that can be used within the field parameter.
Value Definition	This field defines how the program will carry out certain functions depending on what value is associated with the field parameter.

trc.properties

Definitions of the properties in the `trc.properties` file that is packaged with the IBM Endpoint Manager for Remote Control Server.

DO NOT EDIT THE FOLLOWING LINE

```
rc.enabled=
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
rc.heartbeat_timeout=
```

Modifiable Field	**rc.heartbeat_timeout**
Field Description	While an endpoint is active, it periodically reports back to the server. This value is the number of minutes between each report back to the server or heartbeat.
Possible Values	User Defined
Value Definition	

```
rc.create.assets.from.callhome=
```

Modifiable Field	**rc.create.assets.from.callhome**
Field Description	If target information sent from the target to the server is not already in the database, create these targets in the database
Possible Values	true or false
Value Definition	**true** target information is added to the database. **false** target information is not added to the database.

`rc.create.assets.from.brokers=`

Modifiable Field	**rc.create.assets.from.brokers**
Field Description	Use to allow an unregistered target to register with the server at the start of a remote control session that uses a broker. The target information is sent to the server when the target user enters the connection code.
Possible Values	True or False
Value Definition	**True** Unregistered targets are added to the database. **False** Unregistered targets are not added to the database.

DO NOT EDIT THE FOLLOWING LINES

```
rc.validation.relative.url=
rc.audit.relative.url=
rc.upload.url=
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

`rc.show.controller.splash=`

Modifiable Field	**rc.show.controller.splash**
Field Description	Use this property to determine whether the controller splash screen is displayed before the remote control session starts.
Possible Values	True or False
Value Definition	**True** The controller splash screen is displayed before the remote control session starts. True is the default value. **False** The controller splash screen is not displayed during the initiation of a remote control session.

`rc.recording.directory=`

Modifiable Field	**rc.recording.directory**
Field Description	Directory that is used for storing session recordings on the Server
Possible Values	User-defined: for example: `rc_recordings`. Can be specific or relative

Value Definition	

unknown.recording.action=

Modifiable Field	**unknown.recording.action**
Field Description	Determines what action is returned to the target if a target requests to upload a recording for a session that is not known to the server.
Possible Values	0, 1, 2
Value Definition	**0** The target can upload the recording. **1** The target must keep the recording locally in its file system. **2** The target must delete the recording.

rc.dialog.session.accept.directory=

Modifiable Field	**rc.dialog.session.accept.directory**
Field Description	Directory that is used for storing bitmap files that are uploaded when you configure the session acceptance window.
Possible Values	User-defined: for example: /sad_config. Can be specific or relative
Value Definition	

DO NOT EDIT THE FOLLOWING LINE:

schema=

Category Description: Email Settings

email.enabled=

Modifiable Field	**email.enabled**
Field Description	Enable the email function.
Possible Values	True or False
Value Definition	**True** email is enabled. **False** email is not enabled.

smtp.server=

Modifiable Field	**smtp.server**
Field Description	The address of the SMTP server you are using for email.
Possible Values	User-defined - for example: myserver.email.com
Value Definition	

smtp.authentication=

Modifiable Field	**smtp.authentication**
Field Description	The SMTP server must authenticate the SMTP user ID and password.

Possible Values	True or False
Value Definition	**True** SMTP server must authenticate the user ID and password. **False** SMTP server does not authenticate the user ID and password.

`smtp.userid=`

Modifiable Field	**smtp.userid**
Field Description	The user ID for the SMTP server.
Possible Values	User-defined string
Value Definition	

`smtp.password=`

Modifiable Field	**smtp.password**
Field Description	The password for the SMTP server.
Possible Values	User-defined
Value Definition	

`error.admin.contact=`

Modifiable Field	**error.admin.contact**
Field Description	Details or relevant message for contacting an administrator to report a problem.
Possible Values	User-defined message. For example: Contact helpdesk on 123456-123-123
Value Definition	

`file.email.name =`

Modifiable Field	**file.email.name**
Field Description	Default file name that is used when a report is mailed out. For example, Selecting **Email Report** from the **Options** menu. The report is exported into a CSV file with this file name and attached to the email.
Possible Values	User-defined - for example: `report.csv`.
Value Definition	Must not be blank and must contain only characters that are valid for a file name.

`file.email.mime.type =`

Modifiable Field	**file.email.mime.type**
Field Description	Represents the mime type for the file that is attached to an email when a report is mailed out.
Possible Values	User-defined - for example: `application/vnd.ms.excel`.
Value Definition	User-defined; default is `application/vnd.ms.excel`. Must be a mime-type that is compatible only with plain-text or comma-separated value (CSV) files.

`file.email.encoding =`

Modifiable Field	**file.email.encoding**
Field Description	Represents the encoding for the file that is attached to an email when a report is mailed out.
Possible Values	UTF-8, UTF-16BE, UTF16LE
Value Definition	Default value is UTF16LE (Windows standard for Excel)

`file.email.type =`

Modifiable Field	**file.email.type**
Field Description	Represents the type for the file that is attached to an email when a report is mailed out.
Possible Values	TSV, CSV
Value Definition	User-defined. TSV (Tab Separated Value), CSV (comma-separated value).

Category Description: Email Templates

`url=`

Modifiable Field	**url**
Field Description	The main URL users use to access the IBM Endpoint Manager for Remote Control Server UI.
Possible Values	User-defined - for example `http://192.0.2.0/trc`
Value Definition	User-defined. URL and context root of application.

`secure.url=`

Modifiable Field	**secure.url**
Field Description	Determines the base url that is used to redirect requests when secure communications are required.
Possible Values	User-defined - for example**https://*X.X.X.X*/trc** where *X.X.X.X* is the IP address of your IBM Endpoint Manager for Remote Control Server. **Note:** The **url** property must also be configured. Do not replace http with https in the **url** property because the ports for each might be different.
Value Definition	User-defined. URL and context root of application when you use secure connections.

`enforce.secure.web.access=`

Modifiable Field	**enforce.secure.web.access**
Field Description	An HTTP request that is not a target request. The upload, or validation request is redirected to the same URL but uses the value that is set in the **secure.url** parameter as a base.
Possible Values	True or False

Value Definition	**True** The http request is redirected to the secure url. **False** The http request is not redirected to the secure url. **Note:** When you change the value of this property, you must restart the IBM Endpoint Manager for Remote Control Server service for the new value to take effect.

`enforce.secure.endpoint.callhome=`

Modifiable Field	**`enforce.secure.endpoint.callhome`**
Field Description	Determines the url that is used by targets when they send information to the IBM Endpoint Manager for Remote Control Server.
Possible Values	True or False
Value Definition	**True** If an HTTP request is received from a target, the request is redirected to the secure url. The secure url is also returned in the response form the server. Forces targets to use the secure url when they contact the IBM Endpoint Manager for Remote Control Server. When you enable this property and you configure a broker in your environment, you must set the **`ServerURL`** parameter in the broker properties file to HTTPS. Otherwise, the broker does not redirect to the secure url and the target cannot send information to the server. **False** Targets are not forced to use the secure url when they contact the IBM Endpoint Manager for Remote Control Server. False is the default value. **Note:** When you change the value of this property, you must restart the IBM Endpoint Manager for Remote Control Server service for the new value to take effect.

`enforce.secure.endpoint.upload=`

Modifiable Field	**`enforce.secure.endpoint.upload`**
Field Description	Determines whether the controller or target must use the secure url to upload the recordings and audit information to the server.
Possible Values	True / False

Value Definition	**True** If an HTTP upload or a validation request is received, the server redirects the request to an equivalent URL. The URL is built with the value that is defined in **secure.url** as a base. The server also uses the value of **secure.url** as a base to provide the upload and validation URLs to the controller and target when the session starts. When you enable this property and you configure a broker in your environment, you must set the **ServerURL** parameter in the broker properties file to HTTPS. Otherwise, the broker does not redirect to the secure url and the target cannot send information to the server. **False** If an HTTP upload or a validation request is received, the server does not redirect to the secure url. **Note:** When you change the value of this property, you must restart the IBM Endpoint Manager for Remote Control Server service in order for the new value to take effect.

`enforce.secure.weblogon=`

Modifiable Field	**enforce.secure.weblogon**
Field Description	Forces the default logon from the server UI to use https. This property requires **secure.url** to be set with the full host name.
Possible Values	True / False
Value Definition	**True** Log on requests from the IBM Endpoint Manager for Remote Control Server UI use HTTPS. HTTPS is not shown in the url, but the logon page with USERID/PASSWORD is posted by using HTTPS. The URL that is defined in the **secure.url** parameter is used. If **secure.url** is set incorrectly, the logon does not succeed. Enabling this parameter does not prevent a logon request that uses HTTP through another tool or page. **False** Log on by using HTTP or HTTPS. Whichever protocol that is used in the URL that is entered in the browser is used.

`enforce.secure.alllogon=`

Modifiable Field	**enforce.secure.alllogon**
Field Description	Force any logon action to use HTTPS, deny any non-HTTPS logon. When you enable this property, you must set **secure.url** with the full host name.
Possible Values	True / False

Value Definition	**True** Any logon attempt that uses HTTP is rejected and redirected to the logon page. **False** Log on by using HTTP or HTTPS. Whichever protocol that is used in the URL that is entered in the browser is used.

`account.lockout=`

Modifiable Field	**account.lockout**
Field Description	Lock a user account after a consecutive number failed logon attempts. Set to 0 to disable this function.
Possible Values	user defined
Value Definition	User-defined. integer.

`account.lockout.timeout=`

Modifiable Field	**account.lockout.timeout**
Field Description	If user account is locked out due to consecutive failed logon attempts, re-enable the account after this time. The period can be MIN, HOUR, DAY, MONTH. **Note:** This property is only valid when **account.lockout** is enabled.
Possible Values	User-defined
Value Definition	User-defined. MIN, HOUR, DAY, MONTH. For example, set to *5MIN* means that the account is locked for 5 minutes. Set to *2DAY* means that the account is locked for 2 days. **Note:** If left blank, the account is locked until manually set.

`account.lockout.allowlogonfrom=`

Modifiable Field	**account.lockout.allowlogonfrom**
Field Description	Use this property to allow users to log on from this host even if their account is locked out due to consecutive failed logon attempts. If your account is locked, you can log on to the IBM Endpoint Manager for Remote Control Server from the computers whose IP address is listed. For example: 192.0.2.1;192.0.2.2; **Note:** It is important to end each host name with a semi-colon.
Possible Values	User-defined -
Value Definition	User-defined. A list of IP addresses separated by a semi-colon. End the list with a semi-colon.

`account.lockout.reset.on.emailpassword=`

Modifiable Field	**account.lockout.reset.on.emailpassword**
Field Description	Determines whether a locked account is reset when the user selects the forgotten password check box on the logon screen.
Possible Values	True / False

Value Definition	**True** The locked account is reset when the password reset email is received from the administrator. **False** The locked account is not reset when the forgotten password request is received. **Note:** As this property uses the forgotten password feature, email must be enabled in the system.

DO NOT EDIT THIS LINE

```
ip.address=
email.from=
```

Modifiable Field	**email.from**
Field Description	The email address to which users respond when they receive email requests; in some cases, this email address might be the same as the administrators email address.
Possible Values	User-defined - for example: trc@example.com
Value Definition	Email address

```
email.admin=
```

Modifiable Field	**email.admin**
Field Description	The email address of the administrator for reporting problems to.
Possible Values	User-defined: for example, admin@example.com
Value Definition	Email address

DO NOT EDIT THE FOLLOWING LINES

```
task.use.other.threads.queue.limit =
http =
audit.relative.url =
upload.relative.url=
addasset.relative.url=
call.home.relative.url=
oms.relative.url=
call.home.command.parameters=
match.on.assettag =
match.on.computername.if.valid.serial.or.uuid.stored =
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
queue.processors =
```

Modifiable Field	queue.processors
Field Description	Number of processors (CPUs) in the system that is running the IBM Endpoint Manager for Remote Control Server Used to determine the number of working threads that can be used by the IBM Endpoint Manager for Remote Control Server program.
Possible Values	User-defined
Value Definition	User-defined integer

DO NOT EDIT THE FOLLOWING LINES

```
queue.max.length =
serialised.queue.object=
row.sample =
character.width =
max.column.character.width =
min.table.character.width =
```

YOU CAN EDIT THE FOLLOWING FIELD:

```
use.scrollable.table
```

Modifiable Field	**use.scrollable.table**
Field Description	Determine whether you can scroll the results table.
Possible Values	True or False.
Value Definition	**True** you can scroll the table. **False** you cannot scroll the results table.

DO NOT EDIT THE FOLLOWING LINES

```
max.retries=
default.query=
default.pagerows=
query.authorised.queries=
all.users.query=
all.other.users.query=
all.groups.query=
selected.user.query=
selected.users.query=
selected.asset.query=
user.search.query=
asset.search.query=
selected.email.query=
scheduled.task.query=
task.list.query=
all.tasks=
report.list.query=
menu.links.query=
menu.actions.query=
menu.tasks.query=
menu.static.links.query=
menuscheduled.task.log.query=
attachments.query=
query.latest.unprocessed.revision=
query.all.unprocessed.revisions=
query.asset.count=
query.processed.incorrectly=
query.selected.task=
query.all.xml.revisions=
query.users.assets=
query.user.queries=
query.asset.queries=
query.unknown.pc.serial=
query.uploads.in.period.defined=
query.average.upload.time=
query.unprocessed.security.assets=
query.new.assets.in.period.defined=
query.average.process.time=
query.processed.in.period.defined=
query.selected.user.custom.query=
query.all.custom.query=
query.selected.users.groups=
```

```
query.unprocessable.pc.assets.count=
query.menu.static.items=
search.limit.results =
max.keys =
```

Category Description: Action Authority Settings

DO NOT EDIT THE FOLLOWING LINES

```
update.password.auth=
update.details.auth=
change.asset.owner.auth=
add.user.auth=
all.user.auth=
all.asset.auth=
all.custom.reports.auth=
query.builder.auth=
search.auth=
task.auth=
reprocess.auth=
group.auth=
view.group.auth=
delete.user.auth=
email.report.authority=
edit.printer.auth=
user.skill.auth=
add.ticket.auth=
edit.ticket.auth=
setup.ticket.auth=
edit.table.auth=
edit.probeset.auth=
edit.po.auth=
rc.auth=
asset.revisions =
asset.keep.baseline=
```

THE FOLLOWING LINE CAN BE EDITED FOR YOUR ENVIRONMENT:

```
delete.target.auth=
```

Modifiable Field	**delete.target.auth**
Field Description	Determines what level of access is required to delete a target when you use the Delete Target action.
Possible Values	U, S, A
Value Definition	**U** User authority. **S** Super User authority. **A** Administrator authority. This value is the default value. **Note:** If you change the value of this property, you must restart the server service for the new value to take effect.

```
browse.targets.auth=
```

Modifiable Field	**browse.targets.auth**
Field Description	Determines which levels of user authority sees the **Browse** option that is displayed in the **Targets** menu.
Possible Values	U, S, A

Value Definition	**U** User authority. All user authorities see the **Browse** option in the **Targets** menu. This value is the default value. **S** Super User authority. Only Super Users and Admin users see the **Browse** option in the **Targets** menu. **A** Administrator authority. Only Admin users see the **Browse** option in the **Targets** menu. **Note:** If you change the value of this property, you must restart the server service for the new value to take effect.

`view.all.targets.auth=`

Modifiable Field	**`view.all.targets.auth`**
Field Description	Determines which levels of user authority see the **All targets** option that is displayed in the **Targets** menu.
Possible Values	U, S, A
Value Definition	**U** User authority. All user authorities see the **All targets** option in the **Targets** menu. This value is the default value. **S** Super User authority. Only Super Users and Admin users see the **All targets** option in the **Targets** menu. **A** Administrator authority. Only Admin users see the **All targets** option in the **Targets** menu. **Note:** 1. If you change the value of this property, you must restart the server service for the new value to take effect. 2. If the home page of a user is set to the **All targets** report, their authority to view the report is determined by the value of **`view.all.targets.auth`**. If they do not have authority to view All targets, the Search targets page is displayed. 3. If you set **`view.all.targets.auth`** to *S* or *A*, you must set **`target.search.minimum.nonwildcards`** to greater than 1. Otherwise, users with user authority can use the search targets page to display all of the targets.

`search.session.history.auth=`

Modifiable Field	**`search.session.history.auth`**
Field Description	Determines which levels of user authority sees the **Search** option that is displayed in the **Sessions** menu.
Possible Values	U, S, A

Value Definition	**U** User authority. All user authorities see the **Search** option in the **Sessions** menu. This value is the default value. **S** Super User authority. Only Super Users and Admin users see the **Search** option in the **Sessions** menu. **A** Administrator authority. Only Admin users see the **Search** option in the **Sessions** menu. **Note:** If you change the value of this property, you must restart the server service for the new value to take effect.

Category Description: Schedules

DO NOT EDIT THE FOLLOWING LINES

```
scheduled.upload=
update.client.files=
scheduled.upload.interval=
scheduled.upload.queue.threshold=
scheduled.upload.queue.lookup.threshold=
scheduled.update.demographics=
scheduled.demographics.check.interval=
get.application.files.relative.url=
changed.software.upload =
changed.hardware.upload =
scheduled.launch.on.startup=
```

YOU CAN EDIT THE FOLLOWING LINES

Category Description - LDAP synchronization task

`scheduled.interval=`

Modifiable Field	**`scheduled.interval`**
Field Description	The frequency in numeric value that the server must check for scheduled tasks.
Possible Values	User-Defined
Value Definition	User-Defined. Positive Integer **Note:** If you change the value of this property, you must restart the server service for the new value to take effect.

`scheduled.interval.period=`

Modifiable Field	**`scheduled.interval.period`**
Field Description	The unit of time in which the server must check for scheduled tasks.
Possible Values	minutes or hours or days
Value Definition	Minutes or Hours or Days

`scheduled.task.period=`

Modifiable Field	**`scheduled.task.period`**
Field Description	The interval units to be used when scheduling tasks.

Possible Values	minutes or hours or days
Value Definition	Minutes or Hours or Days

DO NOT EDIT THE FOLLOWING LINES

```
scheduler.use.queue=
task.process.xml.max.queue.length=
task.process.files.max.queue.length=
task.process.filescan.max.queue.length=
task.process.software.security.length=
```

YOU CAN EDIT THE FOLLOWING LINES

DBCleaner is a looping utility that is used to clean up older log files that are based on age of entries (in days). Frequency is in days. To disable cleaning, set the value to **-1**.

```
dbcleaner.launch.on.startup=
```

Modifiable Field	**dbcleaner.launch.on.startup**
Field Description	Start **dbCleaner** when the server application starts.
Possible Values	1 or 0
Value Definition	1 to start **dbCleaner**. 0, do not start **dbCleaner**.

```
dbcleaner.frequency=
```

Modifiable Field	**dbcleaner.frequency**
Field Description	Frequency the DBCleaner runs at in days
Possible Values	set to *-1* to disable cleaning
Value Definition	User-Defined - number of days

```
dbcleaner.interval.period=
```

Modifiable Field	**dbcleaner.interval.period**
Field Description	Period the database logs are cleaned
Possible Values	User-Defined. for example: *mins*, or *hours*, or *days*, or *months*
Value Definition	User-Defined - number of days

```
server.log.max.age=
```

Modifiable Field	**server.log.max.age**
Field Description	Maximum age of entries in the server log file, before they are deleted.
Possible Values	User-Defined
Value Definition	User-Defined - number of days

DO NOT EDIT THE FOLLOWING LINE

```
tx.log.max.age=
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
task.log.max.age=
```

Modifiable Field	**task.log.max.age**
Field Description	Maximum age of entries in the task log table before they are deleted.
Possible Values	User-Defined
Value Definition	User-Defined - number of days

`transfers.history.max.age=`

Modifiable Field	**transfers.history.max.age**
Field Description	Maximum age of entries in the transfer table before they are deleted.
Possible Values	User-Defined
Value Definition	User-Defined - number of days

`user.access.max.age=`

Modifiable Field	**user.access.max.age**
Field Description	Maximum age of entries in the access table before they are deleted.
Possible Values	User-Defined
Value Definition	User-Defined - number of days

DO NOT EDIT THE FOLLOWING LINES:

`logon.disclaimer=`

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

Category Description: Password Settings

`password.encrypt=`

Modifiable Field	**password.encrypt**
Field Description	Determines whether passwords are encrypted in the database.
Possible Values	Yes or No
Value Definition	**Yes** passwords are encrypted in the database. **No** passwords are not encrypted in the database.

`password.reuse=`

Modifiable Field	**password.reuse**
Field Description	Whether users can reuse passwords.
Possible Values	Yes or No
Value Definition	**Yes** users can reuse passwords. **No** users cannot reuse passwords.

`expire.new.password=`

Modifiable Field	**expire.new.password**

Field Description	Determines whether users are required to set their own password after they receive the computer-generated password.
Possible Values	True or False
Value Definition	**True** users must set their own password after they receive the computer-generated password. **False** users do not have to set their own password after they receive the computer-generated password.

`password.timeout=`

Modifiable Field	**password.timeout**
Field Description	Determines whether passwords expire.
Possible Values	True or False
Value Definition	**True** passwords expire. **False** passwords do not expire.

`password.timeout.period=`

Modifiable Field	**password.timeout.period**
Field Description	After how many days passwords expire.
Possible Values	User-defined
Value Definition	User-defined integer

`password.period=`

Modifiable Field	**password.period**
Field Description	Maximum number of days before a password can be reused.
Possible Values	User-defined
Value Definition	User-defined integer

`password.check=`

Modifiable Field	**password.check**
Field Description	Determines whether to enable password rule checking.
Possible Values	True or False
Value Definition	**True** passwords must follow certain rules. **False** passwords do not follow rules.

`password.must.have.non.numeric=`

Modifiable Field	**password.must.have.non.numeric**
Field Description	Determines whether passwords must contain non-numeric characters.
Possible Values	True or False

Value Definition	**True** passwords must contain non-numeric characters. **False** passwords do not need to contain non-numeric characters.

`password.must.have.numeric=`

Modifiable Field	**password.must.have.numeric**
Field Description	Determines whether passwords must contain numeric characters.
Possible Values	True or False
Value Definition	**True** passwords must contain numeric characters. **False** passwords do not have to contain numeric characters.

`password.must.have.non.alphanumeric=`

Modifiable Field	**password.must.have.non.alphanumeric**
Field Description	Whether passwords must contain non-alphanumeric characters.
Possible Values	True or False
Value Definition	**True** passwords must contain non-alphanumeric characters. **False** passwords do not have to contain non-alphanumeric characters.

`password.min.length=`

Modifiable Field	**password.min.length**
Field Description	Minimum length of a password.
Possible Values	User-defined
Value Definition	User-defined integer

`password.max.length=`

Modifiable Field	**password.min.length**
Field Description	Maximum length of a password.
Possible Values	User-defined
Value Definition	User-defined integer

`password.max.matching.sequential.chars=`

Modifiable Field	**password.max.matching.sequential.chars**
Field Description	Maximum number of sequential password characters that can match.
Possible Values	User-defined
Value Definition	User-defined integer

`password.max.previous.chars=`

Modifiable Field	**password.max.previous.chars**
Field Description	Maximum number of sequential password characters that can be reused in a new password.
Possible Values	User-defined
Value Definition	User-defined integer

```
password.iterationcount =
```

Modifiable field	**password.iterationcount**
Field Description	Use to define the number of times that a password is hashed before it is stored in the database.
Possible Values	User defined.
Value Definition	Default is 5000. There is no maximum value. The higher the iteration count, the longer it takes for someone to try to break the password. However, the larger the iteration count, the slower it is to log on to the server or to change your password. A higher iteration count slows the system down. Therefore you must set it to a value that is acceptable to your environment and maintains acceptable performance.

DO NOT EDIT THE FOLLOWING LINE

```
table.column.internationalisation =
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
csv.export.use.byte.order.mark=
```

Modifiable Field	**csv.export.use.byte.order.mark**
Field Description	Determines whether a Unicode UTF-8 Byte Order Mark (BOM) is included at the start of the file when you export a CSV file.
Possible Values	True or False
Value Definition	**True** Include a Unicode UTF-8 Byte Order Mark (BOM). **False** Do not include a Unicode UTF-8 Byte Order Mark (BOM).

```
tsv.export.use.byte.order.mark=
```

Modifiable Field	**tsv.export.use.byte.order.mark**
Field Description	Determines whether a Unicode UTF-8 Byte Order Mark (BOM) is included at the start of the file when you export a TSV file.
Possible Values	True or False
Value Definition	**True** Include a Unicode UTF-8 Byte Order Mark (BOM). **False** Do not include a Unicode UTF-8 Byte Order Mark (BOM).

```
edit.properties.show.file.comments =
```

Modifiable Field	**edit.properties.show.file.comments**
Field Description	Determines whether you see the comments in the properties file when you edit the properties in the server UI.
Possible Values	1 / 0
Value Definition	**1** The comments are displayed when you edit the properties. **0** The comments are not displayed when you edit the properties.

`edit.properties.show.translated.comments=`

Modifiable Field	**edit.properties.show.translated.comments**
Field Description	Determines whether you see the available globalized comments in the properties file when you edit the properties in the server UI.
Possible Values	1 / 0
Value Definition	**1** The comments are displayed when you edit the properties. **0** The comments are not displayed when you edit the properties.

`date.time.format=`

Modifiable Field	**date.time.format**
Field Description	Defines the way dates and times are input into any date/time fields
Possible Values	User-defined
Value Definition	User-defined for example EEEE, dd MMMM yyyy, HH:mm:ss

`date.only.format =`

Modifiable Field	**date.only.format**
Field Description	Defines the way dates are input into any date only fields
Possible Values	User-defined
Value Definition	User-defined for example EEEE, dd MMMM yyyy

`time.only.format =`

Modifiable Field	**time.only.format**
Field Description	Defines the way dates are input into any date only fields
Possible Values	User-defined
Value Definition	User-defined for example: HH:mm:ss

`invalid.macs =`

Modifiable Field	**invalid.macs**

Field Description	List of target Mac addresses that are unacceptable to send to the server in the target information.
Possible Values	User Defined for example - 000000000001
Value Definition	

`invalid.assettags =`

Modifiable Field	**invalid.assettags**
Field Description	List of target **assettags** that are unacceptable to send to the server in the target information.
Possible Values	User Defined for example, unknown
Value Definition	

`invalid.net.addresses =`

Modifiable Field	**invalid.net.addresses**
Field Description	List of target network addresses that are unacceptable to send to the server in the target information.
Possible Values	User Defined for example -0.0.0.0,127.0.0.0/8
Value Definition	

`report.timeout.frequency =`

Modifiable Field	**report.timeout.frequency**
Field Description	When a report is generated its output is cached, so that it can be reloaded without the application going back to the database for the data. The property **report.timeout.frequency** defines the time value that the report output is cached for.
Possible Values	User Defined
Value Definition	

`report.manager.frequency =`

Modifiable Field	**report.manager.frequency**
Field Description	This property defines the time value for how often the Report manager loops and re loads the report data from the database
Possible Values	User Defined
Value Definition	

`report.manager.period =`

Modifiable Field	report.manager.period
Field Description	Defines the time period that is used for **report.timeout.frequency** and **report.timeout.frequency**.
Possible Values	User Defined. for example seconds, minutes, hours. Default is minutes
Value Definition	

`allow.target.group.override =`

Modifiable Field	**allow.target.group.override**
Field Description	Determines the group that a target is made a member of during a silent target installation when the **GROUP_LABEL** parameter is used.
Possible Values	True or False
Value Definition	**True** The target is assigned to the target group that the **GROUP_LABEL** parameter defines. **False** The target is assigned to the default target group that is defined for the **default.group.name** property.

`default.group.name =`

Modifiable Field	**default.group.name**
Field Description	Defines the name that is given to the default group of users
Possible Values	User Defined. for example DefaultGroup
Value Definition	

Category Description: Default Non-Binary Policies values

`default.rc_def_inactivity =`

Modifiable Field	**default.rc_def_inactivity**
Field Description	Number of seconds to wait before the remote control session connection stops automatically if there is no session activity.
Possible Values	User Defined - seconds
Value Definition	• 0 - disables the timer and the session does not time out. • less than 60 - session times out after 60 seconds. • greater than 60 - session times out when the value is reached.

`default.rc_def_grace_time =`

Modifiable Field	**default.rc_def_grace_time**
Field Description	Sets the number of seconds to wait for the target user to respond before a session starts or times out, used with **Enable user acceptance for incoming connections**.
Possible Values	User-defined - 0 - 60 seconds
Value Definition	If set to 0, the session starts without displaying the user acceptance window on the target. Default is 5

`default.rc_def_timeout_op =`

Modifiable Field	**default.rc_def_timeout_op**

Field Description	Determines what action is taken if the user acceptance window timeout lapses. That is, the target user does not click accept or refuse within the number of seconds defined for **Acceptance Grace time**
Possible Values	ABORT or PROCEED
Value Definition	**Abort** Session is not started. Default is Abort. **Proceed** Session is started.

DO NOT EDIT THE FOLLOWING LINES

```
default.rc_def_local_audit
default.rc_def_pre_script =
default.rc_def_post_script=
```

YOU CAN EDIT THE FOLLOWING LINES

```
default.rc_def_script_op =
```

Modifiable Field	**default.rc_def_script_op**
Field Description	Determines what action is taken if the prescript execution fails. A positive value or 0 is considered as a successful run of the pre-session script. A negative value, script not found, or not finished running within 3 minutes is considered a failure.
Possible Values	ABORT or PROCEED
Value Definition	**Abort** If the prescript run is a fail, the session does not start. **Proceed** If the prescript run is a fail, the session continues.

```
default.rc_def_insession_ft =
```

Modifiable Field	**default.rc_def_insession_ft**
Field Description	Controls the transfer of files during an **Active** session. Its value determines the availability of the **Send file** or **Pull file** options in the **File Transfer menu** within the controller window.
Possible Values	NONE, BOTH, SEND, PULL

Value Definition	**Set to NONE** The **Send file** and **Pull file** options are not available for selection. No file transfers can be initiated. **Set to BOTH** The **Send file** and **Pull file** options are available for selection. Files can be transferred to the target and transferred from the target. BOTH is the default value. **Set to PULL** Only the **Pull file** option is available for selection. Files can be transferred only from the target. **Set to SEND** Only the **Send file** option is available for selection. Files can be transferred only to the target.

DO NOT EDIT THE FOLLOWING LINES

```
default.rc_def_ft_actions =
default.rc_def_allowed_times
new.password.template
access.request.request.template
access.request.request.anon.template
access.request.reject.template
access.request.reject.anon.template
access.request.grant.template
access.request.grant.anon.template
```

YOU CAN EDIT THE FOLLOWING LINES

```
trc.feature.remote.install =
```

Modifiable Field	**trc.feature.remote.install**
Field Description	Determines the availability of the Remote Install function.
Possible Values	True or False
Value Definition	**True** The Remote Install function is available in the **Admin** menu. **False** The Remote Install function is not available in the **Admin** menu. **Note:** If you set this property back to true, after it is set to false you must restart the server service.

```
trc.feature.denied.program.execution.list =
```

Modifiable Field	**trc.feature.denied.program.execution.list**
Field Description	Determines the availability of the Denied Program Execution policy when you create groups or permissions links.
Possible Values	True / False

Value Definition	**True** The **Denied program execution list** policy is displayed on the Edit group screen and the Manage Permissions screen. **False** The **Denied program execution list** policy is not displayed on the Edit group screen and the Manage Permissions screen. **Note:** This feature works only on the following operating systems • Windows XP (32-bit editions only) • Windows Server 2003 (32-bit editions only) **Note:** If you set this property back to true, after it is set to false, you must restart the server service.

`trc.ticket.allow.access =`

Modifiable Field	**trc.ticket.allow.access**
Field Description	Determines the availability of the **Request Access** function.
Possible Values	1 or 0
Value Definition	**1** The **Request Access** option is displayed on the start session screen. This option allows the controller user to temporarily access a target that they do not have permission to access. **0** The **Request Access** option is not displayed on the start session screen and the **Request Access** menu item is disabled.

`trc.ticket.allow.allaccess =`

Modifiable Field	**trc.ticket.allow.allaccess**
Field Description	Determines the availability of the **Request Access** function when a user who is not registered in IBM Endpoint Manager for Remote Control tries to access by using the anonymous URL. For more information about the anonymous URL and how to request access to targets when you are not a registered user in the IBM Endpoint Manager for Remote Control Server, see the IBM Endpoint Manager for Remote Control Controller User's Guide .
Possible Values	1 or 0
Value Definition	**1** The Request Access to target screen is displayed when the user types in the anonymous URL. `http://servername/trc/requestAccessAnon.do` where *servername* is the address of your IBM Endpoint Manager for Remote Control Server **0** The logon screen is displayed when the user types in the anonymous URL.

trc.ticket.admin =

Modifiable Field	**trc.ticket.admin**
Field Description	Defines the user group of administrators who receive an email when an access request is submitted.
Possible Values	User defined, for example: *Adminemail*. **Note:** 1. The group name must be a valid user group that is already defined in the server. 2. If this field is left blank, the email address that is set for the property **email.admin** receives an email when an access request is submitted.
Value Definition	The group name must be already defined in the database.

trc.ticket.groupprefix =

Modifiable Field	**trc.ticket.groupprefix**
Field Description	Defines the prefix that is assigned to the name of the temporary user and target groups that are created when an access request is granted.
Possible Values	User-defined for example: t$t
Value Definition	The temporary groups names are in the format P_R_Gwhere • P = trc.ticket.groupprefix property • R = the request key value for the access request • G = the group type U for user group, T for target group. for example : t$t_5_U

trc.ticket.priority =

Modifiable Field	**trc.ticket.priority**
Field Description	Defines the default priority level for access request permissions.
Possible Values	0, 1, or 5
Value Definition	The priority value that is used when you set permissions for an access request. The value overrides any other permission values. For example: 5 is the highest priority. 5 overrides 1 and 1 overrides 0.

trc.default.request.priority =

Modifiable Field	**trc.default.request.priority**
Field Description	Defines the priority value that is displayed first in the priority list when you set the permissions for an access request.
Possible Values	0, 1, 5

Value Definition	**0** 0 is displayed first in the list. **1** 1 is displayed first in the list. **5** 5 is displayed first in the list.

DO NOT EDIT THE FOLLOWING LINES

```
trc.ticket.temp.usergrpupdesc
trc.ticket.temp.targetgrpupdesc
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

`task.logdistribution.enabled =`

Modifiable Field	**task.logdistribution.enabled**
Field Description	Determines whether the logs that contain session information are written to the IBM Endpoint Manager for Remote Control Server.
Possible Values	True or False
Value Definition	**True** The logs are written to the server to the location defined by `task.logdistribution.path`. **False** The logs are not written to the server.

`task.logdistribution.path =`

Modifiable Field	**task.logdistribution.path**
Field Description	Determines the location that the log file that contains session information is written to on the server.
Possible Values	User defined. for example `c:\logtask\logs`
Value Definition	

DO NOT EDIT THE FOLLOWING LINE

```
task.logdistribution.file
```

YOU CAN EDIT THE FOLLOWING LINES

`registry.title.`***X*** `=`

Modifiable Field	**registry.title.***X*
Field Description	Defines the name of the menu item that is displayed in the registry keys menu. Use the menu to view the value for the specific registry key that is defined by **registry.key.***X*
Possible Values	User defined. for example Services
Value Definition	*X* = 0 - 9.

`registry.key.`***X*** `=`

Modifiable Field	**registry.key.***X*

Field Description	Defines the path to a specific registry key that you can use to view its value on the target.
Possible Values	User defined. for example `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services`
Value Definition	*X* = 0 - 9.

`nat.ip.support =`

Modifiable Field	**nat.ip.support**
Field Description	Used to define the list of IP addresses that are used by the server when a connection is made to a target when NAT addresses are present.
Possible Values	0, 1, 2, 3, 4
Value Definition	**0** IP=heartbeatlist. Server uses the heartbeat list of IP addresses to make a connection with the target. **1** *IP= heartbeatlist; source* Server uses the **heartbeatlist** list of IP addresses then the source IP address to make a connection with the target. **2** *IP = source;heartbeatlist* Server uses the source IP address then the **heartbeatlist** of IP addresses to make a connection with the target. **3** *IP = heartbeat;source* Server checks the IP addresses that are listed in the **nat.exclude.list** property to see whether the source IP is there. If it is not, the server uses the **heartbeatlist** of IP addresses and then source IP address to make a connection with the target. **4** *IP = source;heartbeat* Server checks the IP addresses listed in the **nat.exclude.list** property to see whether the source IP is there. If it is not, the server uses the source IP and then the **heartbeatlist** of IP addresses to make a connection with the target.

`nat.exclude.list =`

Modifiable Field	**nat.exclude.list**
Field Description	Defines a list of NAT addresses that are ignored by the server.
Possible Values	User defined.
Value Definition	

`match.allow.data.changes =`

Modifiable Field	**match.allow.data.changes**

Field Description	Is used to find a match for a target in the database if a perfect match cannot be found. For more information about how targets are registered, see Chapter 16, “Ensuring targets are registered correctly,” on page 141.
Possible Values	True or False
Value Definition	**True** This value is the default value. When set to true, a best match is considered if all but 1 of the 4 perfect match criteria match an already registered target. **False** If the perfect match process is enabled and no match is found for all 4 of the target criteria, the best match option is not considered. Depending on the value of **match.change.notifications**, if no match is found then a new target entry is created in the database.

`match.computername.only =`

Modifiable Field	**match.computername.only**
Field Description	Determines whether a targets computer name is used to see whether it is already registered with the IBM Endpoint Manager for Remote Control Server. When a target contacts the server, its computer name is compared to the computer names of the targets that are already registered with the server. If a match is found, the details of the matched target are updated. If no match is found, a new target entry is created. For more information about how targets are registered, see Chapter 16, “Ensuring targets are registered correctly,” on page 141.
Possible Values	True or False
Value Definition	**True** When a target contacts the server, the targets computer name is checked against the computer names of already registered targets. If a match is found, the details of the matched target are updated with the details of the target that is contacting the server. If no match is found, a new target entry is created. **False** When a target contacts the server, the targets computer name is not used to see whether the target is already registered with the server.

`match.guid.only =`

Modifiable Field	**match.guid.only**

Field Description	Determines whether a targets *guid* is used to see whether it is already registered with the IBM Endpoint Manager for Remote Control Server. When a target contacts the server, its *guid* is compared to the *guid* values of the targets that are already registered with the server. If a match is found, the details of the matched target are updated. If no match is found, a new target entry is created. For more information about how targets are registered, see Chapter 16, "Ensuring targets are registered correctly," on page 141.
Possible Values	True or False
Value Definition	**True** When a target contacts the server, the targets *guid* is checked against the *guid* values of already registered targets. If a match is found, the details of the matched target are updated with the details of the target that is contacting the server. If no match is found, a new target entry is created. **False** When a target contacts the server, the targets *guid* is not used to see whether the target is already registered with the server.

`match.change.notification =`

Modifiable Field	**`match.change.notification`**
Field Description	Use this property to force a target to save its configuration details locally. If any of the target details change, it can send the old details and its current details to the server. The details can be used to try to find a match in the database. For more information about how targets are registered, see Chapter 16, "Ensuring targets are registered correctly," on page 141.
Possible Values	True or False
Value Definition	**True** This value is the default value. The target saves its details locally to a file called `tgt_info.proprties`. When the target contacts the server, it sends its old details and its new details. The old details are used to try to find a perfect match for the target in the database. **False** The old target details are not sent to the server and the new changed details are used to try to find a match. However if only one of the 4 criteria changes and the **`match.allow.data.changes`** property is set to true, then a best match is looked for.

`rc.tmr.at.registration =`

Modifiable Field	**`rc.tmr.at.registration`**

Field Description	Determines whether a target is assigned to target groups by using rules the first time it registers with the IBM Endpoint Manager for Remote Control Server
Possible Values	True or False
Value Definition	**True** When a target contacts the server for the first time, its computer name and IP address is compared to the computer names and IP addresses that are defined in the target membership rules. If a match is found, the target is assigned to the target groups that are defined in the matching rules. **False** When a target contacts the server for the first time, the targets computer name and IP address are not checked against any defined rules.

`rc.tmr.at.every.callhome =`

Modifiable Field	**`rc.tmr.at.every.callhome`**
Field Description	Determines whether a target is assigned to target groups by using rules every time it contacts the IBM Endpoint Manager for Remote Control Server
Possible Values	True or False
Value Definition	**True** Every time that a target contacts the server its computer name and IP address are compared to the computer names and IP addresses that are defined in the target membership rules. If a match is found, the target is assigned to the target groups that are defined in the matching rules. Therefore, the targets group membership is recalculated every time that it contacts the server. **False** Every time that a target contacts the server its computer name and IP address are not checked against any defined rules.

`rc.tmr.at.triggered.callhomes =`

Modifiable Field	**`rc.tmr.at.triggered.callhomes`**
Field Description	Determines whether a target is assigned to target groups by using rules any time it contacts the IBM Endpoint Manager for Remote Control Server because of a change to its configuration or when it comes online.
Possible Values	True or False

Value Definition	**True** When a target contacts the server because of a configuration change or when it comes online, its computer name and IP address are compared to the computer names and IP addresses that are defined in the target membership rules. If a match is found, the target is assigned to the target groups that are defined in the matching rules. **False** Any time a target contacts the server because of a configuration change or when it comes online, its computer name and IP address is not checked against any defined rules.

```
rc.tmr.at.rules.change =
```

Modifiable Field	**rc.tmr.at.rules.change**
Field Description	When a rule is added, edited, or deleted. Determines whether the target group membership is altered for targets that were assigned to target groups by using rules.
Possible Values	True or False
Value Definition	**True** Applies to targets whose group membership was assigned by using rules. Their group membership is recalculated whenever a rule is added, edited, or deleted. **False** Applies to targets whose group membership was assigned by using rules. Their group membership is not recalculated whenever a rule is added, edited, or deleted.

DO NOT EDIT THE FOLLOWING LINES

```
hb.timeout.lookup.mode
hb.timeout.att.defn
```

THE FOLLOWING LINE CAN BE EDITED FOR YOUR ENVIRONMENT:

```
oracle.increment.keys.off =
```

Modifiable Field	**oracle.increment.keys.off**
Field Description	Used as a workaround for a driver bug in the Oracle JDBC versions 5 & 6 drivers that are included with Oracle 11g
Possible Values	1 or 0
Value Definition	**1** Set to 1 if you are using the Oracle JDBC versions 5 & 6 drivers. **0** Set to 0 if you are using JDBC 4 drivers (Oracle 10i) or if future versions of the JDBC driver address the get autogenerated keys bug.

```
default.homepage.method=
```

Modifiable Field	**default.homepage.method**
Field Description	Used to determine whether the default home page is a report, or the search targets page. This property is useful if you have numerous targets in the IBM Endpoint Manager for Remote Control database. The default home page that is set by the server is the **All targets** report. The report can take some time to load if you have numerous targets. Then you must scroll through the report to find the relevant target. If you set the search page as the home page, you can search for specific targets as soon as you log on.
Possible Values	report or search
Value Definition	**report** The default home page is set to the report that is defined by the query in the **default.query** property. By default it is the **All targets** report. **search** The default home page is set to the search targets page. **Note:** This property is overridden if a home page is already defined. For example, • The user defines their own home page. • A home page is defined for the user groups that the user belongs to. For more information about setting a home page, see Chapter 12, "Managing the home page for a user or group," on page 105.

```
workaround.rdp.console.w2k3 =
```

Modifiable Field	**workaround.rdp.console.w2k3**
Field Description	Used as a workaround for a Windows 2003 limitation. A remote control session cannot capture the display if a remote desktop session has taken place or is taking place on the target.
Possible Values	0, 1 or 2

Value Definition	When a Remote Desktop user uses the **/admin** or **/console** option to start a Remote Desktop session with a Windows Server 2003 system and a IBM Endpoint Manager for Remote Control user starts a remote control session before, during or after the Remote Desktop session, remote control is unable to capture the display. The result is that a gray screen is displayed in the controller. This issue is a limitation in Windows Server 2003, therefore this property provides a workaround that will reset the Windows session either after each Remote Desktop session ends, or before a IBM Endpoint Manager for Remote Control session starts, depending on the value selected. **0** The workaround is disabled. This value is the default value. **1** Reset the session automatically when a remote control session is started. **Note:** The Windows sessions take a couple of minutes to initialize and the controller sees a blank desktop until the initialization is complete. A message is displayed to inform the controller user that the session is being reset and it might take a few minutes. **2** Reset the session automatically when the Remote Desktop user logs out. **Note:** 1. The value set for this property applies to all targets that are registered with the server. You can set an attribute for a target group to limit the action to selected targets. For more information about the attribute, see "Creating target groups" on page 22. If the server property has a different value to the target group attribute, the target group value takes precedence for those targets who are members of the specific target group. 2. If a Remote Desktop session (admin or console) is in progress when the controller attempts to connect to a target, a message is displayed to the controller. The message provides details of the Remote Desktop user and the IP address and computer name that the session is running from.

`target.search.minimum.nonwildcards =`

Modifiable Field	**target.search.minimum.nonwildcards**
Field Description	Sets the minimum number of non-wildcard characters that are allowed to be entered when you search for a target.
Possible Values	User-defined integer, default is 0.

Value Definition	Determines the minimum non-wildcard characters that must be entered in the search targets field on the search targets page. For example set to 2 means that at least 2 non-wildcard characters must be entered. For example, `se` or `te`. If you enter less than the minimum characters, the following error is displayed on the screen - `The search string must contain at least X non-wildcard characters.` ***X*** is the value set in the property. **Note:** If you set **`view.all.targets.auth`** to `S` or `A`, you must set **`target.search.minimum.nonwildcards`** to greater than 1. The reason is to prevent users who have user authority from using the search targets page to display all targets.

`target.search.maximum.wildcards =`

Modifiable Field	**`target.search.maximum.wildcards`**
Field Description	Sets the maximum number of wildcard characters that are allowed to be entered when you search for a target. The wildcard characters that are allowed are *, %, * and _.
Possible Values	User-defined integer, default is 0.
Value Definition	The value set determines the maximum number of wildcard characters that you can enter in the search targets field, on the search targets page. For example, set to 1 means that only 1 wildcard characters can be entered. For example, `se*` or `te*`. If you enter more than the maximum characters the following error is displayed on the screen - `The number of wildcards in the search string cannot exceed X .` ***X*** is the value set in the property.

To reduce the volume of unnecessary heartbeats the following properties can be configured.

`heartbeat.retry =`

Modifiable Field	**`heartbeat.retry`**
Field Description	If a target cannot contact the IBM Endpoint Manager for Remote Control Server, use this property to define the number of minutes that the target waits before trying to contact it again.
Possible Values	User-defined: minutes
Value Definition	Default is 10.

`heartbeat.delay=`

Modifiable Field	**`heartbeat.delay`**
Field Description	The maximum delay in minutes that a target waits between sending heartbeats to the IBM Endpoint Manager for Remote Control Server.
Possible Values	User-defined: minutes

Value Definition	Default is 20 minutes. Prevent multiple heartbeats in quick succession by delaying the actual heartbeat when a heartbeat is triggered.

`heartbeat.on.wake =`

Modifiable Field	**heartbeat.on.wake**
Field Description	Trigger a heartbeat when the target system wakes from standby or hibernation.
Possible Values	1 or 0
Value Definition	**1** Trigger a heartbeat when the target system wakes from standby or hibernation. **0** Do not trigger a heartbeat when the target system wakes from standby or hibernation. This value is the default value.

`heartbeat.on.userchange =`

Modifiable Field	**heartbeat.on.userchange**
Field Description	Trigger a heartbeat when a user logs on or off
Possible Values	1 or 0
Value Definition	**1** Trigger a heartbeat when a user logs on or off. This value is the default value. **0** Do not trigger a heartbeat when a user logs on or off.

`heartbeat.on.change =`

Modifiable Field	**heartbeat.on.change**
Field Description	Trigger a heartbeat when any of the values included in a heartbeat change.
Possible Values	1 or 0
Value Definition	**1** Trigger a heartbeat when any of the values included in a heartbeat change. This value is the default value. **0** Do not trigger a heartbeat when any of the values included in a heartbeat change. This value is the default value.

`heartbeat.on.stop =`

Modifiable Field	**heartbeat.on.stop**
Field Description	Trigger a heartbeat when the target is stopped or the system is shutting down
Possible Values	1 or 0

Value Definition	**1** Trigger a heartbeat when the target is stopped or the system is shutting down. **0** Do not trigger a heartbeat when the target is stopped or the system is shutting down. This value is the default value. **Note:** **HeartBeatOnStop** set to 1 is not recommended unless **HeartBeatDelay** is set to 0. Otherwise, remote control sessions cannot be started while the heartbeat is being delayed.

`broker.code.length =`

Modifiable Field	**broker.code.length**
Field Description	Determines the number of characters that are required to be entered for the connection code. Enter the connection code when you start a remote control session through an Internet Connection Broker.
Possible Values	User-defined integer.
Value Definition	Default is 7. There is no limit to the number of characters that can be set. However, you must use your discretion when you set the value.

`broker.code.timeout =`

Modifiable Field	**broker.code.timeout**
Field Description	Determines the number of seconds the connection code timer counts down from, before a new code is needed. The timer is displayed on the controller when you start a remote control session by using a broker.
Possible Values	User defined.
Value Definition	Default is 900.

`broker.trusted.certs.required =`

Modifiable Field	**broker.trusted.certs.required**
Field Description	Determines whether strict certificate validation is enabled.
Possible Values	true or false.
Value Definition	**true** Strict certificate validation is enabled. This value is the default value. **false** Strict certificate validation is disabled.

`rc.recording.filename.format =`

Modifiable Field	**rc.recording.filename.format**
Field Description	Specifies the file name format that is used in the server to store the recordings
Possible Values	User defined. Some formatting variables can be added to the file name to customize it

Value Definition	For example, `trcrecording_%S_%D_%T.trc` where *%S* is placeholder for the session id of the recording *%D* is placeholder for the date of the recording *%T* is placeholder for the time stamp of the recording *%H* is placeholder for the host name of the target

common.properties

`index.title=`

Modifiable Field	**index.title**
Field Description	Title of the Application
Possible Values	User defined - for example IBM Endpoint Manager for Remote Control
Value Definition	

DO NOT EDIT THE FOLLOWING LINES

`product=`
`jndi.context=`

YOU CAN EDIT THE FOLLOWING LINES

`datasource.context=`

Modifiable Field	**datasource.context**
Field Description	Defines the jndi name for the database
Possible Values	User Defined - for example jdbc/trcdb
Value Definition	

`fips.compliance=`

Modifiable Field	**fips.compliance**
Field Description	Used as part of the process for enabling FIPS compliance on the server. For more information about enabling FIPS compliance, see the IBM Endpoint Manager for Remote Control Installation Guide.
Possible Values	True or False
Value Definition	**true** Used as part of the process for enabling FIPS compliancy on the server. You should also follow the instructions in the IBM Endpoint Manager for Remote Control Installation Guide for enabling FIPS compliancy. **false** FIPS compliancy will not be enabled.

`sp800131a.compliance=`

Modifiable Field	**sp800131a.compliance**

Field Description	Used as part of the process for enabling NIST SP800-131A compliance on the server. For more information about enabling NIST SP800-131A compliance, see the *IBM Endpoint Manager for Remote Control Installation Guide*.
Possible Values	True or False
Value Definition	**true** NIST SP800-131A compliance is enabled. Used as part of the process for enabling NIST SP800-131A compliance on the server. You must also follow the instructions in the *IBM Endpoint Manager for Remote Control Installation Guide* for enabling NIST SP800-131A compliance. **false** NIST SP800-131A compliance is not enabled.

`authentication.LDAP=`

Modifiable Field	**authentication.LDAP**
Field Description	Determines whether LDAP authentication is used
Possible Values	True or False
Value Definition	**True** LDAP authentication is used **False** LDAP authentication is not used

`authentication.LDAP.config=`

Modifiable Field	**authentication.LDAP.config**
Field Description	Name of the properties file which contains the LDAP properties
Possible Values	User Defined for example - ldap.properties
Value Definition	

`sync.LDAP=`

Modifiable Field	**sync.LDAP**
Field Description	This is used to synchronize the users and group from Active Directory with the IBM Endpoint Manager for Remote Control database.
Possible Values	True or False
Value Definition	**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

DO NOT EDIT THE FOLLOWING

```
application.log.file
application.resources
default.properties.0=
default.properties.1=
default.properties.2=
default.properties.3=
```

```
generic.database.create=
generic.database.directory=
generic.database.populate=
db.scripts.use.new.line=
```

THE FOLLOWING LINE CAN BE EDITED FOR YOUR ENVIRONMENT:

```
properties.backup.archive=
```

Modifiable Field	**properties.backup.archive**
Field Description	Number of copies of the property backups to keep
Possible Values	User defined Integer
Value Definition	

DO NOT CHANGE THE FOLLOWING FIELDS

```
common.schema
auto.increment.keys
automatically.adjust.database
user.table.1
user.table.2
```

THE FOLLOWING LINES CAN BE EDITED FOR YOUR ENVIRONMENT:

```
users.title.required=
```

Modifiable Field	**users.title.required**
Field Description	Whether the title field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

```
users.forename.required=
```

Modifiable Field	**users.forename.required**
Field Description	Whether the forename field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

```
users.surname.required=
```

Modifiable Field	**users.surname.required**
Field Description	Whether the surname field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

```
users.country.required=
```

Modifiable Field	**users.country.required**

Field Description	Whether the country field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.userid.required=`

Modifiable Field	**users.userid.required**
Field Description	Whether the userid field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.address_1.required=`

Modifiable Field	**users.address_1.required**
Field Description	Whether the address1 field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.address_2.required=`

Modifiable Field	**users.address_2.required**
Field Description	Whether the address2 field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.email.required=`

Modifiable Field	**users.email.required**
Field Description	Whether the email field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.town.required=`

Modifiable Field	**users.town.required**
Field Description	Whether the town field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.postcode.required=`

Modifiable Field	**users.postcode.required**
Field Description	Whether the postcode field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.nickname.required=`

Modifiable Field	**users.nickname.required**
Field Description	Whether the nickname field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.tel_no.required=`

Modifiable Field	**users.tel_no.required**
Field Description	Whether the tel_no field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.mob_no.required=`

Modifiable Field	**users.mob_no.required**
Field Description	Whether the mob_no field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.employeeid.required=`

Modifiable Field	**users.employeeid.required**
Field Description	Whether the employeeid field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

`users.department.required=`

Modifiable Field	**users.department.required**
Field Description	Whether the department field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

users.location.required=

Modifiable Field	**users.location.required**
Field Description	Whether the location field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

users.password.required=

Modifiable Field	**users.password.required**
Field Description	Whether the password field is required to be filled in on the screens where user information is submitted to the database.
Possible Values	True or False
Value Definition	True for field must be filled in, False for not required

THE FOLLOWING 9 FIELDS ARE USED FOR COLLECTING ADDITIONAL USER DATA

user_info.customX.required=

Modifiable Field	**user_info.customX.required**
Field Description	Additional User information - X=1 to 9
Possible Values	True or False
Value Definition	True for required False for not required

users.display.left.x=

Modifiable Field	**users.display.left.X**
Field Description	Display on the registration screen left hand side. x = 0 to n
Possible Values	User Defined for example, users.surname
Value Definition	

users.display.right.x=

Modifiable Field	**users.display.right.X**
Field Description	Display on the registration screen right hand side. x =0 to n
Possible Values	User Defined for example, users.surname
Value Definition	

limit.recently.accessed=

Modifiable Field	**limit.recently.accessed**
Field Description	Max. number of recently accessed targets to display when the recently accessed action is performed
Possible Values	User Defined integer
Value Definition	User defined

sql.messages.maxlen=

Modifiable Field	**sql.messages.maxlen**
Field Description	The maximum number of characters that should be displayed in report-related messages before truncating
Possible Values	Any number >= 1
Value Definition	The number of characters, defined in the value, is displayed in the message followed by '....'

DO NOT EDIT THE FOLLOWING LINES

```
export.data.directory
file.upload.directory
trc.ticket.expiry
eg2.file.directory
```

ldap.properties

This section describes the architecture of the **ldap.properties file**.

This is only used if COMMON.PROPERTIES authentication LDAPconfig is 1

ldap.connectionName =

Modifiable Field	**ldap.connectionName**
Field Description	The username used to authenticate to a read-only LDAP connection. If left blank, an anonymous connection is attempted
Possible Values	User defined for example, administrator@example.com
Value Definition	User defined

ldap.connectionPassword =

Modifiable Field	**ldap.connectionPassword**
Field Description	The password used to establish a read-only LDAP connection. The password can be entered here in plain text or it can be encrypted.
Possible Values	User defined
Value Definition	User defined

ldap.connectionURL =

Modifiable Field	**ldap.connectionURL**
Field Description	URL of the LDAP server
Possible Values	User defined for example:**ldap://ldap.server.com**
Value Definition	

ldap.security_authentication=

Modifiable Field	**ldap.security_authentication**

Field Description	Specifies the security level to use. If this property is unspecified, the behavior is determined by the service provider.
Possible Values	none, simple, strong
Value Definition	String

`ldap.groupName=`

Modifiable Field	**ldap.groupName**
Field Description	LDAP group name
Possible Values	User Defined for example:ldapGroup
Value Definition	

`ldap.groupNameTrim=`

Modifiable Field	**ldap.groupNameTrim**
Field Description	Specifies whether the group name must be trimmed .
Possible Values	True or False
Value Definition	

`ldap.groupDescription=`

Modifiable Field	**ldap.groupDescription**
Field Description	Field for group description
Possible Values	User defined for example : description
Value Definition	

`ldap.groupMembers=`

Modifiable Field	**ldap.groupMembers**
Field Description	Specifies user membership within a group
Possible Values	User Defined
Value Definition	

`ldap.groupBase=`

Modifiable Field	**ldap.groupBase**
Field Description	Defines the starting location for the search of the LDAP groups. The Distinguished Name (DN) specified will indicate the location in the directory structure in which all groups are contained.
Possible Values	User Defined ldap.groupBase=OU=Groups,OU=MyLocation, DC=MyCompany,DC=com
Value Definition	

`ldap.groupSearch=`

Modifiable Field	**ldap.groupSearch**

Field Description	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 that are needed are imported to IBM Endpoint Manager for Remote Control.
Possible Values	User Defined for example : ldap.groupSearch=(objectClass=group) = Imports all AD groups to IBM Endpoint Manager for Remote Control. Be aware some environment can have thousands of groups.
Value Definition	

`ldap.groupSubtree=`

Modifiable Field	**`ldap.groupSubtree`**
Field Description	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 (a nonrecursive search).
Possible Values	True or False
Value Definition	

`ldap.userPassword =`

Modifiable Field	**`ldap.userPassword`**
Field Description	Password field
Possible Values	User Defined
Value Definition	

`ldap.userEmail=`

Modifiable Field	**`ldap.userEmail`**
Field Description	LDAP field for Email
Possible Values	User Defined for example: userPrincipalName
Value Definition	

`ldap.userid=`

Modifiable Field	**`ldap.userid`**
Field Description	LDAP field for userid
Possible Values	User Defined
Value Definition	

If the following parameters are defined they is mapped into the local database

`ldap.forename=`

Modifiable Field	**`ldap.forename`**
Field Description	LDAP field for forename

Possible Values	User Defined
Value Definition	User defined string

`ldap.surname=`

Modifiable Field	**ldap.surname**
Field Description	LDAP field for surname
Possible Values	User defined
Value Definition	User defined string

`ldap.title=`

Modifiable Field	**ldap.title**
Field Description	LDAP field for title
Possible Values	User Defined
Value Definition	User defined string

`ldap.initials=`

Modifiable Field	**ldap.initials**
Field Description	LDAP field for initials
Possible Values	User Defined
Value Definition	User defined string

`ldap.company=`

Modifiable Field	**ldap.company**
Field Description	LDAP field for company
Possible Values	User Defined
Value Definition	User defined string

`ldap.department=`

Modifiable Field	**ldap.department**
Field Description	LDAP field for department
Possible Values	User Defined
Value Definition	User Defined string

`ldap.telephone=`

Modifiable Field	**ldap.telephone**
Field Description	LDAP field for telephone
Possible Values	User defined
Value Definition	User defined string

`ldap.mobile=`

Modifiable Field	**ldap.mobile**
Field Description	LDAP field for userid

Possible Values	User defined
Value Definition	User defined

`ldap.state=`

Modifiable Field	**`ldap.state`**
Field Description	LDAP field for state
Possible Values	User defined
Value Definition	User defined string

`ldap.country=`

Modifiable Field	**`ldap.country`**
Field Description	LDAP field for country
Possible Values	User defined
Value Definition	User defined string

`ldap.userBase=`

Modifiable Field	**`ldap.userBase`**
Field Description	the base of the sub tree containing users. If not specified, the search base is the top-level context.

Possible Values	User Defined
	`for example`
	`ldap.userBase=OU=Users,OU=MyLocation,DC=MyCompany,DC=com`

Value Definition	

`ldap.userSearch=`

Modifiable Field	**`ldap.userSearch`**
Field Description	Pattern to use for searches
Possible Values	for example (userPrincipalName={0}@ActDirTest.SDC.COM)
Value Definition	All users who match the search criteria are imported into the IBM Endpoint Manager for Remote Control database. To limit this further you can use the **`ldap.userInGroup`** parameter.

`ldap.userSubtree =`

Modifiable Field	**`ldap.userSubtree`**
Field Description	Search up the subtree
Possible Values	True or False
Value Definition	True for search the subtree, False do not search

`ldap.userInGroup =`

Modifiable Field	**`ldap.userInGroup`**
Field Description	Determines whether a user who matches the user search criteria also has to be a member of the groups found in the group search.

Possible Values	True or False
Value Definition	**True** only users who match the user search criteria and are members of the groups found in the group search are imported. **False** all users who match the user search criteria regardless of their group membership are imported. **Note:** Users are imported into the DefaultGroup as well as any other groups that they belong to.

log4j.properties

This section describes the architecture of the `Log4j.properties` file. This file is used in the setup and configuration of logging output and messages from the application.

For more information, see the following two areas:

- ***http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html***
- ***http://logging.apache.org/log4j/1.2/manual.html***

`log4j.rootLogger =`

Modifiable Field	**`log4j.rootLogger`**
Field Description	Defines the level of the logger and where it outputs the logging requests to, that is it's appenders.
Possible Values	User defined for example - WARN, A1, Rolling Logger has a level of WARN and two appenders A1 and Rolling.
Value Definition	There are various levels of logger FATAL, ERROR, WARN, INFO, DEBUG, TRACE, ALL For more details, see ***http://logging.apache.org/log4j/1.2/manual.html***

`log4j.logger.com.ibm =`

Modifiable Field	**`log4j.logger.com.ibm`**
Field Description	Defines the level of logging information to be output.
Possible Values	• TRACE • DEBUG • INFO • WARN • ERROR • FATAL • OFF

Value Definition	The above values are displayed in order of how much information is logged. Whichever value is set, information for this level and above is logged. For example setting the value to DEBUG means that information from debug messages to fatal messages is logged. For a value of WARN, means that warning information to fatal information is logged. **Note:** After changing the value for this property and clicking Submit to save the file, you should restart the IBM Endpoint Manager for Remote Control Server service.

`log4j.appender.A1 =`

Modifiable Field	**log4j.appender.A1**
Field Description	Defines the output destination that appender A1 will send the formatted messages to .
Possible Values	User defined, for example org.apache.log4j.ConsoleAppender sends the messages to the console
Value Definition	

`log4j.appender.A1.layout =`

Modifiable Field	**log4j.appender.A1.layout**
Field Description	Used to specify the output format of the log messages
Possible Values	User defined for example - org.apache.log4j.PatternLayout
Value Definition	

`log4j.appender.A1.encoding =`

Modifiable Field	**log4j.appender.A1.encoding**
Field Description	Encoding type to be used for the message output
Possible Values	User defined - for example UTF8
Value Definition	

`log4j.appender.A1.layout.ConversionPattern =`

Modifiable Field	**log4j.appender.A1.layout.ConversionPattern**
Field Description	Defines the pattern to be used for formatting the output of the log messages
Possible Values	User defined
Value Definition	See ***http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html***

`log4j.appender.Rolling =`

Modifiable Field	**log4j.appender.Rolling**
Field Description	Defines the output destination that appender Rolling will send the formatted messages to .

Possible Values	User defined, for example **org.apache.log4j.RollingFileAppender** sends the messages to a file
Value Definition	

`log4j.appender.Rolling.File =`

Modifiable Field	**log4j.appender.Rolling.File**
Field Description	The name of the file that the messages are logged to.
Possible Values	User defined - for example `trc.log`
Value Definition	

`log4j.appender.Rolling.encoding =`

Modifiable Field	**log4j.appender.Rolling.encoding**
Field Description	Encoding type to be used for the message output
Possible Values	User defined
Value Definition	

`log4j.appender.Rolling.MaxFileSize =`

Modifiable Field	**log4j.appender.Rolling.MaxFileSize**
Field Description	Maximum size for the log file
Possible Values	User defined - for example 2MB
Value Definition	

`log4j.appender.Rolling.MaxBackupIndex =`

Modifiable Field	**log4j.appender.Rolling.MaxBackupIndex**
Field Description	Defines the number of back up log files to keep
Possible Values	User defined - for example 4
Value Definition	integer

`log4j.appender.Rolling.layout =`

Modifiable Field	**log4j.appender.Rolling.layout**
Field Description	Used to specify the output format of the log messages
Possible Values	User defined, for example: org.apache.log4j.PatternLayout
Value Definition	

`log4j.appender.Rolling.layout.ConversionPattern =`

Modifiable Field	**log4j.appender.Rolling.layout.ConversionPattern**
Field Description	Defines the pattern to be used for formatting the output of the log messages
Possible Values	User defined
Value Definition	See ***http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html***

appversion.properties

This section describes the architecture of the `appversion.properties file`. which is used to define the version and date of the application

DO NOT EDIT THE FOLLOWING LINES

```
version.date =
version.number =
```

controller.properties

Edit the `controller.properties` file to create and configure properties for the IBM Endpoint Manager for Remote Control controller component to use during a remote control session with a target.

This section describes the architecture of the `controller.properties` file. This file is used in the configuration of the controller component that is used during remote control sessions that are initiated from the server. For details of configuring controller properties for peer to peer remote control sessions see the IBM Endpoint Manager for Remote Control Controller User's Guide

Running tools on the target during a remote control session

Configuration settings to add custom menu items on the controller to launch commands on the target machine during a remote control session. These menu items are added to the **Perform Action in Target** menu.

Note: If too many items are added to the **Perform Action in Target** menu the last items in the menu might extend beyond the bottom of the screen, particularly on smaller screen size, since there is no support for scrolling menus.
There are seven pre configured tools by default that you can change to your own requirements. There are also three blank tools available by default. To add more tools, manually edit the `controller.propreties` file.

Note: After manually editing the file, restart the server service for the new tools to be displayed on the screen.

The tools properties should be configured using the following definition formats.

```
prefix.ToolName =
```

Modifiable Field	**prefix.ToolName**
Field Description	Display name used in the **Perform Action in target** menu. Each defined tool name should have a different prefix.
Possible Values	User Defined. For example, `tool01.ToolName=Command Prompt` The text, Command Prompt, is displayed in the **Perform Action in target** menu.
Value Definition	

```
prefix.ToolName.$lang$=
```

Modifiable Field	**prefix.ToolName.$lang$**

Field Description	Display name used in the **Perform Action in target** menu. Translation of display name. $lang$ is ISO language code.
Possible Values	User Defined.
Value Definition	

`prefix.ToolCommand=`

Modifiable Field	**prefix.ToolCommand**
Field Description	Command to execute the tool, without parameters.
Possible Values	User Defined. For example, tool01.ToolCommand=[SystemFolder]\\control.exe The tool command can be a fully qualified path or just the filename. The file needs to be on the PATH environment variable of the logged in user. You can specify executable files but also files associated with an executable. Do not use quotes, even when there are spaces in the path or filename. For example, **tool01.ToolCommand=cmd.exe** and **tool01.ToolCommand=[SystemFolder]\\cmd.exe** are equivalent. **Note:** When using a backslash in the path you need to enter two backslashes. You can use the following folder properties when defining windows tools parameters. The target substitutes these with the actual path on the target system. **[WindowsFolder]** The target uses the following path to execute the tool. `[WindowsVolume]\Windows` **[SystemFolder]** The target uses the following path to execute the tool. `[WindowsFolder]\System32` Folder properties are not relevant for Linux targets. `lnxcontrol.ToolCommand = /usr/bin/gnome-control-center`
Value Definition	

`prefix.ToolParameters =`

Modifiable Field	**prefix.ToolParameters**
Field Description	Optional parameters for the command to execute.
Possible Values	User defined
Value Definition	

`prefix.ToolUser =`

Modifiable Field	**prefix.ToolUser**
Field Description	Determines which privileges or credentials the command is executed with.
Possible Values	<blank> or admin

Value Definition	**<blank>** Run the tool as the logged on user. **Note:** Might trigger UAC prompts depending on the version of Windows. This is the default value. **admin** Run the tool with UAC prompt to elevate privileges.

Pre configured tools

The following list of tools are pre configured and can be edited using the **Edit properties files** option.

Note: Although the tools are pre configured, each specific tool will only be displayed in the **Perform action in target** menu if the target has the command required for running the tool already installed. Therefore some sessions might have all tools displayed and other sessions might only have a few pre configured tools displayed. Only windows tools will be displayed when you are connected to a Windows target and Linux tools on a Linux target.

```
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 =
```

Sending key sequences to the target during a session

Configuration settings to add custom key sequence shortcuts to the controller to inject on the target machine during a remote control session. For details of the supported key codes see the IBM Endpoint Manager for Remote Control Controller User's Guide

`keyX.KeySequenceName=`

Modifiable Field	**keyX.KeySequenceName**
Field Description	Display name used in the **Perform Action in target** menu. Each defined key sequence name should have a different prefix. For more details see the IBM Endpoint Manager for Remote Control Controller User's Guide. X = 01 to n
Possible Values	User Defined. For example, `key01.KeySequenceName = Inject F1` The text, **Inject F1**, is displayed in the **Perform Action in target** menu.
Value Definition	

`keyX.KeySequenceName.language=`

Modifiable Field	**keyX.KeySequenceName.language**
Field Description	Translations for display name. This property is optional. X = 1 to n
Possible Values	User Defined. For example, `key01.KeySequenceName.es = Inyectar F1`
Value Definition	

`keyX.KeySequenceValue=`

Modifiable Field	**keyX.KeySequenceValue**
Field Description	Macro sequence. The sequence of keys defined here are sent to the target machine. X = 1 to n
Possible Values	User Defined. For example, `key01.KeySequenceValue = [F1]`
Value Definition	

Chapter 22. Reducing the volume of target connections to the server

To reduce the load on the server you can reduce the number of heartbeats being sent to the server from a target by using properties in the **trc.properties** file. Use these properties to reduce the volume of unnecessary heartbeats coming from a target, to prevent multiple heartbeats in quick succession, by delaying the actual heartbeat when a heartbeat is triggered, and during the delay merging these into a single heartbeat.

An exception is made for important or urgent heartbeats, for example:

- Reporting a new IP address
- Reporting the start or end of a remote control session
- Reporting status to the server requested by the user
- Reboot requested by the controller
- Target going offline

You can control the delay by using the **HeartBeatDelay** property.

Table 9. HeartBeatDelay property

Name	Value	Default Value
HeartBeatDelay	Maximum delay in minutes	20

A random factor is also applied to the delay to distribute the heartbeat volume more evenly over time. The target chooses a random delay starting from a quarter of the maximum delay time. With the default setting, the random delay ranges from 5 minutes to 20 minutes.

Note: By default, the very first contact the target makes with the server, after the installation is not delayed so that the target can be registered in the server immediately.

If you are carrying out a mass deployment of targets this might cause the server to be overloaded with registrations. To alleviate this you can use the **RegistrationDelay** target property to randomly delay the registration and distribute it evenly through the deployment to avoid too many machines trying to register at the one time.

Table 10. HeartBeatDelay and RegistrationDelay properties

Name	Value	Default Value
HeartBeatDelay	Maximum delay in minutes	20
RegistrationDelay	Maximum delay in minutes	0

You can use the following properties to prevent a heartbeat from being triggered for certain events.

Table 11. Heartbeat properties to control heartbeats for certain events

Name	Value	Default value	Description
HeartBeatOnWake	Yes/No	Yes	Trigger a heartbeat when the system wakes from standby or hibernation
HeartBeatOnUserChange	Yes/No	Yes	Trigger a heartbeat when a user logs on or off
HeartBeatOnChange	Yes/No	Yes	Trigger a heartbeat when any of the values included in a heartbeat have changed
HeartBeatOnStop	Yes/No	No	Trigger a heartbeat when the target is stopped or the system is shutting down

Chapter 23. Broker configuration

When you install broker support you can use the installed `trc_broker.properties` file to configure your environment for using the broker function.

When the broker support is installed, a configuration file, **trc_broker.properties**, is created which provides examples of the configuration parameters you can use to create a broker configuration to satisfy your network requirements.

In the configuration file you can define default broker setup parameters and also any connections required for your environment.

- The broker supports multiple instances of each connection type
- The configuration directives for each connection have a user defined prefix.

Configuring the broker properties

You can edit the `trc_broker.properties` file to configure the parameters and connection types required for using brokers in your environment.

To configure the broker to your requirements, edit the `trc_broker.properties` file.

On a windows machine this file is located in the `\Broker` directory within the brokers's working directory.

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

When using Windows 2008 server the file is located in \ProgramData\IBM\Tivoli\ Remote Control\Broker\. In Linux the file is located in the `/etc` directory.

Note: Any errors in the configuration file do not stop the broker from starting. Examine the broker log to verify that the broker is running as expected. For more details about configuring logging parameters, see "Logging broker activity" on page 232.

Setting server connection parameters

Edit the `trc_broker.properties` file to set the parameters for the server that the broker authenticates with.

At the start of a broker remote control session, the broker connects to the server to authenticate the session. Use the following parameters to define the server.

ServerURL

Determines the URL of the server that the broker authenticates the session with. This parameter must be set to the base URL, for example `https://trcserver.example.com/trc`. A trailing '/' character is allowed. This parameter is a required parameter.

Note: The broker requires a connection to the remote control server to authenticate sessions and connection codes. As the broker is typically located outside of the intranet while the server is inside of it, this connection requires a proxy server or a chain of gateways. Use HTTPS and

not HTTP if the connection from the broker to the server passes through an unsecure or untrusted network. Also, use HTTPS if the following properties are enabled in the `trc.properties` file, **`enforce.secure.endpoint.callhome`**, or **`enforce.secure.endpoint.upload`**. Otherwise, the target cannot send audit information or status updates to the server. For more information about the **`enforce.secure`** properties, see "trc.properties" on page 172.

ProxyURL
Add the URL of a proxy server or gateway if you are using one. This parameter is optional.

Configuring the broker certificate

Use the following parameters to define the location of the certificate, and password for the broker.

DefaultTLSCertificateFile
Filename or path to the TLS certificate for this broker. For more details on creating and managing broker certificates, see Chapter 25, "Certificate management," on page 245. Default is `server.pem`.

DefaultTLSCertificatePassphrase
Password for the private key associated with the TLS certificate This parameter is optional.

Allowing endpoints to connect to a broker

To allow the broker to accept connections from controllers and targets you can define and configure inbound connections using the `trc_broker.properties` file.

You can configure multiple inbound connections and define a prefix for each connection parameter to allow the broker to find all required settings for each connection. Configure any inbound connections when configuring the `trc_broker.properties` file. For more details about editing this file, see "Configuring the broker properties" on page 229.

Note:

1. Do not prefix with # or ! as these are reserved for comments in properties files.
2. If you want to include spaces in the prefix you have to escape them with `\` for example : `my connection.ConnectionType should be defined as my\connection.ConnectionType`

To configure inbound connections complete the following steps:

1. Configure the following parameters within the `trc_broker.properties` file

   ConnectionType
   Defines the type of connection. Should be set to `Inbound` or `Inbound6` when you are using IPv6 networks. `For example: my\ connection.ConnectionType=Inbound`

   PortToListen
   Defines the TCP port that endpoints should use to connect to this broker. The port for listening for inbound connections. Required parameter.

AllowEndpoints

Determines whether endpoints can connect to this broker.

Yes Endpoint connections can be made to this broker. This is the default value.

No Endpoint connections cannot be made to this broker.

AllowBrokers

Determines whether other brokers can connect to this broker. Set to `No` or `<blank>` means other brokers cannot connect to this broker. If other brokers can connect to this broker, provide a list of brokers that are allowed to connect. For example `broker1.ibm.com,broker2.ibm.com,broker3.ibm.com`.

Note: The hostnames listed here must match the certificate and the hostnames used when registering the brokers in the remote control server.

2. Save the file.

If you are configuring multiple brokers in your environment which will connect to each other to complete the connection between the controller and target, you should configure broker connections in the broker properties file. For more details, see "Support for multiple brokers." When you have finished creating a broker configuration you can register the brokers in the IBM Endpoint Manager for Remote Control Server database to be used for facilitating remote control connections across the internet. For more details, see "Registering a broker on the server" on page 243.

Support for multiple brokers

To allow the broker to accept connections from other brokers you can define and configure broker connections using the `trc_broker.properties` file.

When you have multiple brokers defined in your environment you should configure broker control connections and define a prefix for each connection parameter to allow the broker to find all required settings for each connection. Broker connections need to be configured between the brokers that will connect to each other. The brokers use the network of control connections to determine which broker has the connection from the target. When the target is located, the controller is reconnected to the same broker as the target. Configure any broker connections when configuring the `trc_broker.properties` file.

Note:

1. Do not prefix with # or ! as these are reserved for comments in properties files.
2. If you want to include spaces in the prefix you have to escape them with `\` `for example : my connection.ConnectionType should be defined as my\connection.ConnectionType`

To configure broker connections complete the following steps.

1. Configure the following parameters within the `trc_broker.properties` file of the broker that will connect to connect to another broker.

   ConnectionType

   Defines the type of connection. Should be set to `Broker For example: my\connection.ConnectionType=Broker`

DestinationAddress
Defines the hostname of the broker that the connection is being made to. The broker with this address needs to be configured to accept inbound connections. This parameter is required. `For example: my\connection.DestinationAddress=mybroker.ibm.com`

Note: Set the **`AllowBrokers`** parameter in the configuration file of the broker that this connection is being made to. Set this parameters to allow other brokers to connect to it. For more details, see "Allowing endpoints to connect to a broker" on page 230.

DestinationPort
Defines the TCP port of the broker to connect to. This parameter is required.

PublicBrokerURL
Determines the public address and port for the broker you are currently configuring. When there are multiple brokers configured, if the target connects to this broker and the controller connects to a different broker, the property is used to identify this broker so that the controller can connect to it and then successfully reach the target. This property should be set to *hostname:port* where *hostname* is the hostname of this broker machine and *port* is the port that this broker is listening for connections on. Default value is <blank.> .

Note: The hostname used here should be the same as the hostname used when registering the broker on the IBM Endpoint Manager for Remote Control server.

2. Save the file.

When you have created a broker configuration you can register the brokers in the IBM Endpoint Manager for Remote Control database to be used for facilitating remote control connections across the internet. For more details, see "Registering a broker on the server" on page 243.

Logging broker activity

Broker session activity is saved to the broker log files. These files are named using the following format.

TRCICB-*computername-suffix*.log

where *computername* is the computer name of the broker and *suffix* is determined by the LogRotation and LogRollover settings.

For example, `TRCICB-RCBROKER.example.com-Tue.log`

The broker log files are located in the `\Broker` directory within the brokers's working directory.

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

When using Windows 2008 server the file is located in \ProgramData\IBM\Tivoli\Remote Control\Broker\. In Linux the file is located in the `/var/opt/ibm/trc/broker` directory. Use the following properties to configure the logging level and how often the broker log file is renewed.

Logging level

Set the required logging level. The logging level determines the types of entries and how much information is added to the broker log file. Default value is 2.

Logging level	Description
0	no logging
1	error
2	info
4	debug information

LogRotation

Controls the period after which an older log file will be overwritten. Log rotation can be disabled. Default value is Weekly.

LogRotation	Description	Suffix for hourly rollover	Suffix for daily rollover
Daily	Overwrite log files after one day	00H to 23H	Not valid
Weekly	Overwrite log files after one week.	Mon-00H to Sun-23H	Mon - Sun
Monthly	Overwrite log files after one month.	01-00H to 31-23H	01 to 31
Disabled	LogRotation is disabled	YYYY-MM-DD-hh	YYYY-MM-DD

LogRollOver

Controls the period after which a new log file is started. This period has to be smaller than the LogRotation period, therefore not all combinations are valid. LogRollover cannot be disabled. Default value is Daily.

LogRollover	Description	Comments
Hourly	Start a new log file on the hour.	Recommended for busy brokers or when using log levels higher than 2.
Daily	Start a new log file every day.	Default setting.

Configuring optional parameters

The following optional parameters can be used to further configure your broker.

Global parameters

FIPSCompliance

Determines whether a FIPS certified cryptographic provider is used for all cryptographic functions. Default value is No.

SP800131ACompliance
Determines whether NIST SP800-131A compliant algorithms and key strengths are used for all cryptographic functions. Default value is No.

Request Pool
An area of memory that is known as the Request Pool is used to track requests. The connection requests from other brokers are kept in the pool until the pool is full and the oldest requests are recycled. The following parameters can be used to configure the request pool:

Request Pool.size
The amount of memory, in kilobytes, to reserve for the request pool. The default is 2048 or 2 megabytes.

Request Pool.MinimumTTL
The minimum time, in minutes, before a request can be recycled. The default is 5 minutes.

RecordingDir
Use RecordingDir to define the directory that the session recording is temporarily stored on the broker if **Force Session Recording** is set to Yes.

For example, `RecordingDir=c:\\tmp`. When you are using a backslash in the path, you must enter two backslashes.

You can also specify relative directories. For example, `RecordingDir=tmp`. The recording is temporarily stored in the tmp directory within the working directory of the broker.

If you do not add `RecordingDir` to the properties file, the recording is temporarily stored in the working directory of the broker.

Parameters for inbound connections

BindTo
Used to accept incoming connections on specific network interfaces.

For example:`my\connection.BindTo=192.0.2.0` Default is 0.0.0.0.

RetryDelay
Defines the time in seconds between attempts to open the configured port for listening for incoming connections. Default is 45 seconds.

TLSCipherList
List of allowed ciphers. For more information about allowed ciphers, see "Default configuration parameters" on page 235.

Parameters for broker connections

BindTo
This parameter is optional and can be configured to allow the broker to establish the outgoing broker connection from a specific network interface. For example, if a firewall on the network is configured to allow only 1 of the broker 's interfaces through. Defines the IP address of the network interface through which the connections are made. For example: broker.1.BindTo=192.0.2.0 Default is 0.0.0.0.

KeepAlive
Defines the time in seconds between keepalive requests. This parameter is optional. Default is 45 seconds.

RetryDelay
Defines the time in seconds between attempts to establish or re-establish the control connection. This parameter is optional. Default is 45 seconds.

SourcePort
Defines the port that the outgoing broker connection is using. By default the broker uses an unused port.

TLSCipherList
List of allowed ciphers. For more information about allowed ciphers, see "Default configuration parameters."

Default configuration parameters

Default parameters

Use the set of default parameters, prefixed with Default to set your configuration, and also configure multiple connections. The parameters have a set of default values that you can be change. The values can be applied to the parameters prefixed with Default and also to the connection parameters.

Table 12. Default parameter values

Keyword	Default Value	Required
ServerURL	<blank>	Yes
ProxyURL	<blank>	No
DefaultPortToListen	<blank>	Yes
DefaultBindTo	0.0.0.0	No
DefaultBindTo6	::	No
DefaultRetryDelay	45	No
DefaultKeepAlive	900	No
DefaultTLSCertificate	server.pem	No
DefaultTLSCertificatePassphrase	<blank>	No
DefaultTLSCipherList	TLSv1+HIGH:!SSLv2:!aNULL:!eNULL :!3DES:@STRENGTH	No
DefaultHTTPSCipherList	TLSv1:!SSLv2:!aNULL:!eNULL :!3DES:@STRENGTH	No

The default values can be used to set values for all connections. However, values that are set for specific connections override the default value for that connection.

Example 1: Using a default value

```
DefaultKeepAlive = 300

Inbound.1.ConnectionType = Inbound
Inbound.1.PortToListen = 8887

Broker.1.ConnectionType = Broker
Broker.1.DestinationAddress = broker1.example.com
Broker.1.DestinationPort = 8887
```

Broker.2.ConenctionType = Broker
Broker.2.DestinationAddress = broker2.example.com
Broker.2.DestinationPort = 8887
Broker.2.KeepAlive = 100

In this example, the **DefaultKeepAlive** value of 300 is used for the **Inbound.1** connection and the **Broker.1** connection. Setting the default parameter means that you do not need to add the property to each specific connection. However, the **Broker.2** connection uses the KeepAlive value of 100 since the **Broker.2.KeepAlive** property is set. The specific connection value overrides the default value.

Example 2: Using specific values

Inbound.1.ConnectionType = Inbound
Inbound.1.PortToListen = 8887
Inbound.1.KeepAlive = 300

Broker.1.ConnectionType = Broker
Broker.1.DestinationAddress = broker1.example.com
Broker1.DestinationPort = 8887
Broker.1.KeepAlive = 300

In this example, no **DefaultKeepAlive** value is set. A KeepAlive property value is set for each specific connection.

Required default parameters

Required parameters do not have a built-in default value. These parameters must be set either to the value given in the file or within the connection configurations. When a required parameter is set in the connection parameters, this value overrides any default values set for the same parameter.

Table 13. Required parameters values used

Default parameter set	Connection parameter set	Value Used
No	No	Not defined, a required parameter must be defined in the configuration.
No	Yes	Connection parameter is used
Yes	No	Default parameter is used.
Yes	Yes	Connection parameter is used.

Optional default parameters

Optional parameters have a built-in default value. If the parameter is not set within the default parameters or within the connection parameters, the built-in default value is used. If the parameter is set within the default parameters, but is not set within the connection parameters, the default parameter value is used by any connections.

Table 14. Optional parameters

Default parameter set	Connection parameter set	Value used
No	No	Built in default value is used
No	Yes	Connection parameter is used
Yes	No	Default parameter is used
Yes	Yes	Connection parameter is used

Parameter definitions

DefaultPortToListen
Defines the TCP port that endpoints must use to connect to this broker. The port for listening for inbound connections. Required parameter.

DefaultSourcePort
Defines the port that the outgoing connection is using. This parameter is optional. Default is 0.

DefaultBindTo
This parameter is optional. Defines the IP address that is used to create connections with.

For example: `my\connection.BindTo=192.0.2.0` Default is `0.0.0.0`. Optional parameter.

DefaultBindTo6
This parameter is optional. Defines the IP address that is used to create connections with in IPv6 networks. Default is `::`. Optional parameter.

DefaultRetryDelay

inbound connections
Defines the time in seconds between attempts to open the configured port for listening for incoming connections. Default is 45 seconds.

broker connections
Defines the time in seconds between attempts to establish or re-establish the control connection. This parameter is optional. Default is 45 seconds.

DefaultKeepAlive
Defines the time in seconds between keepalive requests. This parameter is optional. Default is `900` seconds.

DefaultTLSCertificateFile
Filename or path to the TLS certificate for this broker. For more information on creating and managing broker certificates, see Chapter 25, “Certificate management,” on page 245. Default is `server.pem`.

DefaultTLSCertificatePassphrase
Password for the private key that is associated with the TLS certificate This parameter is optional.

DefaultTLSCipherList and DefaultHTTPSCipherList
Use this configuration keyword to override the selection of cipher suites that can be used to secure network connections to or from a broker. A cipher suite is a combination of four cryptographic algorithms that are

used together to create a secure communication channel. These algorithms are provided by a cryptographic module included with the broker. This module also includes algorithms for compatibility with an earlier versions, even if they are now considered to offer little or no security. By default, the broker selects only cipher suites that offer strong security. The default selection can be overridden if necessary. This is normally not needed, but can be used, for example, to disable an algorithm against which a new cryptographic attack is discovered. The documentation for the syntax of the cipher list can be found on the OpenSSL website. http://www.openssl.org/docs/apps/ciphers.html#CIPHER_LIST_FORMAT

Default Cipher List

TLSv1+HIGH
Only ciphers from the TLSv1 cipher suite with key lengths larger than 128 bits and some cipher suites with 128-bit keys.

TLSv1 Only ciphers from the TLSv1 cipher suite.

!SSLv2
Permanently remove all ciphers from the SSLv2 cipher suite.

!aNULL
Permanently remove all ciphers without authentication.

!eNULL
Permanently remove all ciphers without encryption.

!3DES Permanently remove all ciphers that use the triple DES encryption algorithm.

@STRENGTH
Order the cipher list in order of encryption algorithm key length.

Note: The broker supports only TLSv1. Support for SSLv2 and SSLv3 is disabled due to known vulnerabilities in those versions of the protocol, even if you include SSLv2 or SSLv3 in the cipher list.

Types of cryptographic algorithms

Authentication
Verify the identity of the client or server that is using digital certificates.

Key Exchange
Establish shared secrets to be used as encryption keys and message authentication keys for the session.

Encryption
Protects the session data from being accessed by unauthorized entities.

Message authentication
Protects the session data from being tampered with.

With the version of OpenSSL that is included with the broker component and the default cipher list, the following ciphers can be used:

Encryption

- AES key length 256 bits
- AES key length 128 bits

Authentication

- RSA
- DSA

Key Exchange

- RSA
- Diffie-Hellman

Message Authentication

SHA-1

Broker setup examples

The following example illustrates a broker and gateway setup.

There are 3 networks present, an intranet, a DMZ network and an internet facing network. A firewall between the Intranet and the Internet allows outbound connectivity but blocks all inbound connections. There is also a security policy in force that does not allow connections to be initiated from the DMZ to the intranet or from the Internet Facing network to the DMZ.

Hosts in the Internet Facing network do not have public IP addresses. The internet gateway uses DNAT to map internal IP addresses to public IP addresses, only for the ports needed for specific public services. In this example, the public service is the broker.

The broker requires connectivity to the server, but direct connections from the Internet Facing network to the server are not allowed. A chain of gateways is deployed to allow the broker to connect to the server.

The following tables provide details of the components and settings present in the example environment.

Table 15. TRC components

Network name	Server	Broker	Gateway	Controller	Target
Intranet	Yes	No	Yes	Yes	Yes
DMZ	No	No	Yes	No	No
Internet facing	No	Yes	Yes	No	No
Internet	No	No	No	No	Yes

Table 16. Networks

Network name	Subnet Address	Subnet Mask
Intranet	10.1.0.0	255.255.255.0
DMZ	10.2.0.0	255.255.255.0
Internet Facing	10.3.0.0	255.255.255.0

Table 17. Machines

Host name	IP address	Roles
SERVER.example.com	10.1.0.2	TRC server on port 443
BROKER1.example.com	10.3.0.10	TRC broker on port 8887
BROKER2.example.com	10.3.0.11	TRC broker on port 8887

Table 17. Machines (continued)

Host name	IP address	Roles
GATEWAY1.example.com	10.1.0.254	TRC gateway
GATEWAY2.example.com	10.2.0.254	TRC gateway on port 8881
GATEWAY3.example.com	10.3.0.254	TRC gateway on port 8881, inbound tunnel on port 8880
CONTROLLER1.example.com	Dynamic IP in 10.1.0.0/24	TRC controller
TARGET1.example.com	Dynamic IP in different networks	TRC target on mobile system

Table 18. Firewall

Source	Destination	Port	Description
10.1.0.254/ 255.255.255.255	10.2.0.254/ 255.255.255.0	8881	Allow GATEWAY1 to connect to GATEWAY2
10.2.0.254/ 255.255.255.255	10.3.0.254/ 255.255.255.0	8881	Allow GATEWAY2 to connect to GATEWAY3

Table 19. DNAT

Public DNS Name	Public IP	Private IP	Port
BROKER1.example.com	203.0.113.23	10.3.0.10	8887
BROKER2.example.com	203.0.113.24	10.3.0.11	8887

Broker Configuration

Each broker is configured with

- Inbound connection for endpoints to connect
- Connection to the server via a gateway

Broker 1 is configured with an additional inbound connection for control connections from broker 2. Broker 2 is configured with a control connection to broker 1.

The following section provides examples of what would be set in the broker and gateway properties files for each of the relevant components.

BROKER1.example.com

PublicBrokerURL = BROKER1.example.com:8887

ServerURL = https://SERVER.example.com/trc/

ProxyURL = trcgw://GATEWAY3.example.com:8880

DefaultTLSCertificateFile = BROKER1.p12

DefaultTLSCertificatePassphrase = **********

Inbound1.ConnectionType = Inbound

Inbound1.PortToListen = 8887

Broker2.ConnectionType = Broker

Broker2.DestinationAddress = BROKER2.example.com

Broker2.DestinationPort = 8881

BROKER2.example.com

PublicBrokerURL = BROKER2.example.com:8887

ServerURL = https://SERVER.example.com/trc/

ProxyURL = trcgw://GATEWAY3.example.com:8880

DefaultTLSCertificateFile = BROKER2.p12

DefaultTLSCertificatePassphrase = **********

Inbound1.ConnectionType = Inbound

Inbound1.PortToListen = 8887

Inbound2.ConnectionType = Inbound

Inbound2.PortToListen = 8881

Inbound2.AllowEndpoints = no

Inbound2.AllowBrokers = BROKER1.example.com

Gateway Configuration

GATEWAY1

Gateway 1 is configured with a control connection to gateway 2 and an outbound tunnel connection to the server.

Gateway2.ConnectionType = Gateway

Gateway2.DestinationAddress = 10.2.0.254

Gateway2.DestinationPort = 8881

Server.ConnectionType = OutboundTunnel

Server.DestinationAddress = 10.1.0.2

Server.DestinationPort = 443

GATEWAY2

Gateway 2 is configured with an inbound connection and a control connection to gateway 3.

Inbound.ConnectionType = Inbound

Inbound.PortToListen = 8881

Gateway3.ConnectionType = Gateway

Gateway3.DestinationAddress = 10.3.0.254

Gateway3.DestinationPort = 8881

GATEWAY3

Gateway 3 is configured with an inbound connection and an inbound tunnel connection.

Inbound.ConnectionType = Inbound

Inbound.PortToListen = 8881

Server.ConnectionType = InboundTunnel

Server.PortToListen = 8880

Chapter 24. Managing brokers

After installing broker support you can register the broker machines in the IBM Endpoint Manager for Remote Control server. When they have been registered you can view the list of brokers, edit the broker details and delete brokers that are no longer required.

The registered broker list is passed from the server to the targets when the targets register, in response to contact from the target, or at the start of a remote control session. The list is stored in the target property **BrokerList**.

When a target user enters a connection code to start a remote control session using a broker, the target machine tries to connect to each broker in the list until it makes a successful connection to one of them. Therefore, when making changes to the broker list you should ensure that there is still one unchanged broker in the list so that the targets can still connect in a remote control session, then when they are in the session they can contact the server and receive the updated broker list.

Registering a broker on the server

After installing and configuring broker support in your environment you can register a broker in the IBM Endpoint Manager for Remote Control server This section will explain how to add a broker to the server.

To register a broker complete the following steps

1. Select **Admin** > **New Remote Control Broker**
2. On the Add Remote Control Broker screen enter the relevant information

   Fully qualified hostname
   Enter the fully qualified (DNS) hostname for the broker.

   Port Enter the port that the broker will be listening for connections on.

   Description
   Enter a description for the broker. This is optional.
3. Click **Submit**.

The broker is added to the IBM Endpoint Manager for Remote Control database.

Viewing a list of registered brokers

After you have registered brokers you can view the list of brokers by displaying the **All Remote Control Brokers** report.

To view the registered brokers select **Admin** > **All Remote Control Brokers**

The list of registered brokers is displayed.

Editing broker details

After registering a broker on the IBM Endpoint Manager for Remote Control server you can use the edit broker feature to change any of the saved information for the broker .

To edit broker information complete the following steps

1. Select **Admin** > **All Remote Control Brokers**
2. Select the required broker.
3. Select **Edit Remote Control Broker**.
4. Change the relevant information and click **Submit**.

The broker information is updated and saved to the database.

Deleting a broker

You can remove IBM Endpoint Manager for Remote Control brokers from the database if they are no longer required.

To remove a broker from the **All Remote Control Brokers** page, complete the following steps

1. Select **Admin** > **All Remote Control Brokers**
2. Select the required broker.
3. Select **Delete Remote Control Broker**.
4. Click **Confirm** on the Confirm deletion screen.

The selected broker is deleted from the IBM Endpoint Manager for Remote Control database.

Note: Click **Cancel** on the confirm deletion screen to return to the previously displayed screen and the broker is not deleted.

Chapter 25. Certificate management

When using IBM Endpoint Manager for Remote Control to facilitate remote control sessions across the internet, you can use certificates to address the authentication and verification required for ensuring secure connections between brokers and endpoints.

A separate certificate is required for each broker that is added to the IBM Endpoint Manager for Remote Control infrastructure. This certificate needs to be trusted by the components that can connect to the broker, that is other brokers, controllers and targets and this is achieved by having signing certificates that are used to sign the broker certificates. These certificates can be self-signed or part of a chain coming from a valid internal or external Certificate Authority (CA). The signing certificates are held in a trust store on the IBM Endpoint Manager for Remote Control server and are used to verify the broker certificates.

The broker supports two key store formats.

PKCS#12
This key store format is supported by the IBM Key Management tool (ikeyman), which ships as part of IBM Endpoint Manager for Remote Control in the embedded Websphere Application Server (WAS) or standalone WAS.

PEM PEM files can be generated with the OpenSSL command line tool or other third party tools. The OpenSSL command-line tool is not shipped with IBM Endpoint Manager for Remote Control.

The PEM file needs to contain the following items, in the order listed below.

1. Broker's certificate
2. Any intermediate certificates, if required
3. Root certificate
4. Broker's private key

Use a text editor or the UNIX cat command to combine all the items in a single file.

IBM Endpoint Manager for Remote Control can use multiple types of Public Key Infrastructure (PKI)

- A commercial Certificate Authority (CA)
- An internal CA
- Self signed certificates

There is no difference between using a commercial CA or an internal CA and it is possible to mix the two kinds. For example, you can run the IBM Endpoint Manager for Remote Control server with a self-signed certificate while running all brokers with CA-signed certificates.

IBM Endpoint Manager for Remote Control provides two levels of certificate validation, strict certificate validation and non-strict certification validation.

Non-strict certificate validation

- Non-strict certificate validation performs the following checks against the certificate
  - The identity of the certificate matches the hostname of the broker that you are trying to connect to.
  - The certificate is within its validity period.

  In non-strict mode, the client does not need a trust store to perform the validation.

  Note: This type of certificate validation is strongly discouraged for production usage for remote control sessions over the internet, it is only intended for demo and test environments.

Strict certificate validation

- Strict certificate validation performs one additional check. This additional check requires that the client has a trust store that contains all the root certificates required to validate the certificate chain.

The certificate chains to a valid root CA, whose certificate is in the client's trust store

Creating a self signed certificate

To generate the certificate for a broker you can use the IBM Key Management tool. This tool is provided with the IBM Endpoint Manager for Remote Control application and with IBM WebSphere Application Server.

You can access the IBM Key Management tool if you have the IBM Endpoint Manager for Remote Control server installed with embedded components and also if you have the controller component installed. It is also provided by IBM WebSphere Application Server .

Note: If you are using WAS you should make sure that the 7.0.0-WS-WASSDK-*-FP0000021 update or later has been applied, where * is the platform. For example 7.0.0-WS-WASSDK-WinX32-FP0000021

To create a new keystore complete the following steps

1. Open a command prompt window.
2. Navigate to one of the following directories depending on where you will run the key tool from.

   Remote control server installed with embedded components
   Navigate to the IBM Endpoint Manager for Remote Control installation directory.

   WAS installed
   Navigate to the WAS installation directory.

   Controller component installed
   Navigate to the `...\Controller\jre` directory . For example ,

   Windows systems
   ```
   C:\Program Files\IBM\tivoli\Remote Control\Controller\
   jre
   ```

   Linux systems
   ```
   /opt/ibm/trc/controller/jre
   ```
3. Change to the `bin` directory.

4. Run the `ikeyman` file relevant to your operating system.

   Windows systems
   ikeyman.bat

   Linux systems
   ikeyman.sh
5. Select **Key Database File** > **New**
6. Select **PKCS12** for **Key database type**.
7. Click **Browse**, navigate to the location you want to store the keystore, type a filename for your file and click **Save**.
8. Click **OK**.
9. Enter and confirm a password to protect the keystore and click **OK**.
10. Select **Create** > **New Self-Signed Certificate**
11. Enter a name for the **Key Label**. For example, the hostname of the broker. This is the name that will be displayed in the Personal Certificates list in the key management tool GUI.
12. Select **X509 V3** for the **Version**.
13. Select a **Key Size** value. Default is 1024. Recommended value is 2048.
14. Select a **Signature Algorithm** This is a cryptographic algorithm for digital signatures and should be left as the default value SHA1WithRSA.
15. Type a **Common Name** . Set to the DNS host name and domain of your broker. For example `trcbroker.example.com`
16. Enter any additional optional information as required.
17. Enter a **Validity Period**. This is the number of days that the certificate will be valid for. Default is 365 days.
18. Click **OK**.

The .p12 file is created with the name and selected location chosen in step 7 and is displayed in the list of personal certificates in the key management tool GUI.

Note: The key store contains the private key for the certificate and this must be kept secure at all times. It is recommended that the original copy of the keystore is stored in a secure disk, for example an encrypted USB storage device or similar. Keeping a secure backup of the original keystore is also recommended.

You should copy the new certificate to the broker machine and configure the broker properties. For more details, see "Configuring the keystore on the broker."

Configuring the keystore on the broker

After you have created the keystore which holds the private key and certificate for the broker, it should be copied to the broker machine and the broker properties configured accordingly.

To configure the keystore on the broker you require a `.p12` file when using self signed certificates, see "Creating a self signed certificate" on page 246 or a `.pem` file if using CA certificates, see "Certificate Authority signed certificates" on page 249.

To configure the keystore on the broker complete the following steps

1. Copy the `.p12` or `.pem` file to the working directory of the broker machine.
2. Edit the `trc_broker.properties` file and configure the **TLSCertificateFile** property, setting it to the name of the `.p12` or `.pem` file.

Note: Use **DefaultTLSCertificateFile** to configure the certificate used for all connections to this broker. Each inbound or broker connection can also be configured to use a different certificate.

3. Use the **TLSCertificatePassphrase** property to define a password for the keystore.
4. Save the properties file.
5. Restart the broker service.

Windows systems

a. Navigate to **Control Panel** > **Administrative tools** > **Services**
b. Right click **IBM Endpoint Manager for Remote Control-Internet Connection Broker** and select **Restart**.

Linux systems

Depending on the type of Linux operating system that you are using, you can use one of the following commands to restart the broker service.

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

Using strict verification with self signed certificates

Strict verification can be used with self-signed certificates in IBM Endpoint Manager for Remote Controll. To do this you should add each broker's certificate to the server trust store.

The IBM Endpoint Manager for Remote Control controller and target, instructed by the remote control server, uses strict certificate validation by default and requires a trust store. Normally, a trust store contains the Certificate Authority's root certificates but when using self-signed certificates, there is no CA.

When using strict certificate verification, the certificate needs to be exported from the keystore and uploaded to the IBM Endpoint Manager for Remote Control. The target downloads and caches the trust store when registering, during the call home process with the server or during a remote control session. The controller downloads the trust store at the start of the remote control session.

The use of strict certificate validation is determined by the **broker.trusted.certs.required** property in the `trc.properties` file on the remote control server.

Set to Yes

Strict certificate validation is enabled. This is the default value.

Set to No

Strict certificate validation is disabled.

Note: Disabling strict verification is not recommended. When strict verification is disabled, the IBM Endpoint Manager for Remote Control controller and target will trust all valid certificates, whether they were generated by you or by a potentially malicious third party.

Extracting the certificate from the keystore

When using strict certificate verification, the certificate needs to be extracted from the keystore before being uploaded to the IBM Endpoint Manager for Remote Control server.

To extract the certificate complete the following steps

1. Open a command prompt window.
2. Navigate to the IBM Endpoint Manager for Remote Control installation directory if you have a remote control server installed with embedded components or the WAS installation directory if you have installed a stand alone remote control server.
3. Change to the `bin` directory.
4. Run the `ikeyman` file relevant to your operating system.

   Windows systems
   ikeyman.bat

   Linux systems
   ikeyman.sh
5. Select **Key Database File** > **Open**
6. Select **PKCS12** for **Key database type**.
7. Click **Browse**, navigate to and select the required .p12 file.
8. Click **Open** then **OK**.
9. Enter the password for the file and click **OK**.
10. For **Key database content** select **Personal Certificates**.
11. Select the required certificate.
12. Click **Extract Certificate**.
13. Use the default Data type **Base64-encoded ASCII data**.
14. Enter a file name and location for saving the certificate file to.
15. Click **OK**.

The certificate file, with extension .arm, will be extracted to the chosen location.

After you have extracted the certificate from the keystore you should add it to the trust store on the remote control server. For more details, see "Adding a certificate to the truststore" on page 250.

Certificate Authority signed certificates

You can use Certificate Authority (CA) signed certificates to address the authentication and verification required for ensuring secure connections between brokers and endpoints.

To use a Certificate Authority (CA) signed certificate you should obtain the following items

- A certificate for each broker in your environment.
- The root certificate and any intermediate certificates for the CA.

Note: As different CA's will operate in different ways you should consult the CA's documentation for instructions on how to obtain these.

When you have obtained the relevant certificate files you should copy the certificate to the broker machine and configure the broker properties, for more details, see Chapter 23, "Broker configuration," on page 229. The root certificate should be added to the IBM Endpoint Manager for Remote Control server, see "Adding a certificate to the truststore" on page 250.

PEM files can be generated with the OpenSSL command line tool or other third party tools. The OpenSSL command-line tool is not shipped with IBM Endpoint Manager for Remote Control. The PEM file needs to contain the following items, in the order listed below.

1. Broker's certificate
2. Any intermediate certificates, if required
3. Root certificate
4. Broker's private key

Truststore configuration

The IBM Endpoint Manager for Remote Control server holds the truststore that is used for verifying the broker certificates.

This truststore is provided to the controller system when a remote control broker session is initiated. It is sent also to the target system after the target contacts the server. The certificates that are contained in the truststore are not generated by the server. They are imported into the truststore by an administrator.

You can carry out the following actions on the certificates:

- Add a certificate to the truststore
- View the certificates in the truststore
- Edit the certificates
- Delete certificates

Note: The truststore received in the response from the server is stored on the target in the directory that is defined in the **TrustStoreDir** target property.

Adding a certificate to the truststore

Certificates are used for verifying the remote control connections that are established by using the Internet Connection Broker. You must add the certificates to the truststore on the remote control server.

If you are using self-signed certificates, you must extract the certificate from the keystore file. For more information about extracting the certificate, see “Extracting the certificate from the keystore” on page 248. If you are using a CA certificate, you are required only to add the root certificate to the server.

You can add a certificate to the truststore by completing the following steps:

1. Log on to the IBM Endpoint Manager for Remote Control server with a valid admin ID and password.
2. Open the certificate file in a text editor. Select the certificate and copy it to the clipboard. Select everything, including the BEGIN CERTIFICATE and END CERTIFICATE lines.
3. Select **Admin** > **New Trusted Certificate**.
4. Paste the certificate data from the clipboard into the **Certificate** field.
5. Click **Submit**. The certificate details are shown.
6. Verify that the correct certificate is shown and click **Submit**.

The certificate is added to the server truststore.

Note: After you add certificates to the truststore, all targets must be forced to contact the server so that they update their local truststore. Otherwise, the target cannot access those brokers for which it does not have a certificate. If there are any brokers for which the target does have a certificate, it can still use those brokers. The target automatically updates the truststore during the session and can use the new certificate in the future.

Viewing certificates in the truststore

After you have added certificates to the truststore, you can view the list of certificates from the IBM Endpoint Manager for Remote Control server UI.

To view the list of certificates in the truststore, select **Admin** > **All Trusted Certificates**.

The list of certificates is displayed.

Editing a trusted certificate

After you add certificates to the truststore on the IBM Endpoint Manager for Remote Control, you can edit the certificate details.

To edit a certificate, complete the following steps:

1. Select **Admin** > **All Trusted Certificates**.
2. Select the relevant certificate.
3. Select **Edit certificate**.
4. Edit the certificate details.
5. Click **Submit**.
6. Verify that the certificate details are correct and click **Submit**.

The certificate details are changed.

Note: After you edit certificates in the truststore, all targets must be forced to contact the server so that they update their local truststore. You must make sure that the certificates on the broker also contain the new details. Otherwise, the target cannot access those brokers whose certificate you changed. The target will then automatically update the truststore during the session and can use the new certificate details in the future.

Deleting a trusted certificate

You can remove certificates from the truststore on the IBM Endpoint Manager for Remote Control server when they are no longer required.

To delete one or more certificates, complete the following steps:

1. Select **Admin** > **All Trusted Certificates**.
2. Select the relevant certificate.
3. Click **Delete certificate**.
4. Click **Submit** on the **Confirm Deletion** screen.

The certificates are deleted from the truststore.

Chapter 26. Migrating to a new certificate

If your existing certificates are due to expire, you can create new certificates. Distribute the new certificates to the relevant endpoints so that they can continue to successfully establish remote control sessions through the broker.

Migrating to a new certificate is required when you are using self-signed certificates and you enable the **broker.trusted.certs.required** property in the `trc.properties` file. For more information about signed certificates, see "Using strict verification with self signed certificates" on page 248.

When you are using CA signed certificates, only the root certificate must be in the server truststore. Root certificates typically have a long lifespan, with typical current CA certificates not expiring until after 10 or 20 years at the time of writing. The SSL certificates signed by the CA usually expire after one year. However, you must update only the SSL certificate on the broker. There is no need to update the truststore on all of the endpoints if any of the following conditions are true.

- The new SSL certificates for the broker are issued by the same CA.
- The root certificate for the CA is already in the truststore on the server and it has been passed to all of your endpoints,

Create your self-signed certificate and distribute it to all the endpoints before you install it on the broker. To migrate to a new certificate, complete the following steps:

1. Generate the new certificate before the old certificate expires. For more information about creating a certificate, see "Creating a self signed certificate" on page 246. When to do this is determined by how long, you think it takes to update the endpoints with the new certificate. Leave the broker running with the old certificate until just before the expiration date.
2. Add the new certificate to the truststore on the server. For more information about adding a certificate, see "Adding a certificate to the truststore" on page 250.
   - Targets that call home from inside the intranet automatically receive the new certificate from the server and update their truststore.
   - Targets that successfully start a session through a broker also automatically update the truststore. Therefore, the broker must continue running with the old certificate because the target trusts this certificate. The target does not yet trust the new certificate, and therefore would be unable to start a session through the broker.
3. Install the new certificate on the broker before the old certificate expires, For more information about installing a certificate, see "Configuring the keystore on the broker" on page 247.
4. Remove the old certificate from the truststore after it expires.

When the old certificate expires, all targets that updated their truststore, can establish a remote control session by using the broker.

Chapter 27. Configuring the session connection code

You can define the number of characters required and the timeout value, for the connection code used when starting a remote control session through a broker.

When starting a remote control session involving one or more brokers, a connection code is required as part of the session authentication to match the correct controller with the correct target. For more information on starting a remote control session using a broker, see the IBM Endpoint Manager for Remote Control Controller User's Guide. You can globally configure properties for this code within the IBM Endpoint Manager for Remote Control server UI. To configure the broker session connection code complete the following steps

1. Select **Admin** > **Edit properties file**
2. Select **trc.properties**
3. Set the connection code length.

   broker.code.length
   Determines the number of characters required to be entered for the connection code, in the connection code window, when starting a remote control session through an Internet Connection Broker. Default is 7.

   Note: There is no limit to the number of characters that can be set however you should use your own discretion when setting this value.
4. Set the connection code timeout value

   broker.code.timeout
   Determines the number of seconds the connection code timer will count down from, for the connection code options available when you are starting a broker session as a controller user. Default is 900.
5. Click **Submit** You should reset the application in order for the new values to take effect by clicking **Admin** > **Reset Application**.

Chapter 28. Target registration before a remote control session

When you have targets that are on the internet or third-party networks and cannot register directly with the IBM Endpoint Manager for Remote Control server you can configure server properties to allow the target to register with the server. When the target registers, you can start a remote control session with the target, by using a broker.

You can also configure the target properties to assign the target to specific target groups when it registers with the server.

Server properties

Use the server property **rc.create.assets.from.brokers** to determine whether targets can register with the remote control server when the target user enters the connection code at the start of the remote control session. For details about starting a remote control session by using a broker, see the IBM Endpoint Manager for Remote Control Controller User's Guide. The **rc.create.assets.from.brokers** property is defined in the `trc.properties` file and is set to **true** by default. For details of the `trc.properties` file see, "trc.properties" on page 172.

rc.create.assets.from.brokers

true Targets can register with the server at the start of a broker remote control session. When they register, they are assigned to the **DefaultTargetGroup** by default.

false Targets cannot register with the server.

Target properties

The following target property values must be set to allow the target to register with the server.

- **Managed** = Yes
- **ServerURL** = the host name or IP address of the server that you want the target to register with.
- **BrokerList** = the list of host names or IP addresses of the brokers and their ports, that you want the target to connect to. In the format *hostname1:port,hostname2:port,hostname3:port*.

Note: You must restart the target service when you change target property values so that the new values take effect.

Assigning targets to target groups when they register

You can assign the target to other target groups when it registers, instead of the **DefaultTargetGroup**, in two ways.

Using the target group override option.

Set the **allow.target.group.override** property to true to assign the target to the groups listed in the **GroupLabel** target property, instead of the **DefaultTargetGroup**.

1. Edit the `trc.properties` file and set **`allow.target.group.override`** = *true*.
2. Save the file.
3. Edit the target properties and set **`GroupLabel`** to a list of target groups.

   Note: These groups must already be defined in the server.

   The target is assigned to the target groups listed in **`GroupLabel`**, when it registers.

Using target membership rules.
Using the **target membership rules** function, create rules that the targets match on to assign them to specific target groups.

If you define rules and the target group override function is also enabled, the target is assigned to the target groups that are defined for both of these options when it registers.

There can be cases where the remote control session cannot start for the following reasons.

- The target was not assigned to any groups.
- The group assignment configuration is incorrect.
- The target is assigned to a group that the controller user does not have permissions to access targets from.

In all cases, no policies can be derived for the session, so even though the target is registered in the server, the session is rejected.

Chapter 29. Configuring target properties

When a target takes part in a peer to peer remote control session, its properties determine what functions are available during the session. Target properties can be configured by creating and running a target configuration task in the IBM Endpoint Manager console. For more details see the, IBM Endpoint Manager for Remote Control Console User's Guide. You can also edit the target properties manually.

Editing the target properties on a Windows target

1. Edit the target registry and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Tivoli\Remote Control\Target`

   Note: On a 64 bit system all the 32-bit registry keys are under the **Wow6432Node** key, for example: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\IBM\Tivoli Remote Control\Target`
2. Right-click the required property and select **Modify**
3. Set the required value and click **OK**.
4. Restart the target service.

Editing the target properties on a Linux target

1. Edit the `ibmtrct.conf` file.
2. Modify the required properties.
3. Save the file.
4. Restart the target service.

Specifying a target IP address for connecting to the server

When a target has multiple IP addresses, use the target property, **LocalIPInterface**, to specify which IP address should be used by the target for remote control sessions and for reporting to the server.

Specifying an IP address for a windows target

Use the, **LocalIPInterface**, property to specify the IP address that the Windows target will use for connecting to the IBM Endpoint Manager for Remote Control server.

Modify this parameter within the Windows registry by completing the following steps:

1. At a command prompt type `regedit`.
2. Navigate to `\HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Tivoli\Remote Control\Target`
3. Right-click **LocalIPInterface** and select **Modify**.
4. Enter the required IP address in the **Value data** field and click **OK**.
5. Restart the target service.

The windows target will use the defined IP address for remote control sessions and for reporting to the IBM Endpoint Manager for Remote Control server.

Specifying an IP address for a Linux target

Use the, **LocalIPInterface**, property to specify the IP address that the Linux target will use for connecting to the IBM Endpoint Manager for Remote Control server.

Modify this parameter within the IBM Endpoint Manager for Remote Control Linux target configuration file by completing the following steps

1. Edit the `ibmtrct.conf` file
2. Set the value of **LocalIPInterface** to the required IP address and save the file.
3. Restart the target service.

Joining or Disconnecting a session

You can configure peer to peer targets so that a controller user can join or disconnect the remote control session that the target is already connected to. For more details of how to use these function see the IBM Endpoint Manager for Remote Control Controller User's Guide. Configure the following target properties to enable these features.

Join the session

- Managed = No
- CheckUserLogin=Yes

Note: Collaboration should also be started for the join feature to be enabled.

Disconnect the session

- Managed = No
- CheckUserLogin=Yes
- AllowForceDisconnect = Yes

AllowForceDisconnect

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.

ForceDisconnectTimeout
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.

Chapter 30. Importing data from other sources

As well as adding user and target data to the database using the server UI you can also import this data into the database either through synchronizing with an LDAP server or by importing a text file.

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

Import data from csv files into the IBM Endpoint Manager for Remote Control database

Use comma-separated text files to import numerous records of information into the IBM Endpoint Manager for Remote Control database instead of adding the records individually. Using these files with *import template*s, that are used to map the data in your file to the relevant columns in the database tables. You can import the data into the database in one go. For example, multiple users details can be imported into the database from a csv file rather than having to be entered individually.

To import data from a csv file, complete the following procedures.

- Create a csv file
- Create an import template
- Import the csv file by using an import template

Creating a csv file

You can create a csv file to list the details of the various items to be imported. These files can be created and saved as type CSV or TSV, with or without a header row, which is a set of column headings corresponding to specific column names within the tables in the database. Each row of the file should have the information, that is added to each column in the database table, separated by a comma for a CSV file or tab for a TSV file.

Below is an example of the content of a CSV file with a header included

FORENAME,SURNAME,EMAIL

Fred,Bloggs,Fbloggs@example.com

John,Smith,JSmith@example.com

David,Brown,DBrown@example.com

Mary,Smith,MSmith@example.com

Below is an example of the content of a CSV file with no header

Fred,Bloggs,Fbloggs@example.com

John,Smith,JSmith@example.com

David,Brown,DBrown@example.com

Mary,Smith,MSmith@example.com

When you have created your csv file, map this data to the IBM Endpoint Manager for Remote Control database using a template that will import the data into the correct tables in the database.

Mapping data in a csv file to the IBM Endpoint Manager for Remote Control database.

To ensure that the data in your csv file is added to the correct tables in the database, you must map the columns in your file to specific columns and tables. Create an import template to import the data. Use the template to define the correct format to be used for reading your file. You can select which columns of data in your file are to be added to the database and where the data is added to in the database. If the data that you are adding does not refer to an item already in the database, you can create a new item in the database. For example, if you are adding user data and the user data is not already in the database, select to create a new user with the data. A knowledge of the database tables and their structure is important for creating import templates. For more information about the database tables, see Chapter 31, “Database table and column descriptions,” on page 283.

Note: When user or target data is being imported, you must supply at least one of the following columns for import from the csv file

Targets
From the ASSET table, **SERIAL_NO**, **UUID**, or **COMPUTERNAME**.

Users From the USERS table, **USERID**, **EMAIL**, or **EMPLOYEEID** .

Note: **USERKEY** is not the same as **USERID**, it is **USERID** that must be used.

To create a new Import Template, complete the following steps:

1. Click **Admin** > **Import Data** > **Create new import template**. The Edit Data Import Template screen is displayed.
2. Type the relevant information.

   Name Type a name for your template.

   File Header
   This field is used if the file that you are importing has a set of column headings that correspond to specific database table column names. Type a comma-separated set of column names. If there is no header in the file, this field is left blank.

   ```
   for example:  USERID,FORENAME,SURNAME
   ```

   Number of Columns
   Type the number of columns of data that is in your csv file. If you decide to change this value, click **Update** to change the numbers that are shown in the Column Number list.

   Note: If you click **Update** after you select the file encoding, you must check that the required encoding is still selected. If it is not, select the encoding value.

   File Delimiter
   Type the character that separates the columns in the file.

   ```
   for example:  , or /
   ```

   File Encoding
   Used to select the file encoding that applies to your CSV file so that it can be interpreted correctly. Choose the appropriate method for selecting the file encoding.
   - Select the required file encoding from the list.
   - Type in all or part of the file encoding name and click **Search**.
   - Leave the field with no selection and the ASCII UTF-8 file encoding is used.

   Date Format
   If you require dates to be imported, follow the instructions on screen for determining the format.

   Create Assets?

   true If the data that you are importing applies to a target that is not already in the ASSET table, create a target. The ASSET table contains the details of already registered targets.

   false If the data that you are importing applies to a target that is not already in the ASSET table, do not import the data into the database.

Create Users?

true If the data that you are importing applies to a user that is not already in the database, create a user.

false If the data that you are importing applies to a user that is not already in the database, do not import the data into the database.

Column Number / Table / Column

The list of input fields under the column headings are used to determine where the data in your import file is placed in the database. Follow the on screen instructions for the database column types that must be specified for importing target and user data.

- From the **Column Number** list, select the number of the column in your file that contains the data to import.
- Click the ? icon next to the **Table** field.
- Select the relevant table from the tables list.
- Select the relevant column from the column list.
- Click **OK**
- Repeat these steps for each column in the file that you are importing.

Note: Select only the columns that you want to import the data for, you do not have to import every column.

For example: If your file contained the following data

USERID, FORENAME,SURNAME,,LOCATION
awilson,Alan,Wilson,Greenock

and you only wanted to import the FORENAME and LOCATION you would select only 2 and 4 for Column Number.

Test / Browse

You can use this function to check that a test csv file, similar to the one to be uploaded, is correctly read and mapped by the import template. The result of the test shows whether the columns and header are mapped and read correctly and if the chosen file encoding reads the characters correctly.

To use this function, complete the following steps:

a. Create a test csv file similar in layout to the file to be uploaded, including the header if your file has one.
b. Click **Browse** and select the test csv file.
c. Click **Test** .
d. The results of the test are shown in a new window and provide the following details.
   - If you include a header in your file, a message about the header is shown.
   - A table that shows the database columns that are defined for each column in the file.
   - The data that is mapped from the csv file.

   From the results, you can see whether the import template handles the data correctly. If not, you can change the template before you save it.

Note:

1) You have not imported any data at this stage. Complete step 3 to save the import template.
2) Check that the required encoding is still selected. If not, select the encoding before you save the template.

3. On the Edit Data Import Template screen click **Submit**

The import template is created. Use the template to import a csv file and map the data in the csv file correctly to the relevant tables in the database. For more information about importing a csv file, see "Importing a csv file."

Viewing the list of defined Import Templates

When you have created import templates you can view the list of all templates that have been defined. To view the list of defined import templates click **Admin** > **Import Data** > **All templates**.

The Show all import templates screen is displayed.

Changing the details of an Import Template

After you have created an import template you can update or change any of the information defined for it. For example you may wish to change its name or add another column to be imported. To change the details for an import template complete the following steps :

1. Click **Admin** > **Import Data** > **All Templates**
2. Select the required email template.
3. From the **Admin** menu OR from the **Action list** select **Edit selected template** The Edit Data Import Template screen is displayed
4. Make the required changes

   Note: If you click the update button after you have selected the file encoding, you will need to check that the required encoding is still selected, if not re select the encoding.
5. Click **Submit**

The details for the selected import template are updated.

Deleting Import Templates

You can delete any import templates that you no longer need.

To delete an import template complete the following steps :

1. Click **Admin** > **Import Data** > **All Templates**
2. Select the required email templates
3. From the **Admin** menu OR from the **Action list** select **Delete Selected templates**

The selected import template is removed and is no longer listed in the **All Templates** report.

Importing a csv file

After you have created a csv file and an import template,you can use the import file function to add the data from your file into the IBM Endpoint Manager for

Remote Control database. This is useful for adding numerous records of data to the database at once instead of having to add the items individually.

To add the data into the database, complete the following steps :

1. Click **Admin** > **Import Data** > **Import File**. The Import Existing Data screen is displayed
2. Choose the appropriate method for selecting your csv file.
   a. Click **Browse** to navigate to and select the required csv file.
   b. Type in the path and name of the file that you wish to import

      for example : `c:\myfiles\test.csv` on Windows systems

      `/myfiles/test.csv` on UNIX-based systems
3. If your file has no header row, select an import template from the list that will be used to map your data to the relevant database table.

   Note: If your file has a header in it, it will match automatically with a defined template and therefore no selection is required.
4. Click **Submit** The message `File has been queued for processing` is displayed

Your data is added to the database. You can check this by displaying the relevant report for this data. For example if you have added user data, you can use the **All users** report to check that the data has been added correctly.

Chapter 31. Database table and column descriptions

The IBM Endpoint Manager for Remote Control Server program comes with a built-in database. By default, the database provides several tables that contain a variety of target and user information. Understanding the information provided with this database can help you perform advanced functions such as creating a custom report. Although you will primarily need to understand tables with target and user information, internal system table information is also included here.

The following information is provided to help you understand the overall structure of the built-in database and to help you understand how information is divided into each table.

Note: Some of the tables described in this section are not used by the current version of IBM Endpoint Manager for Remote Control and are considered deprecated. They might be removed in future versions of the product.

ASSET schema tables

Table 20. ACCESSREQUEST table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ACCESSREQUEST	ACCESSREQUESTKEY	INTEGER	4	No
	ADMINNOTES	VARCHAR	500	Yes
	ANONYMOUS	INTEGER	4	Yes
	ASSETGROUPKEY	INTEGER	4	Yes
	CREATED	TIMESTAMP	10	No
	EMAIL	VARCHAR	256	Yes
	EXPIRED	INTEGER	4	Yes
	GRANTEND	TIMESTAMP	10	Yes
	GRANTSTART	TIMESTAMP	10	Yes
	PASSKEY	VARCHAR	128	Yes
	REQUESTEND	TIMESTAMP	10	Yes
	REQUESTNOTES	VARCHAR	500	Yes
	REQUESTSTART	TIMESTAMP	10	Yes
	REQUESTTYPE	INTEGER	4	Yes
	STATUS	INTEGER	4	Yes
	USERGROUPKEY	INTEGER	4	Yes
	USERKEY	INTEGER	4	Yes

Table 21. ACCESSREQUESTTARGETS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ACCESSREQUESTTARGETS	ACCESSREQUESTKEY	INTEGER	4	No
	CREATED	TIMESTAMP	10	Yes
	HWKEY	INTEGER	4	Yes

Table 21. ACCESSREQUESTTARGETS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	TARGETGROUPKEY	INTEGER	4	No

Table 22. ASSET table - Main Target table for storing the majority of the Target information

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET	HWKEY	INTEGER	4	No
	MAX_REVISION	INTEGER	4	No
	MAX_PROCESSED_REVISION	INTEGER	4	No
	IS_PC_ASSET	CHARACTER	1	No
	USERKEY	INTEGER	4	No
	UUID	VARCHAR	32	Yes
	SERIAL_NO	VARCHAR	64	No
	MANUFACTURER	VARCHAR	64	Yes
	MODEL	VARCHAR	64	Yes
	COMPUTERNAME	VARCHAR	64	Yes
	CUR_USER	VARCHAR	64	Yes
	ENCLOSURE	VARCHAR	64	Yes
	DOMAIN_NAME	VARCHAR	64	Yes
	MAC_ADDRESSES	VARCHAR	128	Yes
	IP_ADDRESSES	VARCHAR	64	Yes
	DATE_TIME	TIMESTAMP	10	No
	FIRST_OWNED_DATE	TIMESTAMP	10	Yes
	IS_LPAR	INTEGER	4	No
	PARENT_HWKEY	INTEGER	4	No

Note: This table may be removed in future releases.

Table 23. ASSET_AUTHENTICATION_KEY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET_AUTHENTICATION_KEY	HWKEY	INTEGER	4	No
	KEY_TYPE	INTEGER	4	No
	UNIQUE_KEY	VARCHAR	50	Yes
	CREATED	TIMESTAMP	10	No

Table 24. ASSET_INFO table - Table for storing additional Asset information. Holds the full demographic information and 9 custom fields

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET_INFO	HWKEY	INTEGER	4	No
	DESCRIPTION	VARCHAR	30	Yes
	COMPANY	VARCHAR	40	Yes
	LOCATION	VARCHAR	60	Yes

Table 24. ASSET_INFO table - Table for storing additional Asset information. Holds the full demographic information and 9 custom fields (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	DEPARTMENT	VARCHAR	30	Yes
	FLOOR	VARCHAR	40	Yes
	ROOM	VARCHAR	40	Yes
	ADDRESS_1	VARCHAR	50	Yes
	ADDRESS_2	VARCHAR	50	Yes
	TOWN	VARCHAR	40	Yes
	POSTCODE	VARCHAR	10	Yes
	COUNTRY	VARCHAR	25	Yes
	STATE	VARCHAR	25	Yes
	ASSETTAG	VARCHAR	30	Yes
	ASSETTYPE	VARCHAR	30	Yes
	STATUS	VARCHAR	30	Yes
	DESK	VARCHAR	8	Yes
	CUSTOM1	VARCHAR	250	Yes
	CUSTOM2	VARCHAR	250	Yes
	CUSTOM3	VARCHAR	250	Yes
	CUSTOM4	VARCHAR	250	Yes
	CUSTOM5	VARCHAR	250	Yes
	CUSTOM6	VARCHAR	250	Yes
	CUSTOM7	VARCHAR	250	Yes
	CUSTOM8	VARCHAR	250	Yes
	CUSTOM9	VARCHAR	250	Yes
	INSTALLED_DATE	TIMESTAMP	10	Yes
	CATEGORY	VARCHAR	64	Yes
	IBM_OWNED	VARCHAR	1	Yes
	IBM_ASSETTAG	VARCHAR	30	Yes
	USER_VERIFIED	VARCHAR	10	Yes
	STATUS_DATE	TIMESTAMP	10	Yes
	LAST_INSPECTION_DATE	TIMESTAMP	10	Yes

Note: This table may be removed in future releases.

Table 25. ASSET_OWNED table - Table for storing Asset purchase information

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSET_OWNED	HWKEY	INTEGER	4	No
	PURCHASE_DATE	TIMESTAMP	10	Yes
	INITIAL_VALUE	DECIMAL	5	No
	DEPRECIATION_PERIOD	INTEGER	4	Yes
	PURCHASER	VARCHAR	50	Yes
	SUPPLIER	VARCHAR	50	Yes

Table 25. ASSET_OWNED table - Table for storing Asset purchase information (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	PO_NO	VARCHAR	50	Yes
	WARRANTY_EXPIRY	TIMESTAMP	10	Yes

Note: This table may be removed in future releases.

Table 26. CALLED_HOME table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CALLED_HOME	HWKEY	INTEGER	4	No
	UUID	VARCHAR	32	Yes
	SERIAL_NO	VARCHAR	64	Yes
	MANUFACTURER	VARCHAR	64	Yes
	MODEL	VARCHAR	64	Yes
	COMPUTERNAME	VARCHAR	64	Yes
	IP_ADDRESS	VARCHAR	15	Yes
	MAC_ADDRESS	VARCHAR	128	Yes
	SUBNET	VARCHAR	15	Yes
	FIRST_CALLHOME	TIMESTAMP	10	No
	LAST_CALLHOME	TIMESTAMP	10	No
	HWCRC	VARCHAR	8	Yes
	SWCRC	VARCHAR	8	Yes

Note: This table may be removed in future releases.

Table 27. CHAT_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CHAT_LOG	CHATKEY	BIGINT	8	No
	USERKEY	INTEGER	4	No
	MSG_DATA	VARCHAR	512	Yes
	DATE_TIME	TIMESTAMP	10	No

Note: This table may be removed in future releases.

Table 28. CURRENT_IPADDRESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CURRENT_IPADDRESS	HWKEY	INTEGER	4	No
	IPADDRESS	VARCHAR	15	Yes
	LAST_UPDATED	TIMESTAMP	10	No

Table 29. EMAIL_TEMPLATE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
EMAIL_TEMPLATE	EMAILKEY	VARCHAR	4	No
	"LOCALE"	VARCHAR	5	No

Table 29. EMAIL_TEMPLATE table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	NAME	VARCHAR	100	No
	DESCRIPTION	VARCHAR	400®	Yes
	EMAIL_FROM	VARCHAR	70	Yes
	TITLE	VARCHAR	240	Yes
	CONTENT	VARCHAR	3000	No
	CREATOR	VARCHAR	20	Yes
	CREATED	TIMESTAMP	10	No

Table 30. IMPORT_TEMPLATE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
IMPORT_TEMPLATE	IMPORTKEY	INTEGER	4	No
	NAME	VARCHAR	55	No
	"ENCODING"	VARCHAR	20	Yes
	HEADER	VARCHAR	100	No
	COLS	INTEGER	4	No
	DELIMITER	VARCHAR	10	No
	REVISION_HANDLER	INTEGER	4	No
	APPEND_HANDLER	INTEGER	4	No
	CREATE_ASSETS	INTEGER	4	No
	CREATE_USERS	INTEGER	4	No

Table 31. IMPORT_TEMPLATE_COLS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
IMPORT_TEMPLATE_COLS	IMPORTKEY	INTEGER	4	No
	COL_NO	INTEGER	4	No
	TABLE_NAME	VARCHAR	20	No
	COL_NAME	VARCHAR	30	No
	UPDATE_COL	SMALLINT	2	No
	ASSET_FIELD	SMALLINT	2	No
	LPAR_FIELD	SMALLINT	2	No

Table 32. MEMBERSHIP_RULES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MEMBERSHIP_RULES	RULEKEY	INTEGER	4	NO
	PRIORITY	INTEGER	1	NO
	CREATED	TIMESTAMP	10	NO
	CREATED_BY	VARCHAR	4	No
	LAST_MODIFIED	TIMESTAMP	10	No
	LAST_MODIFIED_BY	INTEGER	4	No
	STOP_PROCESSING	CHAR	1	No

Table 32. MEMBERSHIP_RULES table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	IP_RANGE_START	VARCHAR	39	No
	IP_RANGE_END	VARCHAR	39	No
	COMPUTER_NAME	VARCHAR	512	No
	COMMENT	VARCHAR	1024	No

Table 33. MEMBERSHIP_RULES_GROUPS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MEMBERSHIP_RULES_GROUPS	MRGKEY	INTEGER	4	No
	RULEKEY	INTEGER	4	No

Note: This table may be removed in future releases.

Table 34. NET_ADAPTERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
NET_ADAPTERS	HWKEY	INTEGER	4	No
	REVISION	INTEGER	4	No
	DEVICE_ID	VARCHAR	50	Yes
	NAME	VARCHAR	100	Yes
	"TYPE"	VARCHAR	50	Yes
	DESCRIPTION	VARCHAR	150	Yes
	MAC_ADDRESS	VARCHAR	20	Yes
	MANUFACTURER	VARCHAR	50	Yes
	SERVICENAME	VARCHAR	50	Yes

Note: This table may be removed in future releases.

Table 35. QUEUE_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUEUE_LOG	EVENT_ID	INTEGER	4	No
	DESCRIPTION	VARCHAR	256	Yes
	PROCESS_TIME_MS	BIGINT	8	No
	HIGH_PRIORITY	INTEGER	4	No
	DATE_TIME	TIMESTAMP	10	Yes

Table 36. RC_GATEWAYS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
RC_GATEWAYS	Gateway.KEY	INTEGER	4	No
	HOSTNAME	VARCHAR	256	Yes
	CONNECTIVITY	VARCHAR	512	Yes
	DESCRIPTION	VARCHAR	256	Yes

Table 37. RC_BROKERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
RC_BROKERS	BROKERKEY	INTEGER	4	No
	HOSTNAME	VARCHAR	256	No
	PORT	INTEGER	4	No
	DESCRIPTION	VARCHAR	256	Yes

Table 38. REVISIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
REVISIONS	HWKEY	INTEGER	4	No
	REVISION	INTEGER	4	No
	PROCESSED	CHARACTER	1	No
	DATE_TIME	TIMESTAMP	10	No

Table 39. SERVER_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SERVER_LOG	EVENT_ID	INTEGER	4	No
	DESCRIPTION	VARCHAR	176	Yes
	DATE_TIME	TIMESTAMP	10	No

Table 40. TASK table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TASK	TASKKEY	INTEGER	4	No
	"TYPE"	VARCHAR	30	No
	NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	255	Yes
	SCHEDULED	INTEGER	4	No
	MENU	VARCHAR	50	Yes
	ACTIVE	INTEGER	4	No
	RUNONCE	INTEGER	4	No
	START_DATE	TIMESTAMP	10	Yes
	END_DATE	TIMESTAMP	10	Yes
	PERIOD	INTEGER	4	No
	USER_QUERY	INTEGER	4	No
	USERLIST	VARCHAR	100	Yes
	QUERY	INTEGER	4	No
	QUERY2	INTEGER	4	No
	QUERY3	INTEGER	4	No
	QUERY4	INTEGER	4	No
	CUSTOM_QUERY	INTEGER	4	No
	CUSTOM_QUERY2	INTEGER	4	No
	MAIL_TEMPLATE	INTEGER	4	Yes

Table 40. TASK table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	SUBREPORT	INTEGER	4	No
	NEXT_TASKKEY	INTEGER	4	No
	CREATOR	VARCHAR	20	Yes
	CREATED	TIMESTAMP	10	No

Table 41. TASK_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TASK_LOG	TASKKEY	INTEGER	4	No
	USERKEY	INTEGER	4	Yes
	USER_LIST	VARCHAR	2000	Yes
	USER_COMMENT	VARCHAR	200	Yes
	DATE_TIME	TIMESTAMP	10	Yes

Table 42. TASK_SELECTED table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TASK_SELECTED	TASKKEY	INTEGER	4	No
	MENU_NAME	VARCHAR	50	Yes
	DESCRIPTION	VARCHAR	250	Yes

Note: This table may be removed in future releases.

Table 43. TRANSFERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TRANSFERS	HWKEY	INTEGER	4	No
	IS_PC_ASSET	CHARACTER	1	No
	OLD_USERKEY	INTEGER	4	No
	NEW_USERKEY	INTEGER	4	No
	APPROVED	CHARACTER	1	No
	USER_COMMENT	VARCHAR	30	No
	REASON	VARCHAR	30	Yes
	CREATED	TIMESTAMP	10	No
	PROCESSED	TIMESTAMP	10	Yes

Table 44. TX_LOG table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TX_LOG	USERKEY	INTEGER	4	No
	HWKEY	INTEGER	4	Yes
	TX_ID	INTEGER	4	No
	TX_DATA	VARCHAR	500	No
	TABLE_COLUMN	VARCHAR	128	Yes
	OLD_VALUE	VARCHAR	128	Yes

Table 44. TX_LOG table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	NEW_VALUE	VARCHAR	128	Yes
	TX_TIME	INTEGER	4	Yes
	DATE_TIME	TIMESTAMP	10	No

Note: This table may be removed in future releases.

Table 45. XML_LOOKUP table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
XML_LOOKUP	SCHEMA_NAME	VARCHAR	64	No
	TABLE_NAME	VARCHAR	64	No
	COLUMN_NAME	VARCHAR	64	No
	TEXT	INTEGER	4	No
	FILETYPE	VARCHAR	20	No
	VERSION	VARCHAR	20	No
	PARENT_XPATH	VARCHAR	255	Yes
	XPATH	VARCHAR	255	Yes
	DEFAULT_VALUE	VARCHAR	255	Yes
	NODETYPE	VARCHAR	10	No
	ISKEY	CHARACTER	1	Yes
	PROBE_SET	INTEGER	4	No
	PRIORITY	INTEGER	4	No

COMMON schema tables

Table 46. ACTIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ACTIONS	ACTIONKEY	INTEGER	4	No
	ACTION_GROUP_ID	INTEGER	4	Yes
	ACTION_INTERNAL_NAME	VARCHAR	100	No
	ACTIONAME	VARCHAR	100	No
	ACTIONDESC	VARCHAR	1024	Yes
	ACTION_LABEL_PROP	VARCHAR	100	Yes
	ACTION_TYPE	INTEGER	4	Yes

Table 47. ASSETPERMISSIONSDEFAULT table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSETPERMISSIONSDEFAULT	ASSETPERMDEFKEY	INTEGER	4	No
	ACTIONKEY	INTEGER	4	No
	ACTIONSTATE	INTEGER	4	Yes
	INT_VALUE	INTEGER	4	Yes
	STR_VALUE	VARCHAR	255	Yes

Table 48. ASSETPERMISSIONSDEFAULTNAME table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ASSETPERMISSIONSDEFAULTNAME	ASSETPERMDEFKEY	INTEGER	4	No
	DEFDESC	VARCHAR	1024	Yes

Table 49. CACHE_GROUPASSET table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CACHE_GROUPASSET	HWKEY	INTEGER	4	No
	GAKEYS	VARCHAR	128	Yes
	EXPIRES	TIMESTAMP	10	Yes

Table 50. CACHE_GROUPUSER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CACHE_GROUPUSER	USERKEY	INTEGER	4	No
	GUKEYS	VARCHAR	128	Yes
	EXPIRES	TIMESTAMP	10	Yes

Table 51. CONFIGURATION table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CONFIGURATION	NAME	VARCHAR	128	No
	VALUE	VARCHAR	256	Yes

Table 52. CUSTOM_QUERY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CUSTOM_QUERY	CUSTOM_QUERYKEY	INTEGER	4	No
	NAME	VARCHAR	50	No
	MENU_NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	120	Yes
	SQL_DATA	CLOB	524288	No
	CREATOR	INTEGER	4	Yes
	CREATED	TIMESTAMP	10	No

Table 53. CUSTOM_QUERY_GROUP_ACCESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CUSTOM_QUERY_GROUP_ACCESS	CUSTOM_QUERYKEY	INTEGER	4	No
	GROUPKEY	INTEGER	4	No

Table 54. CUSTOM_QUERY_USER_ACCESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
CUSTOM_QUERY_USER_ACCESS	CUSTOM_QUERYKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No

Table 55. FAVOURITES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
FAVOURITES	USERKEY	INTEGER	4	No
	HWKEY	INTEGER	4	No

Table 56. GROUPASSET table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPASSET	GAKEY	INTEGER	4	No
	NAME	VARCHAR	50	Yes
	GADESC	VARCHAR	1024	Yes
	ASSETPERMDEFKEY	INTEGER	4	Yes
	CREATED	TIMESTAMP	10	Yes

Table 57. GROUPASSETGROUPMEMBER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPASSETGROUPMEMBER	GAKEY	INTEGER	4	No
	GAPARENTKEY	INTEGER	4	No

Table 58. GROUPASSETMEMBER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPASSETMEMBER	GAKEY	INTEGER	4	No
	GAPARENTKEY	INTEGER	4	No

Table 59. GROUPATTRIBUTES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPATTRIBUTES	ATT_DEFN	INTEGER	4	No
	GROUPTYPE	INTEGER	4	No
	GROUPKEY	INTEGER	4	No
	STR_VALUE	VARCHAR	255	Yes
	INT_VALUE	INTEGER	4	Yes

Table 60. GROUPATTRIBUTEDEFNS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPATTRIBUTEDEFNS	ATT_DEFN_KEY	INTEGER	4	No
	GROUPTYPE	INTEGER	4	No
	ATT_INTERNAL_NAME	VARCHAR	100	No
	ATT_NAME	VARCHAR	100	No
	ATT_DESC	VARCHAR	1024	Yes
	ATT_LABEL_PROP	VARCHAR	100	Yes
	ATT_DATA_TYPE	INTEGER	4	No
	ATT_RULE	INTEGER	4	No

Table 61. GROUP_HOMEPAGE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUP_HOMEPAGE	GHKEY	INTEGER	4	No

Table 61. GROUP_HOMEPAGE table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	GROUPKEY	INTEGER	4	No
	CUSTOM_QUERYKEY	INTEGER	4	Yes
	LAST_UPDATED	TIMESTAMP	10	No

Table 62. GROUPUSERGROUPMEMBER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUPUSERGROUPMEMBER	GROUPKEY	INTEGER	4	No
	GUPARENTKEY	INTEGER	4	No

Table 63. GROUP_MEMBERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
GROUP_MEMBERS	GROUPKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No

Table 64. LIVEPOINTS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
LIVEPOINTS	HWKEY	INTEGER	4	No
	PORT	INTEGER	4	No
	HOSTNAME	VARCHAR	64	Yes
	DOMAIN_NAME	VARCHAR	64	Yes
	CUSTOM1	VARCHAR	128	Yes
	CUSTOM2	VARCHAR	128	Yes
	CUSTOM3	VARCHAR	128	Yes
	IP_ADDRESS	VARCHAR	64	Yes
	LOGGED_USER	VARCHAR	48	Yes
	USER_LANGUAGE	VARCHAR	48	Yes
	OS_NAME	VARCHAR	50	Yes
	OS_LANGUAGE	VARCHAR	48	Yes
	TIMEZONE	VARCHAR	48	Yes
	SCREENSAVER	VARCHAR	300	Yes
	RC_STATE	VARCHAR	128	Yes
	RC_CONTROLLER	VARCHAR	128	Yes
	CUSTOM_REGKEY	VARCHAR	128	Yes
	INT_MODE	VARCHAR	48	Yes
	ENDPOINT_ID	VARCHAR	64	Yes
	TARGET_ID	VARCHAR	64	Yes
	LAST_UPDATE	VARCHAR	10	Yes

Table 65. MENU_ACTIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MENU_ACTIONS	QUERYKEY	INTEGER	4	No

Table 65. MENU_ACTIONS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	MENU	VARCHAR	30	No
	NAME	VARCHAR	30	No
	COL1	VARCHAR	60	No
	COL2	VARCHAR	60	No
	COL3	VARCHAR	60	No
	COL4	VARCHAR	60	No
	MENU_ACTION	VARCHAR	150	Yes
	LOGO	VARCHAR	40	Yes
	MULTIPLE	VARCHAR	15	No
	CLICK_TYPE	CHARACTER	1	No
	DESCRIPTION	VARCHAR	200	Yes
	AUTHORITY	CHARACTER	1	No
	AUTH_PROPERTY	VARCHAR	100	Yes

Table 66. MENU_LINKS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MENU_LINKS	QUERYKEY	INTEGER	4	No
	MENU	VARCHAR	30	No
	COL1	VARCHAR	60	No
	COL2	VARCHAR	60	No
	COL3	VARCHAR	60	No
	COL4	VARCHAR	60	No
	MULTIPLE	VARCHAR	15	Yes
	QUERYKEY2	INTEGER	4	No

Table 67. MENU_STATIC_ITEMS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MENU_STATIC_ITEMS	MENUKEY	INTEGER	4	No
	MENU	VARCHAR	30	Yes
	SUB_MENU	VARCHAR	30	Yes
	NAME	VARCHAR	60	No
	MENU_URL	VARCHAR	150	Yes
	LOGO	VARCHAR	40	Yes
	DESCRIPTION	VARCHAR	200	Yes
	PRIORITY	INTEGER	4	No
	AUTHORITY	CHARACTER	1	No
	AUTH_PROPERTY	VARCHAR	100	Yes
	CONDITIONS	VARCHAR	50	Yes
	CLICK_TYPE	CHARACTER	1	No

Table 68. MENU_STATIC_LINKED_ITEMS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
MENU_STATIC_LINKED_ITEMS	QUERYKEY	INTEGER	4	No
	MENU	VARCHAR	30	No
	MENU_NAME	VARCHAR	30	No
	NAME	VARCHAR	30	No
	COL1	VARCHAR	60	No
	COL2	VARCHAR	60	No
	COL3	VARCHAR	60	No
	COL4	VARCHAR	60	No
	DESCRIPTION	VARCHAR	200	Yes
	AUTHORITY	CHARACTER	1	No
	AUTH_PROPERTY	VARCHAR	100	Yes

Note: This table may be removed in future releases.

Table 69. ORGANISATION table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
ORGANISATION	ORGKEY	INTEGER	4	No
	DEPT_ID	VARCHAR	50	No
	NAME	VARCHAR	128	No
	REAL_DEPT	VARCHAR	250	Yes
	REAL_DEPT_ID	VARCHAR	100	Yes
	PARENT_ORGKEY	INTEGER	4	No
	PARENT_DEPT_ID	VARCHAR	50	Yes
	OWNER_USERKEY	INTEGER	4	No
	OWNER_EMPLOYEEID	VARCHAR	50	Yes
	"TYPE"	VARCHAR	128	Yes
	ADDRESS_1	VARCHAR	128	Yes
	ADDRESS_2	VARCHAR	128	Yes
	CITY	VARCHAR	128	Yes
	STATE	VARCHAR	128	Yes
	POSTCODE	VARCHAR	10	Yes
	COUNTRY	VARCHAR	128	Yes
	CLOSE_STATUS	SMALLINT	2	No
	OPEN_DATE	TIMESTAMP	10	No
	CLOSE_DATE	TIMESTAMP	10	Yes

Table 70. PASSWORDS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PASSWORDS	USERKEY	INTEGER	4	No
	PASSWORD	VARCHAR	100	No
	UPDATED	TIMESTAMP	10	No

Table 71. PERMISSIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PERMISSIONS	PERMISSIONKEY	INTEGER	4	No
	DEFAULTEXPLICIT	INTEGER	4	No
	GROUPKEY	INTEGER	4	No
	GAKEY	INTEGER	4	Yes
	ACTIONKEY	INTEGER	4	No
	DENYACCEPT	INTEGER	4	No
	START_DATE	TIMESTAMP	10	Yes
	END_DATE	TIMESTAMP	10	Yes
	REPEATS	INTEGER	4	Yes
	WEEK_DAYS	VARCHAR	40	Yes
	STR_VALUE	VARCHAR	255	Yes
	INT_VALUE	INTEGER	4	Yes
	LIVE_STATE	INTEGER	4	Yes

Table 72. PERMISSIONSET table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PERMISSIONSET	ACTIONKEY	INTEGER	4	No
	ACTIONSTATE	INTEGER	4	No
	INT_VALUE	INTEGER	4	Yes
	LIVE_STATE	INTEGER	4	Yes
	PRIORITYLEVEL	INTEGER	4	Yes
	SETNAMEKEY	INTEGER	4	Yes
	STR_VALUE	VARCHAR	10	Yes

Table 73. PERMISSIONSETNAMES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
PERMISSIONSETNAMES	CREATED	TIMESTAMP	10	No
	SETNAME	VARCHAR	80	Yes
	SETNAMEKEY	INTEGER	4	No

Table 74. QUERY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUERY	QUERYKEY	INTEGER	4	No
	NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	120	Yes
	SQL_DATA	CLOB	524288	No
	FONTSIZE	INTEGER	4	No
	AUTHORITY	CHARACTER	1	No
	DISPLAY	INTEGER	4	No

Table 74. QUERY table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	REFRESH	INTEGER	4	No
	CREATOR	VARCHAR	20	Yes
	CREATED	TIMESTAMP	10	No

Table 75. QUERY_COL_INFO table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUERY_COL_INFO	QUERYKEY	INTEGER	4	No
	NAME	VARCHAR	30	No
	DISPLAYCOL	INTEGER	4	No
	DISPLAYDATA	INTEGER	4	No
	"ALIAS"	VARCHAR	30	Yes
	ACTION1	VARCHAR	150	Yes
	ACTION2	VARCHAR	150	Yes
	ACTION3	VARCHAR	150	Yes
	ACTION_LOGO	VARCHAR	20	Yes
	ACTION_LOGO2	VARCHAR	20	Yes
	ACTION_LOGO3	VARCHAR	20	Yes
	ACTION_POPUP	VARCHAR	200	Yes
	ACTION_POPUP2	VARCHAR	200	Yes
	ACTION_POPUP3	VARCHAR	200	Yes
	COLOUR	VARCHAR	10	Yes
	ALIGN	VARCHAR	10	Yes
	SUMMARY	VARCHAR	10	Yes
	POPUP	VARCHAR	200	Yes
	DELETEABLE	INTEGER	4	Yes
	AUTHORITY	CHARACTER	1	No

Table 76. QUERY_GROUP table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
QUERY_GROUP	QUERYKEY	INTEGER	4	No
	GROUP_NAME	VARCHAR	50	No

Table 77. REMOTE_INSTALL table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
REMOTE_INSTALL	INSTALLKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No
	INSTALL_TIME	TIMESTAMP	10	No
	TARGET	VARCHAR	100	No
	TARGET_USER	VARCHAR	40	No
	TARGET_PLATFORM	CHAR	7	No
	TARGET_GROUP	VARCHAR	40	No

Table 77. REMOTE_INSTALL table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	SERVER_URL	VARCHAR	200	No
	LISTENING_PORT	INTEGER	4	No
	INSTALL_FOLDER	VARCHAR	255	No
	TEMP_FOLDER	VARCHAR	255	No
	USE_FIPS	INTEGER	4	No
	ALLOW_P2P	INTEGER	4	No
	ALLOW_P2P_FAILOVER	INTEGER	4	No
	PROXY_ADDRESS	VARCHAR	200	Yes
	PROXY_PORT	INTEGER	4	Yes
	PROXY_USER	VARCHAR	40	Yes
	STATUS	VARCHAR	20	No
	ERROR	CLOB	Unlimited	Yes

Table 78. SESSIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSIONS	SESSIONKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No
	HWKEY	INTEGER	4	No
	REQUEST_TIME	TIMESTAMP	10	Yes
	START_TIME	TIMESTAMP	10	Yes
	END_TIME	TIMESTAMP	10	Yes
	DESCRIPTION	VARCHAR	512	Yes

Table 79. SESSIONS_ACTIVE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSIONS_ACTIVE	SESSIONKEY	INTEGER	4	No
	SESSION_TOKEN	VARCHAR	265	Yes
	CONTROLLER_NAME	VARCHAR	256	Yes
	HWKEY	INTEGER	4	No
	STATUS	SMALLINT	2	No
	COLLAB_IP	VARCHAR	255	Yes
	COLLAB_PORT	INTEGER	4	Yes

Table 80. SESSION_AUDIT table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_AUDIT	AUDITEVENTKEY	INTEGER	4	No
	SESSIONKEY	INTEGER	4	No
	LOCALTIMESTAMP	TIMESTAMP	10	Yes
	ORIGINATOR	SMALLINT	2	Yes
	EVENTID	VARCHAR	25	Yes
	ARGUMENT0	VARCHAR	255	Yes
	ARGUMENT1	VARCHAR	255	Yes

Table 80. SESSION_AUDIT table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	ARGUMENT2	VARCHAR	255	Yes
	ARGUMENT3	VARCHAR	255	Yes
	ARGUMENT4	VARCHAR	255	Yes
	ARGUMENT5	VARCHAR	255	Yes
	ARGUMENT6	VARCHAR	255	Yes
	ARGUMENT7	VARCHAR	255	Yes
	ARGUMENT8	VARCHAR	255	Yes
	ARGUMENT9	VARCHAR	255	Yes

Table 81. SESSION_BROKER table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_BROKER	SESSIONID	VARCHAR	64	No
	REQ_USERID	INTEGER	4	No
	REQ_IP	VARCHAR	64	Yes
	TARGET_HWKEY	INTEGER	4	No
	REQ_TIME	TIMESTAMP	10	Yes

Table 82. SESSION_POLICIES table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_POLICIES	SESSIONKEY	INTEGER	4	No
	POLICY_NAME	VARCHAR	25	No
	POLICY_VALUE	VARCHAR	25	Yes

Table 83. SESSION_RECORDING table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_RECORDING	RECORDINGKEY	INTEGER	4	No
	SESSIONKEY	INTEGER	4	No
	FILENAME	VARCHAR	255	Yes

Table 84. TRANSLATIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TRANSLATIONS	NAME	VARCHAR	48	No
	"LOCALE"	VARCHAR	16	No
	VALUE	VARCHAR	128	No

Table 85. TRUSTED_CERTS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
TRUSTED_CERTS	SUBJECT	VARCHAR	256	No
	PEM_DATA	VARCHAR	1500	No
	CERTKEY	INTEGER	4	No

Table 86. USERPERMISSIONSDEFAULT table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USERPERMISSIONSDEFAULT	USERPERMDEFKEY	INTEGER	4	No
	ACTIONKEY	INTEGER	4	No
	ACTIONSTATE	INTEGER	4	Yes
	INT_VALUE	INTEGER	4	Yes
	STR_VALUE	VARCHAR	255	Yes

Table 87. USERPERMISSIONSDEFAULTNAME table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USERPERMISSIONSDEFAULTNAME	USERPERMDEFKEY	INTEGER	4	No
	DEFDESC	VARCHAR	1024	Yes

Table 88. USERS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USERS	USERKEY	INTEGER	4	No
	USERID	VARCHAR	70	No
	EMAIL	VARCHAR	70	No
	TITLE	VARCHAR	5	Yes
	FORENAME	VARCHAR	30	Yes
	SURNAME	VARCHAR	30	Yes
	INITIALS	VARCHAR	30	Yes
	NICKNAME	VARCHAR	30	Yes
	COMPANY	VARCHAR	40	Yes
	LOCATION	VARCHAR	60	Yes
	DEPARTMENT	VARCHAR	60	Yes
	FLOOR	VARCHAR	40	Yes
	ROOM	VARCHAR	40	Yes
	TEAM	VARCHAR	60	Yes
	ORG	VARCHAR	60	Yes
	EMPLOYEEID	VARCHAR	30	Yes
	MAILPOINT	VARCHAR	10	Yes
	ADDRESS_1	VARCHAR	100	Yes
	ADDRESS_2	VARCHAR	100	Yes
	TOWN	VARCHAR	40	Yes
	POSTCODE	VARCHAR	10	Yes
	COUNTRY	VARCHAR	25	Yes
	STATE	VARCHAR	25	Yes
	REGION	VARCHAR	25	Yes
	TEL_NO	VARCHAR	25	Yes
	MOB_NO	VARCHAR	25	Yes
	CID	VARCHAR	8	Yes

Table 88. USERS table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	BUILDING	VARCHAR	64	Yes
	CITY	VARCHAR	64	Yes
	GEO	VARCHAR	64	Yes
	AUTHORITY	CHARACTER	1	Yes
	COST_CENTRE	VARCHAR	30	Yes
	"LOCALE"	VARCHAR	30	Yes
	PASSWORD	VARCHAR	100	No
	EXPIRED	CHARACTER	1	No
	DEMOGRAPHICS_STALE	INTEGER	4	No
	PASSWORD_CHANGED	TIMESTAMP	10	Yes
	LAST_UPDATE	TIMESTAMP	10	Yes
	CREATED	TIMESTAMP	10	No
	ASSIGNMENT_DATE	TIMESTAMP	10	Yes
	START_DATE	TIMESTAMP	10	Yes

Table 89. USER_ACCESS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_ACCESS	USERKEY	INTEGER	4	No
	SUCCESS	INTEGER	4	Yes
	DATE_TIME	TIMESTAMP	10	No

Table 90. USER_ACCOUNTS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_ACCOUNTS	HWKEY	INTEGER	4	No
	REVISION	INTEGER	4	No
	USERID	VARCHAR	100	No
	USERNAME	VARCHAR	100	Yes
	PW_SET	VARCHAR	7	Yes
	PW_AGE	INTEGER	4	Yes
	USER_PRIVILEGE	VARCHAR	100	Yes
	DISABLED	VARCHAR	7	Yes
	PW_NOT_REQUIRED	VARCHAR	5	Yes
	CANNOT_CHANGE_PW	VARCHAR	5	Yes
	LOCKED_OUT	VARCHAR	5	Yes
	PW_NEVER_EXPIRES	VARCHAR	5	Yes
	PW_EXPIRED	VARCHAR	5	Yes

Table 91. USER_AUTHENTICATION_KEY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_AUTHENTICATION_KEY	USERKEY	INTEGER	4	No

Table 91. USER_AUTHENTICATION_KEY table (continued)

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
	KEY_TYPE	INTEGER	4	No
	UNIQUE_KEY	VARCHAR	50	Yes
	CREATED	TIMESTAMP	10	No

Table 92. USER_AUTHORITY table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_AUTHORITY	USERKEY	INTEGER	4	No
	AUTHTYPE	VARCHAR	20	No
	AUTHORITY	CHARACTER	1	No

Table 93. USER_GROUP table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_GROUP	GROUPKEY	INTEGER	4	No
	NAME	VARCHAR	50	No
	DESCRIPTION	VARCHAR	128	Yes
	HASRULE	SMALLINT	2	No
	RULE	VARCHAR	128	Yes
	CREATED	TIMESTAMP	10	No
	USERPERMDEFKEY	INTEGER	4	Yes

Table 94. USER_INFO table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_INFO	USERKEY	INTEGER	4	No
	CUSTOM1	VARCHAR	250	Yes
	CUSTOM2	VARCHAR	250	Yes
	CUSTOM3	VARCHAR	250	Yes
	CUSTOM4	VARCHAR	250	Yes
	CUSTOM5	VARCHAR	250	Yes
	CUSTOM6	VARCHAR	250	Yes
	CUSTOM7	VARCHAR	250	Yes
	CUSTOM8	VARCHAR	250	Yes
	CUSTOM9	VARCHAR	250	Yes

Table 95. USER_PREFERENCE table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
USER_PREFERENCE	USERKEY	INTEGER	4	No
	ATTRIBUTE	VARCHAR	100	No
	VALUE	VARCHAR	100	No

Chapter 32. Troubleshooting and Help

This section is intended to help you solve problems that might occur when using the IBM Endpoint Manager for Remote Control Server program. Error Messages which might occur during a remote control session can be found in the IBM Endpoint Manager for Remote Control Controller User's Guide

Recovering when the program is not running

If, after typing the IBM Endpoint Manager for Remote Control URL in your browser, the logon page does not display, you can check to see if the IBM Endpoint Manager for Remote Control-server service is running on the IBM Endpoint Manager for Remote Control Server by doing the following :

- Within **Control Panel**, select **Administrative Tools** then **Services**
- Scroll down to the entry for IBM Endpoint Manager for Remote Control- server and check if its status is **Started**
- If not, right-click this entry and select **Start**
- If the status is Started, right-click, select **Stop** then restart it again as above
- Type the IBM Endpoint Manager for Remote Control URL in your browser. The logon page should be displayed.

Login failure

When you cannot logon to the IBM Endpoint Manager for Remote Control server you can try the following options.

Login failure when there is no LDAP/AD authentication

- Verify that the database is up and confirm that the application can connect to it. If there is a connection issue, this is logged in the `trc.log` file

  This file can be found in the IBM Endpoint Manager for Remote Control server installation directory, specified at installation. For details, see the IBM Endpoint Manager for Remote Control Installation Guide .
- Restart the database, then restart the IBM Endpoint Manager for Remote Control server service

Login failure when LDAP /AD authentication is enabled

Verify that the IBM Endpoint Manager for Remote Control admin account can log on locally . If the admin user can logon locally then there may be a connectivity problem between IBM Endpoint Manager for Remote Control and LDAP. Again the `trc.log` file can be accessed to see what errors have occurred.

Note: The default admin userid within the IBM Endpoint Manager for Remote Control Application will always authenticate against the IBM Endpoint Manager for Remote Control database regardless of whether LDAP authentication is enabled.

Using log files to solve a problem

The IBM Endpoint Manager for Remote Control components have log files which can provide extra information when troubleshooting an issue.

Obtaining the server log files

You can use the log file in theIBM Endpoint Manager for Remote Control Server program to troubleshoot problems you encounter.

To view a log of all server and database activities, click **Admin** > **View Application Log**. The content of the Application Log is displayed on the screen. To see the most recent activities, scroll to the bottom of the file.

Note: From the Admin menu, select **Send Application Log**, to open or save the application log file, `trc.log`, for attaching to an email.

Log4j logging

The log4j package is used to provide additional logging information and this can be useful when trying to debug a problem using the application log file. The level of logging can be controlled by the property values in the `log4j.properties` file. For more details, see Chapter 21, "Editing the properties files," on page 171. The following levels of logging are available:

- ALL
- DEBUG
- INFO . This is the default value
- WARN
- ERROR
- FATAL
- OFF

To obtain more information for debug purposes complete the following steps

1. Click **Admin** > **Edit properties file**
2. Select **log4j.properties** from the list
3. Set **`log4j.logger.com.ibm=DEBUG,`** Set this value to log information from debug messages to fatal messages.
4. Click **Submit**.
5. Restart the IBM Endpoint Manager for Remote Control- server service
6. Perform the steps that are causing a problem with the application.
7. Click **Admin** > **View Application Log** to view the log information or select **Send Application Log** to save the log file.

There might be multiple copies of trc log files. All of these log files are helpful when debugging a problem and can be sent to the support team when you have a problem. The value of **`log4j.logger.com.ibm`** must be set back to **INFO** when finished.

Obtaining the controller log files

You can create log files on the controller system for debugging a problem by creating a system variable. When this is created the events that take place during a remote control session are logged on the controller system.

To obtain the log file complete the following steps:

1. Create a system variable on the controller system called *TRC_TRACE* and set it to `Yes`.
2. Start a session with the required target.

3. Carry out the required actions and end the session.
4. On the controller system navigate to the home directory and a `trctrace`*XXXXX*`.log` file should be present, where *XXXXX* is the date and time stamp when the file was created.

Obtaining the target log files

You can create log files on the target system for debugging a problem by configuring the target variable *DebugTrace*.

Windows systems

1. Edit the target registry and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\Tivoli\Remote Control\Target`

   Note: On a 64 bit system all the 32-bit registry keys are under the WOW6432Node key. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\IBM\Tivoli Remote Control\Target`
2. Right-click **DebugTrace** and select **Modify**
3. Set the value to `YES` and click **OK**.
4. Restart the target service.
5. Start a session with the required target and perform the steps required for creating the problem.
6. End the session.

   The log files are found in the location defined by the **WorkingDir** property in the target registry.

Linux systems

1. Edit the `ibmtrct.conf` file
2. Set the value of **DebugTrace** to `YES` and save the file.
3. Start a session with the required target and perform the steps required for creating the problem.
4. End the session.

   The log files are found in the location defined by the **WorkingDir** property in the `ibmtrct.conf` file.

The following log files are created:

- `trc_base.txt`
- `trc_dsp.txt`
- `trc_gui.txt`

Note: When you finish gathering log files, set the value of **DebugTrace** to No and restart the target service.

Obtaining the gateway log files

The gateway log file can be used for debug purposes when you have an issue in your environment and gateways have been configured.

The name of the log file is `TRCGATEWAY-`*`hostname-suffix`*`.log` where *hostname* denotes the computer name or host name of the system hosting the gateway and *suffix* denotes the date and time, depending on which rotation and rollover settings are being used. For more information about the log, see “Managing Gateway logs” on page 162.

The log file is located in the following directories:

Windows systems

On Windows 2000, Windows XP, and Windows 2003 operating systems

```
Documents and Settings\All Users\ Application Data\IBM\Tivoli\Remote
Control\Gateway
```

On Windows Vista operating system and later

```
\ProgramData\IBM\Tivoli\Remote Control\Gateway
```

Linux systems

```
/var/opt/ibm/trc/gateway
```

Obtaining the broker log files

The broker log file can be used for debug purposes when you have an issue in your environment and brokers have been configured.

The name of the log file is `TRCICB-`*`hostname-suffix`*`.log` where *hostname* denotes the computer name or host name of the system hosting the broker and *suffix* denotes the date and time, depending on which rotation and rollover settings are being used. For more information about the log, see "Managing Gateway logs" on page 162.

The broker log files are located in the `\Broker` directory within the brokers's working directory.

Windows systems

On Windows 2000, Windows XP, and Windows 2003 operating systems

```
Documents and Settings\All Users\ Application Data\IBM\Tivoli\Remote
Control\Broker
```

On Windows Vista operating system and later

```
\ProgramData\IBM\Tivoli\Remote Control\Broker
```

Linux systems

```
/var/opt/ibm/trc/broker
```

Setting up the Trusted Sites zone

If you encounter problems loading the IBM Endpoint Manager for Remote Control Web pages while running Windows XP with Service Pack 2, you may need to add your IBM Endpoint Manager for Remote Control Server IP address to your Trusted Sites list.

To add the IBM Endpoint Manager for Remote Control program to the Trust Sites zone, perform the following steps:

1. In Internet Explorer, click **Tools** > **Internet Options**.
2. Click the **Security** tab.
3. Click **Trusted sites**.
4. Click the **Sites...** button.
5. Clear the check box beside **"Require server verification (https:) for all sites in this zone"**.
6. Type the server address in the **"Add this Web site to the zone:"** field.
7. Click **Add**.

8. Click **OK** and then load or reload the IBM Endpoint Manager for Remote Control Server pages.

Targets unable to contact the server successfully and a session cannot be established with these targets

Symptom

Targets cannot contact the server successfully and a session cannot be established with the targets.

Causes

The target may not have the correct web address for the server or the host name part of the web address, which it uses to contact the server, does not match the common name in the server's SSL certificate.

Solution

After you install the target software the target tries to contact the server. It uses http or https, and the server web address that you 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 needs to have the correct web address for the server.
- The host name part of the web address must match the common name in the server's SSL certificate.

When you install the IBM Endpoint Manager for Remote Control Server by using the installation program, you must ensure that you enter the correct values in the Web server parameters window. The **upload data to server** field takes the computer name from the Windows operating system settings. The server installer program uses the field value to generate the server URL and the SSL certificate. The server URL is used to set the **`url`** property value in the `trc.properties` file. Therefore, you must specify the correct 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 uses this address to contact the server in the future. If the web address that is sent to the target is incorrect, the symptoms you will see are that the target can register once and then is unable 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 server address 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, for example, has *mytrcserver*, but on the target there is no way to translate 'mytrcserver' to the IP address of the server, then 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.location.uk.example.com*. If you use only *mytrcserver*, then 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.example.com
Address:  192.0.2.21



Type in the hostname of your server

> mytrcserver.location.uk.example.com
Server:  gbibp9ph1--31ndcr.wan.example.com
Address:  192.0.2.21

Name:    mytrcserver.location.uk.example.com
Address:  192.0.2.25



Type in the ip address of your server

> 192.0.2.25
Server:  gbibp9ph1--31ndcr.wan.example.com
Address:  192.0.2.21

Name:    mytrcserver.location.uk.example.com
Address:  192.0.2.25
```

In the example you can see that the server hostname resolves to the correct IP address.

Remotely installed targets cannot contact the server

Symptom

Remotely installed targets cannot contact the server.

Causes

The **URL** property in the `trc.properties` file does not contain the correct web address for the IBM Endpoint Manager for Remote Control server.

Solution

It is important to make sure that the **URL** property in the `trc.properties` file contains the correct web address for the IBM Endpoint Manager for Remote Control server as this property is used when targets contact the server and for determining the server to use during a remote target installation. If the **URL** property value is not correct the remote targets will not be able to contact the server successfully. Edit the `trc.properties` file and make sure that the correct value is set.

Note: If the IP address of the IBM Endpoint Manager for Remote Control server changes at any time this is not reflected in the IBM Endpoint Manager for Remote Control application, therefore it is important to make sure that the **URL** property in `trc.properties` is updated and the server restarted as the targets will try to contact the old IP address till the change to the property is made.

Extending the time period before you are logged out of the server due to inactivity

When you are logged on to the IBM Endpoint Manager for Remote Control server and there is no activity, you are logged out after a time period. You can increase this time interval.

A default time period of 30 minutes is set in the WEB. XML file that is installed with the server. You can increase the timeout value by editing the WEB. XML file.

For a server that is installed by using the server installer, the file is in the following directory, \[server installation directory]\wlp\usr\servers\trcserver\apps\ TRCAPP.ear\trc.war\WEB-INF.

For a server that is installed on a Linux operating system.

/[server installation directory]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/ trc.war/WEB-INF.

For a server that is installed on WebSphere Application Server version 8.5.

\[server installation directory]\trc_war.ear\trc.war\WEB-INF.

To increase the timeout value, complete the following steps.

1. Edit the WEB. XML file.
2. Edit the following property.

   <session-config>
   *<session-timeout>*30*</session-timeout>*
   </session-config>
3. Set the timeout value to the number of minutes.
4. Save the file.
5. Restart the server service.

Gray screen on a Windows 2003 system

When a remote desktop user uses the **/admin** or **/console** option to start a remote desktop session with a Windows Server 2003 system and a remote control user starts a remote control session before, during or after the remote desktop session, the target display cannot be captured. The result is that a gray screen is displayed in the controller window. This issue is a limitation in Windows Server 2003 operating system. Use the **Automatically reset the console after a Remote Desktop console session** attribute as a workaround to reset the Windows session either after each remote desktop session ends, or before a remote control session starts, depending on the value that is selected.

Note: The attribute is not set to any value by default.
To configure this attribute and for a definition of its values see "Creating target groups" on page 22.

Note:

1. The workaround is defined through a target group attribute and not a policy. Therefore, if you start a session immediately after you change the setting, it might not be updated in the target yet.

2. If a target belongs to more than one target group with different values for this attribute, the higher value takes precedence with **After console is logged out** having the highest value.

   For example:

   A target belongs to groups A and B. The value of the attribute is set to **`At session start`** for group A and **`After console is logged out`** for group B. Therefore, the final value that is applied to any sessions with this target is **`After console is logged out`**.
3. If an admin or console remote desktop session is in progress when the controller attempts to connect to a target, a message is displayed on the controller. The message provides details of the remote desktop user and the IP address or computer name that the session is running from.
4. The workaround can also be configured in the `trc.properties` file by using a server policy. If both the server property and target group attribute is set to different values, the target group value takes precedence over the server value.

The following messages are displayed depending on the value that selected for the properties and whether a user is logged at the target computer.

Table 96. Workaround messages

Message #1	Message ID	Message text	Message parameters
1	workaround.w2k3rdp.console.unavailable	IBM Endpoint Manager for Remote Control is unable to control this target system because the Windows console is in a Remote Desktop session with user {0} connected from {1} ({2})	{0} Remote Desktop Client's user name {1} Remote Desktop Client's computer name {2} Remote Desktop Client's IP address
2	workaround.w2k3rdp.console.reset	IBM Endpoint Manager for Remote Control is unable to control this target system because the Windows console is unavailable while it is being reset. This might take a few minutes. You can stop the Remote Control session at any time.	
3	workaround.w2k3rdp.disabled	IBM Endpoint Manager for Remote Control is unable to control this target system because the Windows console is unavailable and the automatic reset is not enabled.	
4	target.capture.failed.start	IBM Endpoint Manager for Remote Control is unable to control this target system because the display capture process failed to start.	

The following table details when the message is displayed.

Table 97. When the workaround messages are displayed

Message #1	Session 0 - user logged in	Session 0 - user logged off
The workaround is disabled	Message #1	Message #3
Reset session automatically when a remote control session is started.	Message #1	Message #2 and reset session
Reset session automatically when the remote desktop user has logged out.	Message #1	Message #2 if the reset was less than 2 minutes ago
Target not running on Windows Server 2003 - workaround does not apply #4	Message #4	Message #4

Getting Help

If you have a problem with the IBM Endpoint Manager for Remote Control Server program or have questions about a specific feature, a variety of sources are available to help you including

- Documentation
- Web Pages

Using the Documentation

Many problems can be solved without contacting IBM for assistance. If you experience a problem or have a question about the operation or functionality of theIBM Endpoint Manager for Remote Control program, begin with the online documentation

To access the online documentation, do the following

- Click **Help** > **Online Documentation**

You are taken to the IBM Endpoint Manager for Remote Control infocenter where you can select the required documents.

Accessing the IBM Endpoint Manager for Remote Control product documentation

TheIBM Endpoint Manager for Remote Control documentation site provides the latest technical information and any downloadable updates that are available.

To access the documentation, use the following web address

http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/index.jsp?/topic/com.ibm.tem.doc_9.1/remotecontrol.html

The list of IBM Endpoint Manager for Remote Control documents are listed. Explore the relevant document.

Broker troubleshooting and FAQs

This section provides some answers to questions that might arise when you are installing or using the broker functions.

Why should I install broker support in my environment?

If a target is situated outside of your enterprise network and it requires support, you must install broker support so that remote control connections can be made across the internet to the target.

Note: It should be noted that the targets should be managed by a remote control server.

What method can I use to install broker support?

If you have access to the IBM Endpoint Manager console you can use the deployment node to deploy the broker support relevant to your operating system. For more details about deploying from the console, see the IBM Endpoint Manager for Remote Control Console User's Guide.

You can also use the IBM Endpoint Manager for Remote Control Console User's Guide installation files to install broker support. For more details, see the IBM Endpoint Manager for Remote Control Installation Guide.

After I install broker support, what do I do next?

After you install the broker support, you must complete the following steps.

1. Create a broker configuration. For more information about configuring brokers, see Chapter 23, “Broker configuration,” on page 229.
2. Register your brokers in the IBM Endpoint Manager for Remote Control server. For more information about broker registration, see “Registering a broker on the server” on page 243.
3. Obtain the required certificates for your broker. For more information about certificates, see “Certificate Authority signed certificates” on page 249. You can create self-signed certificates for each broker that you install. For more information about self-signed certificates, see “Using strict verification with self signed certificates” on page 248.
4. Add the certificates to the broker. For more information about adding the certificates, see “Configuring the keystore on the broker” on page 247
5. Upload the certificates to the server truststore. For more information about uploading the certificates, see “Truststore configuration” on page 250.

Is only one broker allowed?

No, you can install multiple brokers in your environment to suit your specific requirements. For example, a possible motivation would be to provide service failover so that new sessions can continue to be serviced while one of the brokers goes down. When you have installed the brokers, you must configure them. Add the relevant connection parameters that are required to allow connections to be made between your brokers and controllers and targets. For more information about configuring endpoint connections, see “Allowing endpoints to connect to a broker” on page 230. For details about connections between a broker and other brokers, see “Support for multiple brokers” on page 231.

How do I select a target and connect to a broker?

When you start broker remote control session, do not select a target. You must use the **Start a Broker session** option in the IBM Endpoint Manager for Remote Control server GUI to initiate the session and connect to a broker. Pass the connection code to the target user. The target user can start a broker remote control session and use the connection code to make the

correct connection. For more information about starting a broker session, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

If there are multiple brokers installed which broker do I connect to?

You do not connect to a specific broker. When multiple brokers are registered in the remote control server, the list of brokers is known as the brokerlist. When you start a broker remote control session, the controller system tries to connect to each broker in the list until it makes a successful connection to one. The target system also does the same when it is connecting to a broker. If the controller and target connect to different brokers, the controller disconnects and connects to the same broker as the target. To make the connection, the controller uses the host name that is defined in the broker property **PublicBrokerURL**, on the broker that the target is connected to.

Note: The host name that is defined in **PublicBrokerURL** must match the host name that is defined in the certificate for the broker. It must also match the host name that you use to register the broker in the remote control server.
For more information about broker properties, see "Configuring the broker properties" on page 229.

What session modes are available for remote control sessions that connect through a broker?

When you start a remote control session through a broker, an Active session is initiated by default. However, if Active mode is not enabled in the session policies that are defined for the session, the next available session mode is used. The following order of precedence applies, Guidance, Monitor, Chat, File transfer. In addition, if user acceptance is enabled for the session, the target user can select a different session mode to start from the acceptance window. For more details about starting a broker session, see the IBM Endpoint Manager for Remote Control Controller User's Guide.

How do I create a certificate?

If you are using a Certificate Authority (CA) certificate, you must consult their documentation to see how the root certificate and any relevant intermediate certificates can be obtained. For self-signed certificates, you can use the key management tool iKeyman. This tool is included with IBM Endpoint Manager for Remote Control and is also available through IBM WebSphere Application Server. For more information about creating certificates, see "Creating a self signed certificate" on page 246.

What do I do if my certificate is about to expire?

You can add a certificate to the broker and to the truststore on the server. However, to allow the target to start a session through the broker it must continue to use the old certificate. The reason for this is that the target does not yet trust the new certificate, therefore it would be unable to start a session. For more information about changing to a new certificate, see Chapter 26, "Migrating to a new certificate," on page 253.

Appendix A. Gateway sample scenarios

This appendix illustrates the gateway installation and configuration in three different network scenarios to ensure communication between the three IBM Endpoint Manager for Remote Control components (target, server and controller) across firewalls and NAT environments.

Overview

There are three types of connections used between the TRC components:

- The target uses HTTP connections to the server for registration and heartbeats.
- The controller uses TRC's own protocol for remote control sessions to the target. By default, the target uses port 888.
- The controller uses HTTP connections to launch a session.

Scenario 1 - Several networks using Network Address Translation (NAT)

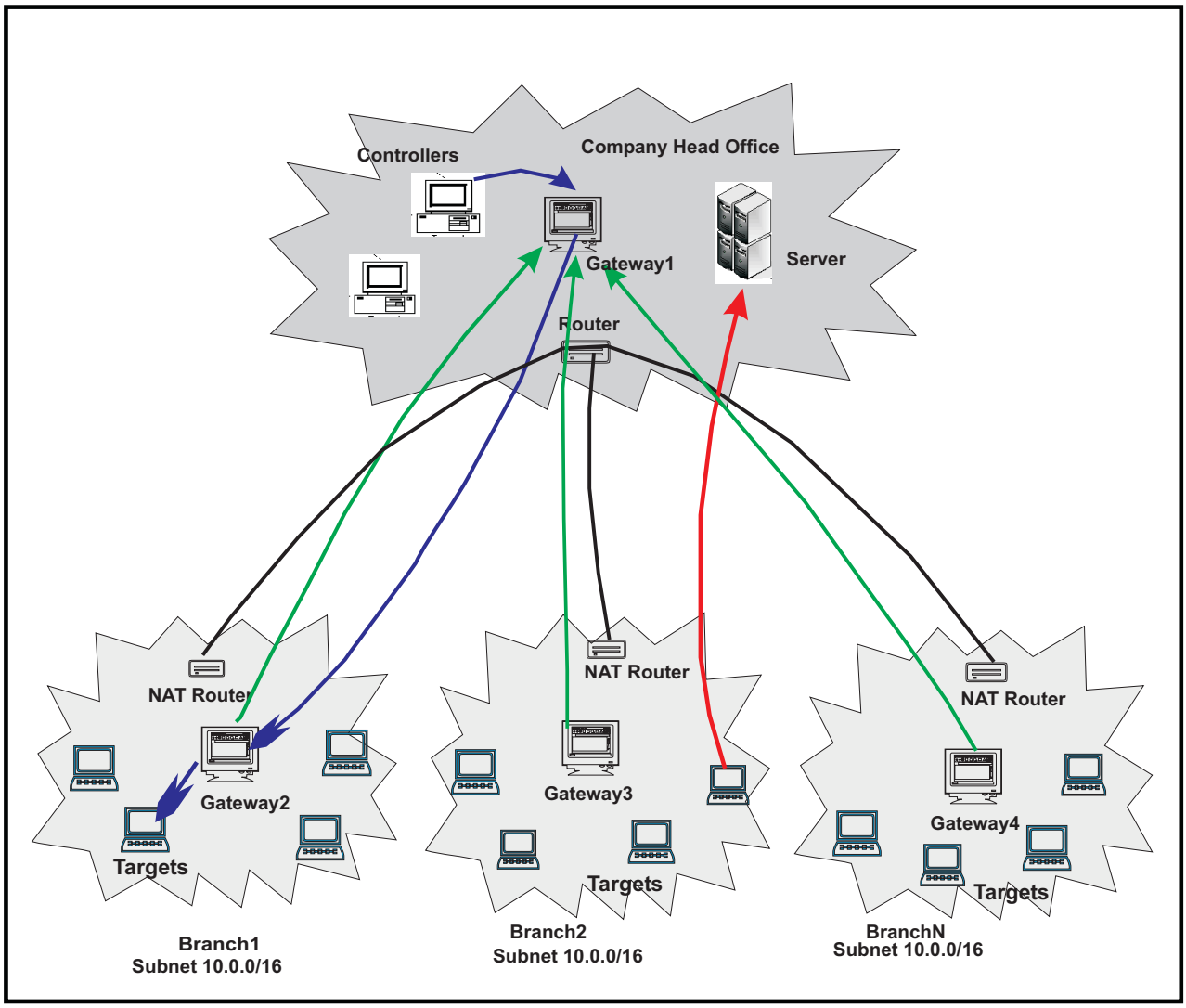

Figure 7. Several networks using NAT

In this scenario, there are multiple networks with targets in all of the networks and the controllers all in the Company Head Office. The NAT routers in the branches prevent the controllers from connecting directly to the targets in the branches and therefore, a gateway must be installed in each network.

Similarly, Gateway 1 cannot connect directly to the gateways in the branches and therefore, Gateway 2, 3 and 4 must connect to it first.

In such a scenario, Gateway 1 must be able to accept the connections from the other gateways and from controllers trying to initiate remote control sessions against targets located in other networks.

However, Gateways 2, 3, and 4 must establish a connection to Gateway 1, and must be able to locate targets in their networks.

Gateway 1 roles:

- Accept remote control connections from gateways 2, 3 and 4. The gateways in each of the branches will connect to gateway 1.
- Accept connection requests from controllers in the head office so that they can be forwarded to the gateways in the branches to allow them to locate the correct target.
- Therefore the configuration file for, *Gateway 1* will contain the following entries:

```
Inbound.1.ConnectionType = Inbound
Inbound.1.PortToListen = 8881
# Optional:
# Inbound.1.BindTo = 0.0.0.0
# Inbound.1.RetryDelay = 45
# Inbound.1.Passphrase =
Inbound.1.AllowGateways = true
Inbound.1.AllowEndpoints = true
```

Nothing else is required for Gateway 1.

The inbound connection, named **Inbound.1** in this example, will allow connections from the other gateways on port 8881. The optional parameters can be configured as required.

AllowGateways set to true, configures the gateway to accept connections from gateways 2, 3 and 4. While AllowEndpoints determines if the gateway is also going to receive controllers requests and therefore, should forward these requests to other gateways in order to locate the right target in their respective networks.

Gateway 2, 3 and 4 roles:

- Create control connection to Gateway 1.
- Locate endpoints in the branch network.
- Therefore the configuration file for, *Gateway 2, Gateway 3* and *Gateway 4* will contain the following entries:

```
Gateway.1.ConnectionType = Gateway
Gateway.1.DestinationAddress = gateway1_ipaddress
Gateway.1.DestinationPort = 8881
# Optional:
# Gateway.1.BindTo = 0.0.0.0
# Gateway.1.SourcePort = 0
# Gateway.1.RetryDelay = 45
# Gateway.1.KeepAlive = 900
# Gateway.1.Timeout = 90
# Gateway.1.Passphrase =
Endpoint.1.ConnectionType = Endpoint
# Optional
# Endpoint.1.SubnetAddress = 0.0.0.0
# Endpoint.1.SubnetMask = 0.0.0.0
# Endpoint.1.BindTo = 0.0.0.0
# Endpoint.1.SourcePort = 0
```

```
# Endpoint.1.Timeout = 90
```

In this case, there are no inbound connections because there are no controllers or gateways connecting to Gateways 2, 3 and 4. These gateways are connecting to Gateway1 and this is defined by the **Gateway.1** connection which has a connection type, gateway. The DestinationAddress of Gateway.1 is set to the IP address for Gateway1 and DestinationPort must match whatever is defined in Gateway 1 PortToListen. AllowEndpoints is set to true.

Another type of connection must be defined for these gateways, an endpoint connection (named Endpoint.1 in this example). This type of connection configures the gateway to search for a target that a controller may want to initiate a remote control session with. It is recommended to specify the subnet address and mask to reduce the amount of network traffic generated by the gateway. With the default values for the subnet, the gateway will try to connect to every single endpoint for which a request is received, even if the endpoint is in a remote network and is unreachable by the gateway.

In the trc server, you would also add **Gateway1** by clicking on **Admin** > **New TRC Gateway**. The port number would be the one defined in the **Inbound.1.PortToListen** property.

Scenario 2 - Meshed Networks

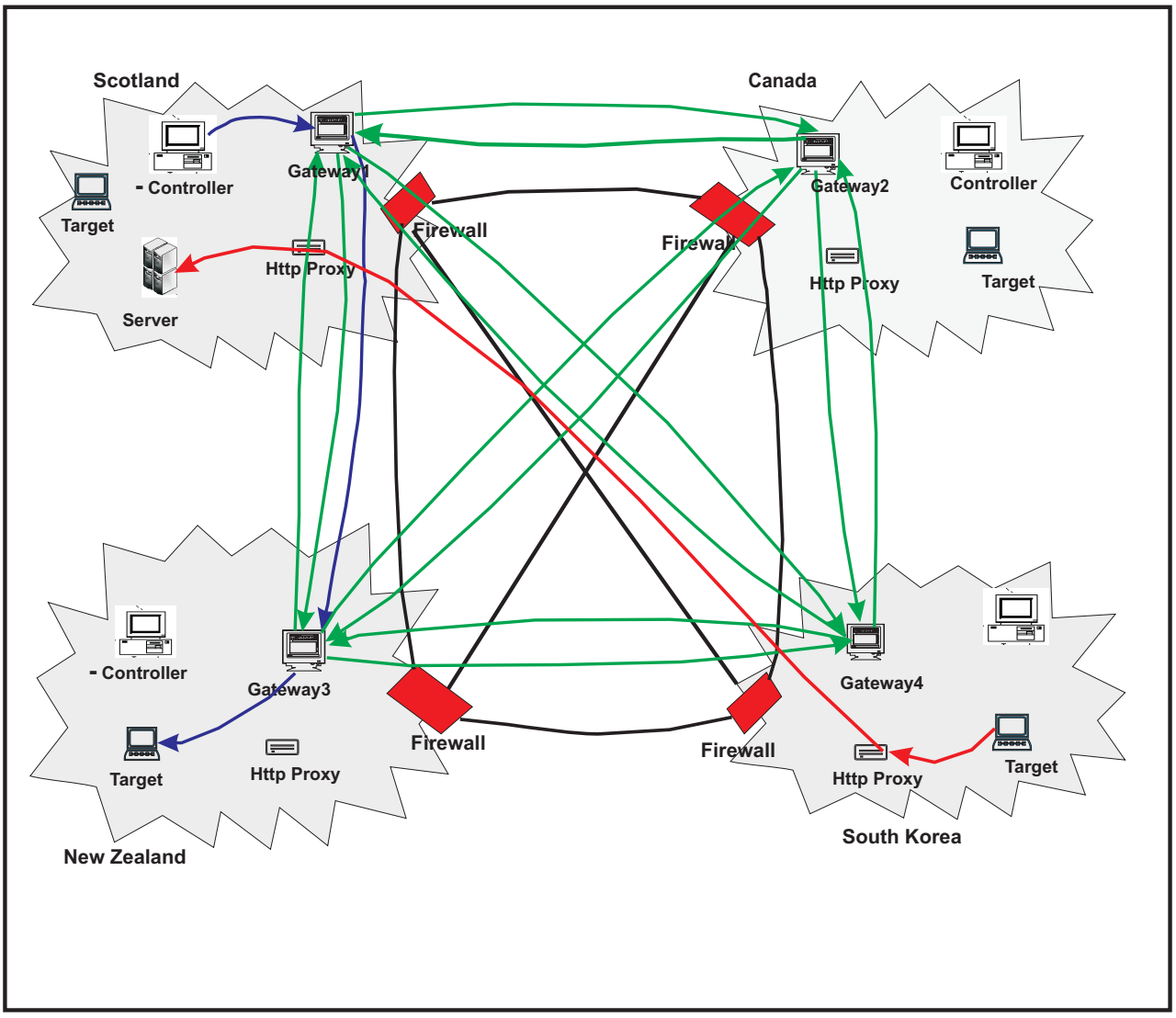

Figure 8. Meshed networks

In this scenario the targets and controllers are distributed over several locations, all of which are protected by a firewall. The firewalls prevent the controllers from connecting directly to the target in remote locations, but they do allow the gateways to connect to *gateways and gateways only*, in remote locations. The existing HTTP Proxy servers, allow the targets to connect to the server.

In this scenario, all of the gateways have the same roles:

- Create a control connection to the 3 other gateways.
- Accept control connections from the 3 other gateways.
- Accept requests from the controllers in the local network.
- Locate endpoints in the local network.

Therefore the configuration file for the gateways will contain the following entries:

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = true
```

Then for each of the gateways it has to connect to:

```
Gateway.X.ConnectionType = Gateway

Gateway.X.DestinationAddress = gatewayX_ipaddress

Gateway.X.DestinationPort = 8881

# Optional:

# Gateway.X.BindTo = 0.0.0.0

# Gateway.X.SourcePort = 0

# Gateway.X.RetryDelay = 45

# Gateway.X.KeepAlive = 900

# Gateway.X.Timeout = 90

# Gateway.X.Passphrase =

Endpoint.1.ConnectionType = Endpoint

# Optional

# Endpoint.1.SubnetAddress = 0.0.0.0

# Endpoint.1.SubnetMask = 0.0.0.0

# Endpoint.1.BindTo = 0.0.0.0

# Endpoint.1.SourcePort = 0

# Endpoint.1.Timeout = 90
```

In this scenario also, all of the gateways will be added to the server.

Scenario 3 - Web hosting

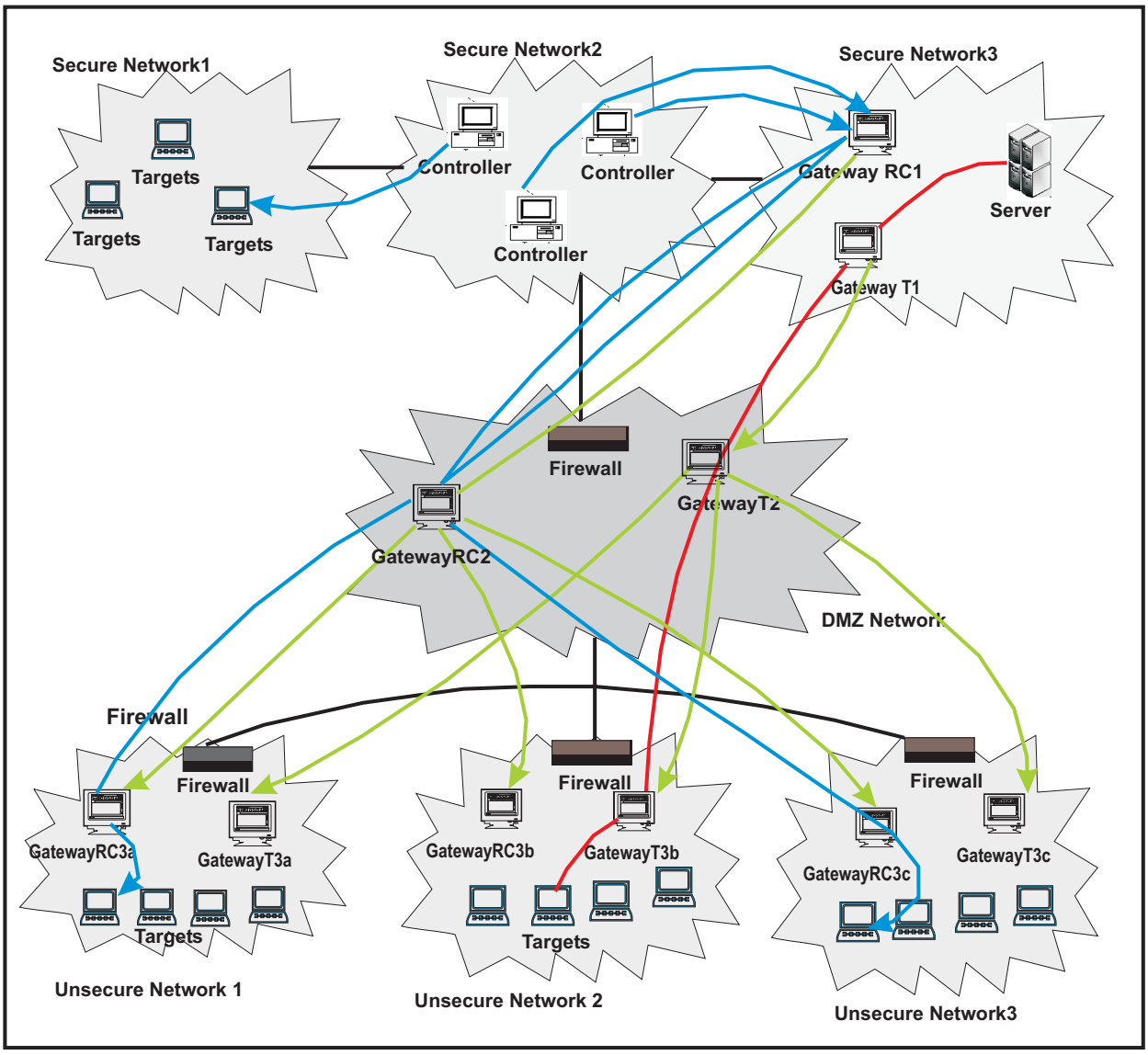

Figure 9. Webb hosting scenario

In this scenario there are two well defined networks, a secure network where the server is installed and the controllers machines are located and an unsecure network, it could be a web facing network, where servers need to be accessed for maintenance and problem resolution.

The two networks are linked by a DMZ network where two gateways, each with a specific purpose, are installed.

Additionally, HTTP proxies are not available in order to enable the targets in the unsecure network to register in the server in the secure network therefore the gateways need to establish a **tunnel** connection to allow this communication.

There are two possible scenarios:

Scenario A:

A gateway in the DMZ network is allowed to connect directly to the targets in the secured network (this scenario requires Gateway T1, Gateway T2, T3x and Gateway RC2)

In this scenario, we would add gateway RC1 to the TRC server.

Scenario B:

No traffic is allowed to the DMZ network and the gateway is NOT allowed to connect directly to the targets in the secured network (this scenario requires Gateway T1, Gateway T2, Gateway T3x, Gateway RC1, Gateway RC2 and Gateways RC3x)

In this scenario, we would add gateway RC1 to the TRC server.

The configuration for each scenario would be as follows:

Configuration common to both scenarios

Gateway T1:

- Create a control connection to Gateway T2 to be used for the tunnel.
- Create connections to the server for tunnel connections.

```
Gateway.3.ConnectionType = Gateway

Gateway.3.DestinationAddress = gatewayT2_ipaddress

Gateway.3.DestinationPort = 8881

# Optional:

# Gateway.3.BindTo = 0.0.0.0

# Gateway.3.SourcePort = 0

# Gateway.3.RetryDelay = 45

# Gateway.3.KeepAlive = 900

# Gateway.3.Timeout = 90

# Gateway.3.Passphrase =
```

Since the targets in the unsecure network cannot connect directly to the server, a **tunnel** connection must be created that will forward the heartbeats from the targets to the server:

```
Outbound.1.ConnectionType = OutboundTunnel

Outbound.1.DestinationAddress = trc_server_ip_address

Outbound.1.DestinationPort = 80

# Optional

# Outbound.1.TunnelID = TRCSERVER
```

```
# Outbound.1.BindTo = 0.0.0.0

# Outbound.1.Timeout = 90
```

Where the DestinationAddress and DestinationPort are the IP address and port of the TRC server.

Gateway T2:

Therefore the configuration file for Gateway T2 will contain the following entries, regardless of the type of scenario:

- Create connections to Gateways T3x
- Accept control connections from gateway T2.

A gateway connection must be defined for each T3 gateway, that is GatewayT3a, GatewayT3b and GatewayT3c.

```
Gateway.T3x.ConnectionType = Gateway

Gateway.T3x.DestinationAddress = gatewayT3x_ipaddress

Gateway.T3x.DestinationPort = 8881

# Optional:

# Gateway.T3x.BindTo = 0.0.0.0

# Gateway.T3x.SourcePort = 0

# Gateway.T3x.RetryDelay = 45

# Gateway.T3x.KeepAlive = 900

# Gateway.T3x.Timeout = 90

# Gateway.T3x.Passphrase =

Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = false
```

Gateways T3x:

The configuration file for Gateways T3x will contain the following entries, regardless of the type of scenario:

- Accept control connections from gateway T2.
- Accept requests from endpoints for tunnel connections to the server.

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = false

InboundTunnel.1.ConnectionType = InboundTunnel

InboundTunnel.1.PortToListen = 8880

# Optional

# InboundTunnel.1.TunnelID = TRCSERVER

# InboundTunnel.1.BindTo = 0.0.0.0

# InboundTunnel.1.RetryDelay = 45
```

Since the targets in the unsecure network cannot connect directly to the server, a **tunnel** connection must be created that will forward the heartbeats from the targets to the server.

PortToListen specifies the port that the target should connect to when connecting to the server via a tunnel. For the targets to use the tunnel, the target configuration must set the ProxyURL to:

```
trcGateway.://<gateway address>:8880
```

Scenario A

Gateway RC2

Gateway RC2 will have the following configuration:

- Accept requests from controllers in the secure network.
- Locate endpoints in the unsecure networks.

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881
```

```
# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

 Inbound.1.AllowGateways = false

Inbound.1.AllowEndpoints = true

Endpoint.1.ConnectionType = Endpoint

# Optional

# Endpoint.1.SubnetAddress = 0.0.0.0

# Endpoint.1.SubnetMask = 0.0.0.0

# Endpoint.1.BindTo = 0.0.0.0

# Endpoint.1.SourcePort = 0

# Endpoint.1.Timeout = 90
```

Scenario B

In this scenario, no traffic other than the gateways traffic is allowed outside the secure network. So we need a new gateway RC1 that will accept the requests from the controllers and pass them to RC2. Similarly, we need a new gateway RC3x in each of the unsecure networks to locate the right target.

Gateway RC1:

Gateway RC1 will have the following configuration:

- Accept requests from controllers in the secure network.
- Connect to Gateway RC2 to forward the connections requests.

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = false

Inbound.1.AllowEndpoints = true
```

```
Gateway.RC2.ConnectionType = Gateway

Gateway.RC2.DestinationAddress = gatewayRC2_ipaddress

Gateway.RC2.DestinationPort = 8881

# Optional:

# Gateway.RC2.BindTo = 0.0.0.0

# Gateway.RC2.SourcePort = 0

# Gateway.RC2.RetryDelay = 45

# Gateway.RC2.KeepAlive = 900

# Gateway.RC2.Timeout = 90

# Gateway.RC2.Passphrase =
```

Gateway RC2

In this scenario Gateway RC2 will have the following configuration:

- Accept control connections from gateway RC1.
- Connect to Gateways RC3x to forward the connections requests.

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

 Inbound.1.AllowGateways = true

 Inbound.1.AllowEndpoints = false
```

A gateway connection must be defined for each RC3 gateway (RC3a, RC3b, RC3c) where x = a, b or c.

```
Gateway.RC3x.ConnectionType = Gateway

Gateway.RC3x.DestinationAddress = gatewayT3x_ipaddress

Gateway.RC3x.DestinationPort = 8881

# Optional:

# Gateway.RC3x.BindTo = 0.0.0.0
```

```
# Gateway.RC3x.SourcePort = 0

# Gateway.RC3x.RetryDelay = 45

# Gateway.RC3x.KeepAlive = 900

# Gateway.RC3x.Timeout = 90

# Gateway.RC3x.Passphrase =
```

Gateway RC3x

These gateways are now required to locate the endpoints that before were directly accessible to Gateway RC2. The configuration file for the gateways will contain the following entries:

```
Inbound.1.ConnectionType = Inbound

Inbound.1.PortToListen = 8881

# Optional:

# Inbound.1.BindTo = 0.0.0.0

# Inbound.1.RetryDelay = 45

# Inbound.1.Passphrase =

Inbound.1.AllowGateways = true

Inbound.1.AllowEndpoints = false

Endpoint.1.ConnectionType = Endpoint

# Optional

# Endpoint.1.SubnetAddress = 0.0.0.0

# Endpoint.1.SubnetMask = 0.0.0.0

# Endpoint.1.BindTo = 0.0.0.0

# Endpoint.1.SourcePort = 0

# Endpoint.1.Timeout = 90
```

Appendix B. 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.

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

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Printed in USA