IBM Endpoint Manager for Remote Control On-demand Target Guide

Version 9.1.0

IBM Endpoint Manager for Remote Control On-demand Target Guide

Version 9.1.0

Note

Before using this information and the product it supports, read the information in "Notices" on page 71.

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

Use IBM® Endpoint Manager for Remote Control to start remote control sessions over the internet with targets that do not have the target software installed.

IBM Endpoint Manager for Remote Control provides a feature that you can use to temporarily install the target software to allow the session to be authenticated and managed by the IBM Endpoint Manager for Remote Control server.

These remote control sessions are started by using the broker component to make the connection. IBM Endpoint Manager for Remote Control provides a default web page that the target user can access to enter any required information before the target software is installed. This web page must be published on the internet. The web page is available when you have the IBM Endpoint Manager for Remote Control server component installed. However, for security, the server must not be visible on the internet. Therefore, the web page can be hosted on an internet-facing HTTP or Application server, or published through a reverse proxy. The broker can be set up as a reverse proxy. Using a reverse proxy allows access to the web page without full access to the server on the internet. For more information about using a reverse proxy, see Chapter 5, "On-demand target portal access for internet users," on page 15. You can customize the web page by adding extra input fields to it. You can also integrate the web page into your own company website.

When the target software is installed and the connection information is authenticated by the server, the remote control session starts. However, if the controller user does not have sufficient permissions to access the target, the remote control session is refused. Connections from an on-demand target can use an HTTP proxy server to reach the broker. If a proxy server is present, the proxy settings are automatically retrieved from either the Internet Explorer proxy settings or the Firefox proxy settings. If authentication is required for the proxy server, the target user is asked to enter proxy credentials before the session starts. The functions available during the remote control session are determined by server policies. At the end of the session, the target software is removed from the target computer. For more information about the functions available during a remote control session, see the *IBM Endpoint Manager for Remote Control Installation Guide*.

Note: Although a session with an on-demand target is managed by the server, the target is classed as unregistered. The target details are not saved on the server and the target software is removed at the end of the session. The policies that are used for the session are based only on the identity of the controller user.

Chapter 2. Configuring the landing page URL

IBM Endpoint Manager for Remote Control provides a default web page that a target user can access to temporarily install the target software. The URL for the web page is `http://trcserver/trc/ondemand/index.jsp`. The variable *trcserver* is the host name or IP address of your IBM Endpoint Manager for Remote Control server. The default web page is provided when you have the IBM Endpoint Manager for Remote Control server installed. You can also configure server properties to provide a URL that the target user can access. The defined URL is displayed to the controller user when they start a broker remote control session.

The property used to define the URL is **`ondemand.url`** and it is contained in the `ondemand.properties` file. To configure the property, complete the following steps:

Note: You can also manually edit the properties file. You must click **Admin** > **Reset Application** after a manual edit.

1. Log on to the server UI with a valid admin ID and password.
2. Click **Admin** > **Edit properties files**.
3. Select **ondemand.properties**.
4. Set the **`ondemand.url`** property to the relevant value.

   Leave the property blank

   When you do not want a URL to be displayed to the controller user, do not enter a value for the property.

   To display a web page

   The **`ondemand.url`** property is set to `http://localhost/trc/ondemand/index.jsp?conncode=%c` by default. Replace `localhost` with the address of your remote control server. To use a reverse proxy, replace `localhost/trc/ondemand` with the public fully qualified domain name of the broker that is configured as a reverse proxy. For example, `http://broker.example.com/index.jsp?conncode=%c`. For more information about configuring a reverse proxy, see Chapter 5, "On-demand target portal access for internet users," on page 15. If you do not replace localhost, the value that is defined for the **`ServerURL`** property in the `trc_broker.properties` file is used to create the URL that is displayed to the controller. The *%c* variable is replaced with the session connection code when the URL is displayed in the controller window. The default page requires the session connection code to be entered.

   You can also set the property to a URL for your own customized web page.

Table 1. How the URL is displayed to the controller user

ondemand.url=	**ServerURL=**	**URL is displayed as**
http://localhost/trc/ondemand/index.jsp	https://mycompany.com/trc	https://mycompany.com/trc/ondemand/index.jsp
http://www.mypage.com/ondemand/index.jsp	https://mycompany.com/trc	http://www.mypage.com/ondemand/index.jsp

Table 1. How the URL is displayed to the controller user (continued)

ondemand.url=	**ServerURL=**	**URL is displayed as**
http://www.mypage.com/index.jsp?conncode=%c	https://mycompany.com/trc	https://mypage.com/trc/ondemand/index.jsp?conncode=1234567 when the connection code is 1234567

5. Click **Submit**.
6. Click **Admin** > **Reset Application**.

The defined URL is displayed in the Connection Code window when you start a broker remote control session.

Chapter 3. Configuring custom input fields

You can add extra input fields to the default web page that is used during the process of downloading and temporarily installing the target software.

IBM Endpoint Manager for Remote Control provides a default web page that has a mandatory connection code field. You can edit server properties to add extra input fields to this web page. However, if you change the look and feel of the page, the customization is not automatically maintained if there is a server upgrade.

To create custom fields, complete the following steps:

1. Log on to the server UI with a valid admin ID and password.
2. Click **Admin** > **Edit properties file**.
3. Select **ondemand.properties**.
4. Enter values for the custom field.

   ondemand.custom.field.x.label
   Enter the display name for the field. The text that is entered for the label is displayed on the default web page.

   ondemand.custom.field.x.required
   Set a value to determine whether this field is a required field.

   True The target user must enter information in the input field.

   Note: When you set the value to true you must also define a value for the label field, otherwise the field is not displayed.

   False The target user can optionally enter information in the input field.

   For more information about the field definitions, see Chapter 19, “Ondemand properties file,” on page 61.
5. Click **Submit**.
6. Click **Admin** > **Reset Application**

The custom fields are displayed on the web page that is used to start the process for downloading and temporarily installing the target software. To add new properties, you must manually edit the properties file. After a manual edit you must click **Admin** > **Reset Application**. For more information about new property values, see Chapter 19, “Ondemand properties file,” on page 61.

Chapter 4. Creating a custom landing page

You can customize the web page that is used to start the process to download and temporarily install the target software. The web page can be integrated into your own company website.

Remote control sessions with on-demand targets require certain resources from the remote control server to be available to users through the Internet. However, it is not desirable to make the remote control server directly available to the Internet.

Therefore, because the number of resources that are required is small, several strategies can be used to enable the on-demand target function:

- Configure at least one of the brokers in your environment as a reverse proxy. This configuration allows internet users to reach a limited set of resources from the remote control server. The resources are needed exclusively to support on-demand target connections through the Internet. For more information about configuring a reverse proxy, see Chapter 5, “On-demand target portal access for internet users,” on page 15.
- Enable a separate website to be used as the portal on which to run remote control sessions with on-demand targets.

In both cases, you must edit the value of the **`ondemand.url`** property in the `ondemand.properties` file. Set the URL to refer to the external service that is providing access to the on-demand target application. You can enable a static website or a dynamic website. For more information about editing the **`ondemand.url`** property, see Chapter 2, “Configuring the landing page URL,” on page 3.

Configuring a static custom web portal

You can integrate the on-demand target function into your own website by configuring a static web portal. This type of integration requires you to copy a set of resources from the default portal on the remote control server to your external website. The website is used as a static portal on which to run on-demand sessions.

The term *static* refers to the content provided by the web server that does not change unless the files themselves are edited in the web server system.

The set of resources that are required to be copied to your website, are the files for the plug-ins and the on-demand target application. These files are copied to your website to allow all the files that are required to start an on-demand session to be downloaded from there.

The drawback of this approach is that there is no communication between the static portal and the internal remote control server. Therefore, it does not allow for providing custom data, or verifying the connection code before the remote control session is started. Because the configuration is also static, the connection code must be provided after the on-demand target is started.

The prerequisite for configuring a static portal is to have a web server already set up to provide content through the internet. You must have permissions on the web server to be able to add and edit content, and knowledge of web technologies.

To configure a static portal, complete the following steps:

1. Navigate to the following directory on the remote control server: *RC_SERVER_INSTALL_DIR*\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\ondemand

   Where: *RCSERVER_INSTALL_DIR* is the IBM Endpoint Manager for Remote Control server installation directory.
2. Copy the 9.x.x.<*version*> directories to an \ondemand directory on your own website. The directories contain the ODTJPlugin.jar, ODTIEPlugin.cab, odtffplugin.xpi, and TRCPlayer.jar files. One of the directories contains an lnx32, lnx64, and win32 directory. The contents of the directories must also be copied.
3. Create a configuration file. The configuration file must contain the details of the available brokers, specifying the list of broker host names and ports, separated by semicolons. It also contains a list of certificates that can be used to verify that the certificate presented by the broker can be trusted. Save the file with extension .properties. For example, config.properties, which contains the following entries.

   ```
   BrokerList=rcbroker.example.org:8881
   -----BEGIN CERTIFICATE-----
   Base64 encoded certificate data
   -----END CERTIFICATE-----
   ```

   where: *Base64 encoded certificate data* is the certificate data for the specific certificate. You can copy the certificate data from the IBM Endpoint Manager for Remote Control server. You must have a BEGIN CERTIFICATE and END CERTIFICATE section for each certificate that you add.

   a. Select **Admin** > **All trusted certificates**

   b. Select the required certificate.

   c. Select **Edit certificate**.

   d. Copy the certificate text to the configuration file.
4. Create HTML pages for each installation method that can be used to start the on-demand target.

   ActiveX control

   The HTML page that is used to provide the ActiveX control installation mechanism must contain a short segment of JavaScript code for launching the applet. It also contains an **<object>** tag to import the ActiveX control. The following example uses a configuration file that is named config.properties and web server rcweb.example.org. You must change the paths and file names to match your environment. In the **<head>** tag, you must add the following elements to include necessary JavaScript code.

   ```
   <script  type="text/javascript">
    function autoLaunch() {
   var ctl = document.getElementById('OnDemandCtl');
    ctl.LaunchOnDemand(
   "http://rcweb.example.org/ondemand/VERSION_NUMBER_2/win32/trc_odt.exe",
    "http://rcweb.example.org/ondemand/config.properties");
    }</script>
   ```

   Replace *VERSION_NUMBER_2* with the version number of the folder that you copied the win32 directory to in step 2. For example, "http://rcweb.example.org/ondemand/9.1.0.0035/win32/trc_odt.exe".

   The **<body>** element of the page must contain the following elements.

```
<div style="height:200px">
<object id="OnDemandCtl"
classid="CLSID:D4C0DB38-B682-42A8-AF62-DB9247543354"
codebase="ondemand/VERSION_NUMBER_1/ODTIEPlugin.cab#VERSION_NUMBER_1" ></object>
</div>
```

You must replace *VERSION_NUMBER_1* with the version number of the folder that you copied the `ODTIEPlugin.cab` file to in step 2 on page 8. For example, codebase="9.1.0.0020/ODTIEPlugin.cab#9.1.0.0020".If the target user is using Internet Explorer and ActiveX is supported and enabled, the on-demand target application is automatically downloaded and started when the HTML page is accessed.

Firefox plug-in

The HTML page that is used to provide the Firefox plug-in installation mechanism must contain the following content. The server must be configured to associate `.xpi` files with the Mime Type: "application/x-xpinstall". The method for configuring the Mime Type varies depending on the web server that you are using. The following examples use a configuration file that is named `config.properties` and web server `rcweb.example.org`. You must change the paths and file names to match your environment. Copy the `ondemand.js` and `ondemandff.js` files from the `ondemand` directory in the IBM Endpoint Manager for Remote Control server to the ondemand directory on your own website. In the **<head>** tag, you must add the following elements to include necessary JavaScript code.

```
<script  type="text/javascript" src="ondemand/ondemandff.js"></script>
<script type="text/javascript">
  function checkForPlugin() {
 ondemandFFPlugin.checkPlugin();
}
</script>
```

The **<body>** tag of the page must contain the **onload** attribute with the following content "setTimeout(checkForPlugin, 2000);".

For example,

```
<body onload="setTimeout(checkForPlugin, 2000);">
```

The **<body>** tag must also contain the following elements.

```
<form name="downloadPlugin" id="downloadPlugin"
action="ondemand/VERSION_NUMBER_1/odtffplugin.xpi"
 method="get" onSubmit="return true;"></form>

<object id="odl-params">
   <param name="config_url"
value="http://rcweb.example.org/ondemand/config.properties"/>
  <param name="odl_path"
 value="http://rcweb.example.org/ondemand/VERSION_NUMBER_2/"/>
</object>

<object id="odl-plugin-handle">
<param name="odt-plugin-version" value="VERSION_NUMBER_1">
</object>
```

Replace *VERSION_NUMBER_1* with the version number of the folder that you copied the `odtffplugin.xpi` file to in step 2 on page 8. For example, action="9.1.0.0020/odtffplugin.xpi. Replace *VERSION_NUMBER_2* with the version number of the folder that you copied the lnx32, lnx64, and win32 directories to in step 2 on page 8. If the Firefox plug-in and JavaScript are enabled when the target user is using a Firefox browser, the on-demand target application is automatically downloaded and started when the HTML page is accessed.

Java™ Applet

The HTML page that is used to provide the Applet installation mechanism must contain the following content in the **<body>** element of the page. The following example uses a configuration file that is named `config.properties` and web server `rcweb.example.org`. You must change the paths and file names to match your environment.

```
<applet archive="VERSION_NUMBER_1/ODTJPlugin.jar"
code="com.ibm.uk.greenock.odt.plugin.app.ODTJPluginApplet">
  <param name="codebase_lookup" value="false" />
  <param name="config_url"
value="http://rcweb.example.org/ondemand/config.properties"/>
  <param name="odl_path"
 value="http://rcweb.example.org/ondemand/VERSION_NUMBER_2/"/>
</applet>
```

You must replace *VERSION_NUMBER_1* with the version number of the folder that you copied the `ODTJPlugin.jar` file to in step 2 on page 8. Replace *VERSION_NUMBER_2* with the version number of the folder that you copied the lnx32, lnx64, and win32 directories to in step 2 on page 8. If Java is enabled in the target user's computer, the on-demand target application is automatically downloaded and started when the HTML page is accessed.

Java Web Start

The Java Web Start installation mechanism does not require an HTML page. It requires that a JNLP file is created. The JNLP file can be linked directly from another HTML page. When the page is accessed, it activates the Java Web Start delivery plug-in for the on-demand target application, which is downloaded and started automatically.

Use the following sample content to create the JNLP file. The example uses a configuration file that is named `config.properties` and web server `rcweb.example.org`. You must change the paths and file names to match your environment. Change 9.x.x in the title to the relevant target version.

```
<?xml version="1.0" encoding="utf-8"?>
<jnlp spec="1.0+"
 codebase="http://rcweb.example.org/ondemand/VERSION_NUMBER_1/">
<information>
 <title>IBM Endpoint Manager for Remote Control Launcher for
 On Demand target 9.x.x</title>
 <vendor>IBM</vendor>
</information>
<security><all-permissions/></security>
<resources>
 <j2se version="1.4+"/>
 <jar href="ODTJPlugin.jar"/>
</resources>
<application-desc>
<argument>--config_url</argument>
<argument>http://rcweb.example.org/ondemand/config.properties</argument>
<argument>--odl_path</argument>
<argument>http://rcweb.example.org/ondemand/VERSION_NUMBER_2/</argument>
</application-desc>
</jnlp>
```

Replace *VERSION_NUMBER_1* with the version number of the folder that you copied the `ODTJPlugin.jar` file to in step 2 on page 8. Replace *VERSION_NUMBER_2* with the version number of the folder that you copied the lnx32, lnx64, and win32 directories to in step 2 on page 8

Note: You can add the URL to the JNLP file to the custom HTML pages as a fallback URL. If the on-demand target fails to start when the target user chooses another installation method, they can click the link. The target is downloaded and started by using the Java Web Start installation method.

5. Optional: Create an HTML page that the target user can access to start the IBM Endpoint Manager for Remote Control player. The player can be used to play back a saved recording of an on-demand session. The page must contain the following element to start the player. The following example uses a web server `rcweb.example.org`. You must change the paths to match your environment.

```
<applet id="player" width="100" height="100" align="middle"
archive="VERSION_NUMBER_1/TRCPlayer.jar"
code="com.ibm.uk.greenock.ayudame.playerui.RecorderApplet">
<param name="codebase_lookup" value="false">
</applet>
```

You must replace *VERSION_NUMBER_1* with the version number of the folder that you copied the `TRCPlayer.jar` file to in step 2 on page 8. For example, `http://rcweb.example.org/ondemand/9.1.0.0020/TRCPlayer.jar`.

Configuring a dynamic custom web portal

You can integrate the on-demand target function into your own website by configuring a dynamic web portal. This type of integration allows your website to communicate with the IBM Endpoint Manager for Remote Control server through a set of service URLs.

The URLs can be used in the following ways.

- To submit custom session data to the IBM Endpoint Manager for Remote Control server, to have session data recorded.
- To validate the connection code, to check it before the on-demand target application and delivery plug-ins are downloaded.
- To retrieve the broker environment configuration dynamically and avoid having to manually edit the properties file. For example, when the set of brokers changes, or a new trusted certificate is added.

The on-demand target function requires a dynamic web to be set up because the interactions between your web server and the internal IBM Endpoint Manager for Remote Control server must be programmed into your website. Therefore, a good working knowledge of the specific dynamic web technology that is used in your environment is required.

Many different technologies can be used to implement a dynamic website. Details cannot be provided about how to achieve the required function because the necessary steps are different depending on the chosen underlying technology.

To configure a dynamic portal, complete the following steps:

1. Navigate to the following directory on the remote control server. *RC_SERVER_INSTALL_DIR*\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\ondemand

where: *RCSERVER_INSTALL_DIR* is the IBM Endpoint Manager for Remote Control server installation directory. The ondemand directory contains 9.x.x version number directories.

2. Copy the following files and directories from the latest version number directory to a version number directory on your own website.

   files `ODTJPlugin.jar`, `ODTIEPlugin.cab`, `odtffplugin.xpi`, and `TRCPlayer.jar`.

   directories
   lnx32, lnx64, and win32.

   The contents of these directories must be copied also to your website.

3. Create a page for the target user to enter the custom data and the connection code. The page can be generated by your web server. You can use the `trc/broker/OnDemandCustomDataConfig` service URL to retrieve the current set of custom data fields that are configured on the IBM Endpoint Manager for Remote Control server.

Table 2. /trc/broker/OnDemandCustomDataConfig URL

URL	**/trc/broker/OnDemandCustomDataConfig**
HTTP Method	GET
Parameters	N/A

Output	HTTP 200 OK with the following payload:
	`<response>`
	`<remotecontrol>`
	`<field name="Field1" label="Label for Field 1" required="true or false"/>`
	`<field name="Field2" label="Label for Field 2" required="true or false"/>`
	`....`
	`</remotecontrol></response>`
	The number of **`<field>`** elements that are returned depends on the configuration in the `ondemand.properties` file on the server.
	The name attribute specifies the parameter name that is expected for the field, when it is submitted back to the server.
	The label attribute specifies the display value for the locale that is requested in the HTTP request by using the Accept-Language header.
	The **`required`** attribute is a true or false value. The attribute specifies whether a value is required for this field when submitted to the IBM Endpoint Manager for Remote Control server.

When the page is submitted to the dynamic portal, the data can be sent to the IBM Endpoint Manager for Remote Control server by using the URL `broker/OnDemandSessionData`. The **`OnDemandSessionData`** URL validates the connection code and any custom data fields provided.

Note: Sending the data is required because the target user's browser cannot access the IBM Endpoint Manager for Remote Control server directly, but can only access your dynamic portal.

Table 3. /trc/broker/OnDemandSessionData URL

URL	**/trc/broker/OnDemandSessionData**
HTTP Method	POST
Parameters	conn_code

Table 3. /trc/broker/OnDemandSessionData URL (continued)

URL	**/trc/broker/OnDemandSessionData**
Output	HTTP 200 OK - If the data is correct No payload HTTP 404 - The connection code is unknown No payload HTTP 400 - The required session information is empty or not provided No payload HTTP 408 - The required session has timed out No payload

If the data is successfully submitted, the dynamic portal can redirect the target user to the page where the installation plug-in is activated.

4. Create a launching page. For information about the content for generating the pages, see step 4 on page 8. You can generate the launching page from your web server by using the `trc/broker/OnDemandSessionConfig` URL. The OnDemandSessionConfig URL returns the configuration to be used by the plug-ins. A simple page must be created that forwards the request to the server and returns the configuration data. Set the value of the **`config_url`** parameter to the URL of the page. The plug-ins then use the URL defined in the **`config_url`** parameter to retrieve the configuration from the IBM Endpoint Manager for Remote Control server.

Table 4. /trc/broker/OnDemandSessionConfig URL

URL	**/trc/broker/OnDemandSessionConfig**
HTTP Method	GET
Parameters	conn_code

Output	HTTP 200 OK - Connection code is valid
	`ConnectionCode=12345`
	`BrokerList=rcbroker.example.org:8881`
	`-----BEGIN CERTIFICATE-----`
	`Base64 encoded certificate data`
	`-----END CERTIFICATE-----`
	where: *Base64 encoded certificate data* is the certificate data for the specific certificate.
	HTTP 404 - Connection code is unknown
	No payload

.

Chapter 5. On-demand target portal access for internet users

A reverse proxy, in a DMZ, can be configured to provide access for Internet users to the on-demand portal that is on the IBM Endpoint Manager for Remote Control server in the intranet. The reverse proxy must not allow access to other sections of the IBM Endpoint Manager for Remote Control server, but only to the on-demand portal.

IBM Endpoint Manager for Remote Control provides an integrated reverse proxy for ease of deployment and configuration. The IBM Endpoint Manager for Remote Control broker component includes limited proxy functions. The integrated reverse proxy means that a broker environment can be deployed with IBM Endpoint Manager for Remote Control components only. No third-party components are required. The reverse proxy supports both HTTP and HTTPS and also supports combining HTTP and HTTPS. For example, the broker URL can be configured with HTTP protocol and the server URL in the broker properties file can be configured with HTTPS. The target user enters an HTTP on-demand URL that contains the broker host name. The reverse proxy accepts this request and uses the defined HTTPS server URL to retrieve the on-demand portal page from the server. The proxy can be used to access the on-demand portal only, it cannot be configured as a general-purpose reverse proxy. It was not designed for scalability. For deployments where heavy usage is expected, you can use an off-the-shelf reverse HTTP proxy. You can also host a custom on-demand portal on your own internet website.

Reverse proxy limitations:

- The broker supports only HTTP 1.0 and 1.1. HTTP requests with other versions result in HTTP 505 Version not supported.
- The broker supports only TLS 1.0.
- The reverse proxy cannot be used as a general purpose reverse proxy server.
- The reverse proxy cannot be used to publish other parts of the IBM Endpoint Manager for Remote Control server to the Internet. For example, the reverse proxy cannot be configured to allow targets to register or users to log in.

Configuring the broker to listen for HTTP and HTTPS connections

To configure the broker to accept HTTP and HTTPS connections, add a connection to the configuration file on the broker.

Edit the `trc_broker.properties` file to configure the connection type and parameters that are required for enabling the proxy feature on the broker.

On a Windows computer, this file is in the `\Broker` directory within the brokers's working directory.

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

If you are using a Windows 2008 server, the file is in `\ProgramData\IBM\Tivoli\Remote Control\Broker\`. In Linux systems, the file is in the `/etc` directory. For more information about broker configuration, see the *IBM Endpoint Manager for Remote Control Administrator's Guide*.

To configure the connections, complete the following steps:

- To configure the broker to accept HTTP connections:
  1. Add a connection to the configuration file by using connection type `InboundHTTP`.

     prefix.ConnectionType
     Defines the type of connection. Must be set to *InboundHTTP* or *InboundHTTP6*.

     InboundHTTP
     Listen for HTTP connections that use IPv4 addresses.

     InboundHTTP6
     Listen for HTTP connections that use IPv6 addresses.
  2. Set optional keywords if required. The connection inherits values from the default configuration, except for `PortToListen`.

     prefix.PortToListen
     The TCP port to use for listening. Default is 80.

     prefix.BindTo
     Accept incoming connections on the specified address only. Default is the `DefaultBindTo` value that is inherited from the default configuration.

     prefix.RetryDelay
     Time between attempts to open the listening port. Default is the `DefaultRetryDelay` value that is inherited from the default configuration.
- To configure the broker to accept HTTPS connections:
  1. Add a connection to the configuration file by using connection type `InboundHTTPS`.

     prefix.ConnectionType
     Defines the type of connection. Must be set to *InboundHTTPS* or *InboundHTTPS6*.

     InboundHTTPS
     Listen for HTTPS connections that use IPv4 addresses.

     InboundHTTPS6
     Listen for HTTPS connections that use IPv6 addresses.
  2. Set optional keywords if required. The connection inherits values from the default configuration, except for `PortToListen`.

     prefix.PortToListen
     The TCP port to use for listening. Default is 443.

     prefix.BindTo
     Accept incoming connections on the specified address only. Default is the `DefaultBindTo` or `DefaultBindTo6` value that is inherited from the default configuration.

     prefix.RetryDelay
     Time between attempts to open the listening port. Default is the `DefaultRetryDelay` value that is inherited from the default configuration.

prefix.TLSCertificateFile
File name and path of the broker's certificate. Default is the **DefaultTLSCertificateFile** value that is inherited from the default configuration.

prefix.TLSCertificatePassphrase
Passphrase for the broker's certificate. Default is the **DefaultTLSCertificatePassphrase** value that is inherited from the default configuration.

prefix.HTTPSCipherList
List of cipher suites that can be used to secure network connections. Default is the **DefaultHTTPSCipherList** value that is inherited from the default configuration.

Note: For more information about default broker configuration parameters, see the *IBM Endpoint Manager for Remote Control Administrator's Guide*.

Sharing a port between the reverse proxy and the broker

When a broker is configured with a reverse proxy, you can use port 443 for both reverse proxy and broker.

It is recommended that the broker is configured on port 443. The reason for this is that clients might be connecting from networks with HTTP proxies or restrictive firewall policies where outgoing connections are blocked, except for a few ports. Connections to port 443 are allowed but might be inspected to ensure that the SSL/TLS protocol is used. You can configure the broker to share port 443.

To configure a port that accepts connections from endpoints, other brokers, and HTTPS requests, configure an **Inbound** or **Inbound6** connection with port 443 and an **InboundHTTPS** or **InboundHTTPS6** connection.
For example,
1.ConnectionType = Inbound
1.PortToListen = 443
2.ConnectionType = InboundHTTPS
When the broker detects that the configuration contains two connections with the same port, **PortToListen**, and interface, **BindTo**, it automatically merges the two connections.
The exception is that an **InboundHTTP** or **InboundHTTP6** connection cannot be merged with another type of inbound connection. This limitation is because the broker does not support unencrypted and encrypted connections on the same port. When an **InboundHTTP** or **InboundHTTP6** connection is configured with the same port and interface as another type of inbound connection, the broker writes an error in the log and internally disables the **InboundHTTP** or **InboundHTTP6** connection.
Parameters for connections are merged in the following way.

Table 5. Parameter values for merged connections

Parameter	Action taken
prefix.RetryDelay	The parameter is taken from the first connection that is loaded. Parameters from subsequent connections are ignored. A warning is written to the log for each conflicting parameter.
prefix.TLSCertificateFile	
prefix.TLSCertificatePassphrase	
prefix.TLSCipherList	**HTTPSCipherList** overrides **TLSCipherList**. A warning is written to the log if the parameters conflict.

Setting the landing page URL to use a reverse proxy

When you configure a reverse proxy on your broker, the URL for the landing page is configured differently. The URL must contain the broker host name or IP address instead of the server host name and IP address.

The property that defines the URL is **`ondemand.url`** and it is contained in the `ondemand.properties` file. To configure the property, complete the following steps:

Note: You can also manually edit the properties file. You must click **Admin** > **Reset Application** after a manual edit.

1. Log on to the server UI with a valid admin ID and password.
2. Click **Admin** > **Edit properties files**.
3. Select **ondemand.properties**.
4. Set the **`ondemand.url`** property to the relevant value. The address must contain the host name or IP address of the broker that is configured with **`inboundHTTP`** or **`inboundHTTPS`** connections. For example, http://*broker.example.com*/index.jsp?conncode=%c
5. Click **Submit**.
6. Click **Admin** > **Reset Application**.

When the target user enters the defined URL into their browser, the request is sent to the proxy and passed to the server. During this process, the reverse proxy rewrites the URL to the relevant server URL so that the page can be retrieved from the server.

Chapter 6. Setting session permissions for unregistered targets

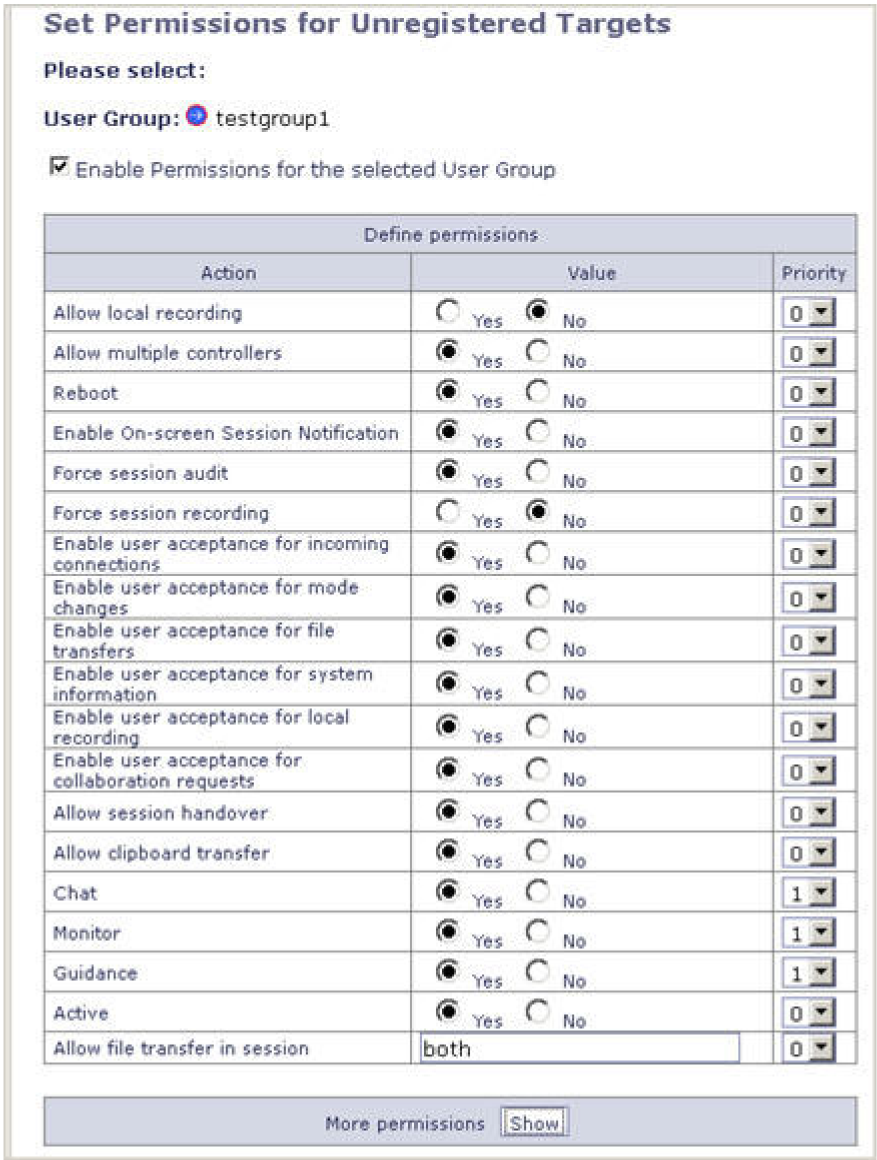
A target that participates in a broker session receives session policies from the server. These policies are resolved from the user and target group permission links that the user and target in the session are associated with. An on-demand target participates in broker remote control sessions. However, it is not registered with the server and does not belong to regular target groups. A computer that has the target software already installed, is configured with correct broker settings, and the target property `Managed` set to no is also an unregistered target. You can define session permissions for unregistered targets by using the **Set Permissions for Unregistered Targets** function.

For unregistered targets, the identity of the computer is not stored on the IBM Endpoint Manager for Remote Control server. Therefore, the target identity cannot be used to determine whether a user can start a remote control session or which policies apply.

To set policies for sessions with unregistered targets, select a user group that the controller user belongs to. Using this group, policies are resolved in the same way as for managed sessions. The policies that are defined for the user groups that the controller user belongs to are combined with the policies selected for unregistered target sessions.

To define policies for a remote control session with an unregistered target, complete the following steps:

1. Log on to the IBM Endpoint Manager for Remote Control server with a valid admin ID and password.
2. Run a report to display the user groups. You can also use the search function.
3. Select a user group.
4. Select **Set Permissions for Unregistered Targets**. The Set Permissions for Unregistered Targets panel is displayed.



Set Permissions for Unregistered Targets

Please select:

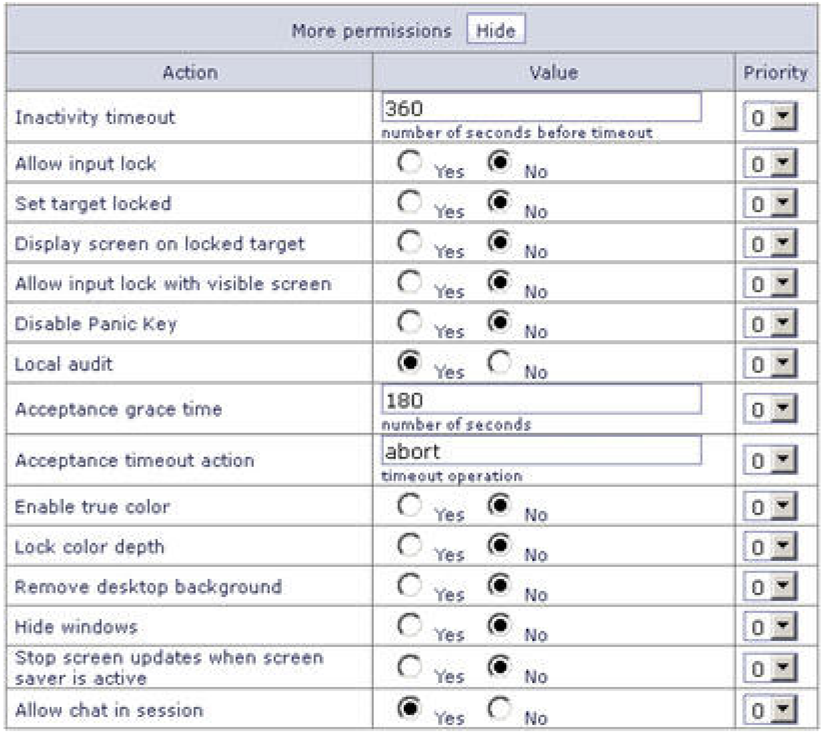
User Group: testgroup1

☑ Enable Permissions for the selected User Group

Define permissions		
Action	Value	Priority
Allow local recording	○ Yes ● No	0
Allow multiple controllers	● Yes ○ No	0
Reboot	● Yes ○ No	0
Enable On-screen Session Notification	● Yes ○ No	0
Force session audit	● Yes ○ No	0
Force session recording	○ Yes ● No	0
Enable user acceptance for incoming connections	● Yes ○ No	0
Enable user acceptance for mode changes	● Yes ○ No	0
Enable user acceptance for file transfers	● Yes ○ No	0
Enable user acceptance for system information	● Yes ○ No	0
Enable user acceptance for local recording	● Yes ○ No	0
Enable user acceptance for collaboration requests	● Yes ○ No	0
Allow session handover	● Yes ○ No	0
Allow clipboard transfer	● Yes ○ No	0
Chat	● Yes ○ No	1
Monitor	● Yes ○ No	1
Guidance	● Yes ○ No	1
Active	● Yes ○ No	0
Allow file transfer in session	both	0

5. Click the icon to select a different user group, if required.
6. To enable the policies, click **Enable Permissions for the selected User Group**.

   Note: If you clear **Enable Permissions for the selected User Group** and click **Submit**, no policies are set for this user group and unregistered targets.
7. Set values for the policies or keep the default values that are selected. You can also set a priority value for the policy. If the controller user is a member of multiple user groups, select a higher priority for policies that you want to override. For example, the controller user is a member of group1 and group2. Group2 is linked to a set of unregistered target policies that are defined with Chat = No. Group1 has Chat = Yes and priority 0. When the server gets the two conflicting values for Chat, because the user belongs to both groups, it applies the No value. Therefore, to override the group2 value of No, so that Chat is set to Yes for the session, set Chat = Yes with priority 1 for group1. For information about the policies, see Chapter 7, “Session policies for unregistered targets,” on page 23.
8. Click **Show** in the **More permissions** section to set values for extra policies if required.



More permissions [Hide]

Action	Value	Priority
Inactivity timeout	360 number of seconds before timeout	0
Allow input lock	○ Yes ● No	0
Set target locked	○ Yes ● No	0
Display screen on locked target	○ Yes ● No	0
Allow input lock with visible screen	○ Yes ● No	0
Disable Panic Key	○ Yes ● No	0
Local audit	● Yes ○ No	0
Acceptance grace time	180 number of seconds	0
Acceptance timeout action	abort timeout operation	0
Enable true color	○ Yes ● No	0
Lock color depth	○ Yes ● No	0
Remove desktop background	○ Yes ● No	0
Hide windows	○ Yes ● No	0
Stop screen updates when screen saver is active	○ Yes ● No	0
Allow chat in session	● Yes ○ No	0

9. Set a permissions schedule if required.
10. To enable the policies now, click **Submit**. To define when the selected policies are enabled, create a schedule. To create a schedule, go to step 11.
11. From the **Repeat Schedule** list, select the options and click **Submit**

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

a. Type in a Start date, in the format **yyyy-mm-dd**, or select the calendar icon to select the date.
b. Type in an End date, in the format **yyyy-mm-dd**, or select the calendar icon to select the 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 until the End date.

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

12. Click **Submit**.

Chapter 7. Session policies for unregistered targets

The set of session policies available for unregistered targets is divided into two sections. The core policies cater for remote support actions during a session. The extended policies cater for the session administration actions during a session. The core policies are always visible on the Set Permissions for Unregistered Targets screen. Click **Show** in the **More permissions** section to set values for the extended policies.

Core policies

For more information about setting session policies, see Chapter 6, "Setting session permissions for unregistered targets," on page 19.

Policy list definitions

Security policies

Reboot

To send a restart request to the target computer to allow it to be rebooted remotely. Determines whether Reboot is available as a session mode option on the start session panel.

Set to Yes

Reboot is displayed as an option on the start session panel.

Set to No

Reboot is not displayed as an option on the start session panel.

Allow multiple Controllers

To enable collaboration to allow more than one controller to join a session. Determines the availability of the collaboration option on the controller window. For details 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 in the controller window.

Set to No

The collaboration icon is not available in the controller window.

Allow local recording

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

Set to Yes

The record icon is available in the controller window.

Set to No

The record icon is not available in the controller window.

Enable On-screen Session Notification

Determines whether a semitransparent overlay is displayed on the target computer, indicating that a remote control session is in progress. Must be used when privacy is a concern to ensure that the target user is clearly notified when somebody is remotely viewing or controlling their computer.

Set to Yes

The semitransparent overlay is displayed on the target screen, together 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 can still interact with their screen.

Set to No

The overlay is not displayed on the target computer.

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

Inactivity timeout

Number of seconds to wait before the connection is automatically stopped if there is no session activity. Set this value to 0 to disable the timer and the session will not time out. The minimum time out value is 60 seconds. A value greater than 0 and less than 60 times out at 60 seconds. Values greater than 60 time out when the value is reached. The default value is 0.

Note: Inactivity time out must be set to 0 for sessions that do not involve sending or receiving information from the controller to the target.

Auditing policies

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 panel.

Set to No

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

Force session audit

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

Set to Yes

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

Set to No

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

Control policies

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 to display the user acceptance window on the target computer when the controller user selects 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 in 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 to display the user acceptance window on the target computer when the controller user selects a different session mode from the session mode list.

Set to Yes
The user acceptance window is displayed each time a session mode change is requested and 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 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 also has the option of selecting a different session mode in the 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 greater than 0 to give the target user time to accept or refuse the session.

Accept
The session starts.

Refuse
The session is not started and a message is displayed.

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

Allow clipboard transfer
Determines the availability of the **clipboard transfer** icon in the controller session window.

Set to Yes
The clipboard transfer icon is available for use in the controller window. Use this icon to 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 handover feature, 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 tries to join a collaboration session. For details about joining collaboration sessions, 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 now joins the collaboration session.

Refuse

A message is displayed to the additional controller to inform them that the target refused the session, and they do not join the collaboration session.

If the target user does not respond to the user acceptance within the time that is defined in **Acceptance Grace Time** a message is displayed to the additional controller informing them that the target has refused the session and they do not join the collaboration session.

Set to No

The user acceptance window is not displayed on the target computer after the master controller accepts to share the session for collaboration. The additional controller automatically joins the session.

Enable user acceptance for local recording

Use this feature to display the user acceptance window when a controller user clicks the record icon in the controller window. The target user must 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 window is displayed. If the target user clicks **Accept**, the controller user can select a location to save the recording to. If the target user clicks **Refuse**, a refusal message is displayed to the controller user.

After the target user accepts the request, the acceptance window is not displayed again if the controller user stops and restarts a local recording in the same session.

Set to No

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

Configuration policies

Active Determines whether the target computer can take part in active sessions and also whether Active is available as a session mode on the start session panel. For details of the Active session mode, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*.

Set to Yes

Active is available for selection as a session mode in the start session panel.

Set to No

Active is not available for selection as a session mode in the start session panel.

Guidance

Determines whether the target computer can take part in guidance sessions and also whether Guidance is available as a session mode on the start session panel. For details of 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 panel

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

Monitor
Determines whether the target computer can take part in monitor sessions and also whether Monitor is available as a session mode on the start session panel. For details about the Monitor session mode, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*.

Set to Yes
The **Monitor** option is available as a session mode on the start session panel.

Set to No
The **Monitor** option is not available as a session mode on the start session panel.

Chat Determines whether the target computer can take part in chat-only sessions and whether Chat is available as a session mode on the start session panel. For details about the Chat session mode, see the *IBM Endpoint Manager for Remote Control Controller User's Guide*.

Set to Yes
Chat is available for selection as a session mode in the start session panel.

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

Allow file transfer in session
Controls the transfer of files while in an Active session. Its value determines the availability of the **Send file** and **Pull file** options in the **File Transfer menu** within the controller window. For details 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. Files cannot be transferred.

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. Default value.

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

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

Extended policies

Policy list definitions

Security policies

Set target locked

Determines whether the local input and display are locked for all sessions. 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 in 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 about 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.

Allow input lock with visible screen

This property works both with **Allow input lock** and on its own. Use **Allow input lock with visible screen** to lock the target user's 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 user's 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 with **Set target locked**, which you can use to enable privacy mode at session startup. Use `Display screen on locked target` to determine whether or not the target user can view their screen during a remote control session, when privacy mode is enabled.

Set to Yes

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

Set to No

The target screen is not visible to the target user and the privacy bitmap is displayed during the session. The target user's mouse and keyboard input is also disabled.

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

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.

Auditing policies

Local Audit

Use to create a log of auditable events that take place during the remote control session. A `trcaudit_`*`date_time`*`.log` file is created, where *date_time* is the date and time that the session took place. For example, `trcaudit_20130805_132527.log`.

Set to Yes

Audit log is created and stored on the controller and target computer in the home directory of the currently logged on user.

Set to No

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

Control policies

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.

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. The controller displays a simulated screen saver to make the controller user aware that a screen saver is active on the remote display. The controller user can close the screen saver in the usual way 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.

Hide windows
Determines whether the **Hide windows** check box is displayed in 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 in the user acceptance window.

Set to No
The **Hide windows** check box is not displayed in the user acceptance window.

Remove desktop background
Use this policy to remove the target's desktop background image from view during a remote control session.

Set to Yes
The desktop background image on the target is not 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.

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. Default 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 with `Enable User Acceptance for incoming connections`.

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

Configuration policies

Allow chat in session

Determines whether chat functions are available while in a remote control session and also the availability of the chat icon in the controller window. For details about 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.

Policy List Values

Table 6. Acceptable and default policy values

Policy	Possible Values - Bold (shipped default)	Default value
Reboot	yes | no	yes
Allow multiple controllers	yes | no	yes
Allow local recording	yes | no	no
Set target locked	yes | no	no
Allow input lock	yes | no	no
Enable on-screen session notification	yes | no	yes
Allow input lock with visible screen	yes | no	no
Display screen on locked target	yes | no	no
Inactivity timeout	number of seconds	360
Force session recording	yes | no	no
Local audit	yes | no	yes
Force session audit	yes | no (live audit on server)	yes
Disable Panic key	yes | no	no
Enable true color	yes | no	no
Enable user acceptance for system information	yes | no	yes
Enable user acceptance for file transfers	yes | no	yes
Enable user acceptance for mode changes	yes | no	yes
Enable user acceptance for incoming connections	yes | no	yes
Allow clipboard transfer	yes | no	yes
Allow session handover	yes | no	yes

Table 6. Acceptable and default policy values (continued)

Policy	**Possible Values - Bold (shipped default)**	**Default value**
Enable user acceptance for collaboration requests	yes | no	yes
Stop screen updates when screen saver is active	yes | no	yes
Enable user acceptance for local recording	yes | no	yes
Hide windows	yes | no	no
Remove desktop background	yes | no	no
Lock color depth	yes | no	no
Acceptance timeout action	abort | proceed	abort
Acceptance Grace Time	number of seconds	180
Allow chat in session	yes | no	yes
Active	yes | no	yes
Guidance	yes | no	yes
Monitor	yes | no	yes
Chat	yes | no	yes
Allow file transfer in session	none | pull | send | both	both

Chapter 8. Defining the temporary recording directory for a broker

You can define the directory where session recordings are temporarily stored on the broker, by configuring broker properties.

For remote control sessions that involve a broker, if the **Force Session Recording** policy is enabled, the session is recorded by the broker. During the recording, the data is temporarily stored on the broker before it is uploaded to the server at the end of the session. You can define in which directory the recording is stored by adding a property to the broker configuration file. To define a recording directory, complete the following steps:

1. Edit the `trc_broker.properties` file. In the Windows operating system, the properties file is in the `\Broker` directory within the brokers's working directory.

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

   In the Windows 2008 server operating system the file is in `\ProgramData\IBM\Tivoli\Remote Control\Broker\`.

   In the Linux operating system, the file is in the `/etc` directory.
2. Add the following property.

   RecordingDir

   Use this property 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.

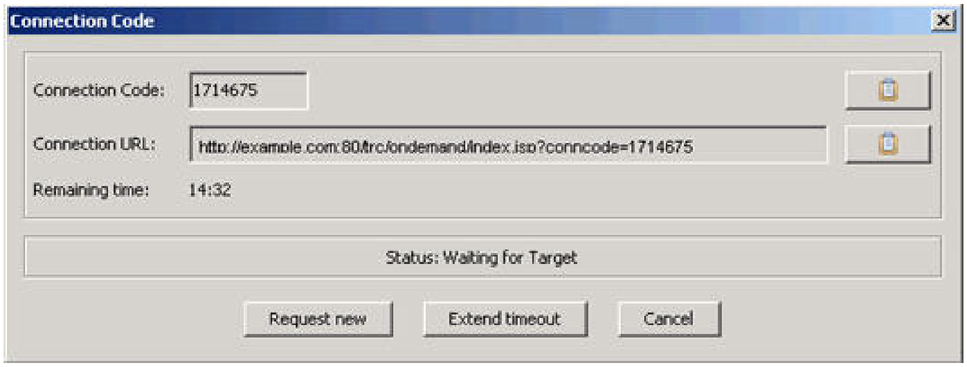
   If you do not add `RecordingDir` to the properties file, the recording is temporarily stored in the working directory of the broker.

Chapter 9. Starting a session with an on-demand target

You can start a remote control session through the internet with a target that does not have the target software already installed.

IBM Endpoint Manager for Remote Control provides a feature that you can use to obtain a URL for a web page that the target user can access to temporarily install the target software. When you start a broker session, a connection code and URL are displayed. The target user must enter the URL into their browser to proceed with the installation process. During this process, they must follow any on-screen instructions.

1. Log on to the IBM Endpoint Manager for Remote Control server with a valid ID and password.
2. Click **Targets** > **Start Broker session**. The Connection code window is displayed.

   Connection Code

   Connection Code: 1714675

   Connection URL: http://example.com:80/trc/ondemand/index.jsp?conncode=1714675

   Remaining time: 14:32

   Status: Waiting for Target

   Connection Code
   The connection code is used by the server to authenticate the session. Use the clipboard icon to copy the connection code to the clipboard.

   Connection URL
   The URL provides the target user with a web page that they can access to download and install the target software. Use the clipboard icon to copy the URL to the clipboard.

   Request new
   Click **Request new** for a new connection code.

   Extend timeout
   Click **Extend timeout** to increase the time that is allowed for the session connection to take place.

   Cancel
   Click **Cancel** to remove the connection code window. The target software is not installed and the connection to the target does not take place.
3. The connection code and URL must be given to the user on the target computer. Ask the target user to enter the URL into their browser and follow the on-screen instructions.

When the target user enters the required information, the target software installation process begins. If the controller user has the required permissions and the session is authenticated by the server, the remote control session starts. If user acceptance for the session is enabled, the target user must accept or refuse the session.

Note: If the target user refuses the session, all files and directories that are associated with the on-demand target are deleted.

Chapter 10. On-demand target installation methods

The on-demand target installation method is determined by the browser that is used by the target user and the configuration of the target computer.

When the target user enters the connection code on the landing page and clicks **I agree**, the on-demand target installation process begins automatically. The installation method that is used is first determined by the browser that the target user is using.

If Internet Explorer is being used and ActiveX is enabled, the ActiveX control installation method is used to install the target. If the browser is not enabled for using ActiveX, the target is installed by using the Java Web Start installation method.

If the target user is using Firefox, the Firefox plug-in installation method is used to install the target.

Finally, the on-demand target can also be installed by using a Java Applet.

In all cases, a launching page is displayed with specific instructions.

Note: If JavaScript is not enabled on the target computer, a launching page is displayed after the user clicks **I agree**. The target user must enable JavaScript on their computer and click **Start** on the launching page.

Downloading the on-demand target by using the ActiveX control

When the target user is using Internet Explorer and ActiveX is enabled, the on-demand target is installed and started automatically by using an ActiveX control.

After the target user clicks **I agree** on the landing page, the launching page is displayed.

The target user must follow the instructions on the page. They must follow the browser instructions and click **Install** to install the plug-in. If a User Account Control prompt is displayed, they must click **Yes**. The on-demand target executable file, with its configuration, is downloaded and installed. Any installation errors are written to a log file. For more information about the errors, see “Errors when using the ActiveX method of installation” on page 65. Before the session starts, the target user might be prompted to accept or refuse the session.

As the ActiveX control is loaded, different icons might be displayed. The icons indicate the status of the installation of the control and the loading of the on-demand target. For more information about the icons, see “On-demand target installation and loading status icons” on page 66.

If the on-demand target fails to start, click **If the on-demand target fails to start, please click here when instructed by the helpdesk agent.** The target is installed by using the Java Web Start installation method. For more information about the Java Web Start installation method, see “Downloading by using Java Web Start” on page 41.

Downloading the on-demand target by using the Firefox plug-in

When the target user is using Firefox, if the Firefox plug-in and Java Script are enabled, the on-demand target is installed and started automatically.

After the target user clicks **I agree** on the landing page, the launching page is displayed.

The target user must follow the instructions on the page. If the plug-in is already installed and does not need to be upgraded, the on-demand target executable file, with its configuration, is downloaded and installed. If the plug-in is not already installed or it must be upgraded, the target user must click **Allow** to download the files. When the file is downloaded, they must click **Install now** to install the target. If a User Account Control prompt is displayed, they must click **Yes**.

As the ActiveX control is loaded, different icons might be displayed. The icons indicate the status of the installation of the control and the loading of the on-demand target. For more information about the icons, see "On-demand target installation and loading status icons" on page 66.

If the on-demand target fails to start, click **If the on-demand target fails to start, please click here when instructed by the helpdesk agent.** The target is installed by using the Java Web Start installation method. For more information about the Java Web Start installation method, see "Downloading by using Java Web Start" on page 41.

Note: To ensure that the Firefox plug-in runs, you must be using Firefox Extended Support Release version 17.0 or later. If the Firefox plug-in is installed but is disabled, the target user is prompted to install the plug-in. The plug-in does not start because it is disabled. The target user must click **If the on-demand target fails to start, please click here when instructed by the helpdesk agent.** to continue.

Downloading the on-demand target by using the Java Applet

The on-demand target can also be installed and started automatically by using a Java applet. This option is not browser-dependent and therefore it can be used with various browsers

After the target user clicks **I agree** on the landing page, the Java applet launching page is displayed.

The target user must follow the instructions on the page. If a prompt to run the application is displayed, they must click **Run** to start the installation process. If a **User Account Control** prompt is displayed, they must click **Yes**. If the **`Enable user acceptance for incoming connections`** policy is enabled for the session, the target user is asked to accept or refuse the session. If they select **Refuse**, or do not accept in time, the session does not start. If the target user selects **Accept**, the session starts. Any errors during the installation are written to a log file. For more information about the errors, see "Errors when you are using the Java applet method of installation" on page 65.

As the Java Applet is loaded, different icons might be displayed. The icons indicate the status of the installation of the control and the loading of the on-demand target. For more information about the icons, see "On-demand target installation and loading status icons" on page 66.

If the on-demand target fails to start, click **If the on-demand target fails to start, please click here when instructed by the helpdesk agent.** The target is installed by using the Java Web Start installation method. For more information about the Java Web Start installation method, see "Downloading by using Java Web Start."

Note: The Java Applet is built with Java version 1.5. Therefore, the target user must have a browser Java plug-in of version 1.5 or later for the Java applet to run correctly.

Downloading by using Java Web Start

The on-demand target is installed and started automatically by using Java Web Start when the target user is using Internet Explorer and ActiveX is disabled. The target user can also select the Java Web Start installation method if the ActiveX, Firefox, or Java Applet installation methods fail.

After the target user clicks **I agree** on the landing page, the Java Web Start launching page is displayed.

The target user must follow the instructions on the page. If the installation process does not begin, they can also click **Start** on the launching page. If a prompt to run the application is displayed, they must click **Run** to start the installation process. If a **User Account Control** prompt is displayed, they must click **Yes.**.

Note: If Java is not installed on the target computer, the user is given the option to download and save the JNLP file. However, the system is unable to run the file.

If the `Enable user acceptance for incoming connections` policy is enabled for the session, the target user is asked to accept or refuse the session. If they select **Refuse**, or do not accept in time, the session does not start. If the target user selects **Accept**, the session starts. Any errors during the installation are displayed and the session does not start. Errors are written also to a log file.

Chapter 11. Limitations during a session with an on-demand target

Some limitations might be in effect during a remote control session with an on-demand target.

Limitations during a session

The on-demand target runs as an application. Therefore, when it is running, the following limitations might be in effect during the remote control session, depending on the user rights on the target computer.

Table 7. Limitations during a remote control session with an on-demand target

	Limitation	Windows XP	Windows Server 2003	Windows 7 Windows Server 2008 R2	Windows 8	Windows server 2012	Linux
1	Lock Screen	All Users	All Users	All Users	All Users	All Users	No
2	UAC Prompts on Secure Desktop	N/A	N/A	All Users	All Users	All Users	N/A
3	Control High Integrity Level Windows	N/A	N/A	Standard Users	Standard Users	Standard Users	N/A
4	Modern UI	N/A	N/A	N/A	Standard Users	Standard Users	N/A
5	Fast User Switching	All Users	N/A	All Users	All Users	N/A	All Users
6	Inject Ctrl+Alt+Del	All Users	All Users	Standard Users	Standard Users	Standard Users	No
7	Full screen text mode	All Users	All Users	All Users	N/A	N/A	All Users
8	Detect input from High Integrity Level Windows	N/A	N/A	All Users	All Users	All Users	N/A
9	Logging out	All Users	All Users	All Users	All Users	All Users	All Users

The following table provides descriptions for the values that are used in Table 7.

Value	Description
All Users	The limitation affects both Standard Users and Admin Users

Value	Description
Standard Users	The limitation affects Standard Users only.
N/A	The limitation is not applicable to this operating system. For example, the operating system does not have User Account Control (UAC).
No	Not a limitation on this operating system.

1. Lock Screen

   When the target system is locked during a remote control session, the following message is displayed on the controller, `"Please wait... Screen capture temporarily interrupted by the target operating system until the end user completes a secure desktop action (UAC prompt, fast user switching, screen locked). Screen capture will resume when the action is completed"`. The lock screen on the target is not displayed in the remote control session window. The controller user also loses input control.
2. UAC Prompts on Secure Desktop

   When a UAC prompt is displayed on the target system, it is not displayed to the controller in the remote control session window. Instead, the following message is displayed, `"Please wait... Screen capture temporarily interrupted by the target operating system until the end user completes a secure desktop action (UAC prompt, fast user switching, screen locked). Screen capture will resume when the action is completed"`. The limitation does not affect Windows XP, Windows Server 2003, or Linux because those operating systems do not have User Account Control.
3. Control High Level Integrity Windows

   The controller is unable to send mouse or keyboard input to windows on the target system. For example: certain Control Panels, Regedit, or Administrator Command Prompt. This limitation does not affect Windows XP, Windows Server 2003, or Linux because those operating systems do not have User Account Control.
4. Modern UI

   When the Modern UI, formerly known as Metro, is visible, the target is unable to display its user interface on top of the display. This issue affects the Start Screen and also the Modern UI style applications. The following UI functions on the target are most affected by this issue.
   - User acceptance prompts
   - On-Screen Session Notification (OSSN)
   - Guidance actions
   - Highlighting and drawing

   The taskbar is not visible also in the Modern UI. Therefore, the target's notification icon is not visible or accessible, and users cannot see whether a session is active. This limitation affects Windows 8 and Windows Server 2012 operating systems only because the Modern UI was first introduced in those versions.
5. *Fast user switching*

   When you switch to a different target user account, the following message is displayed on the controller, `"Please wait... Screen capture temporarily interrupted by the target operating system until the end user completes a secure desktop action (UAC prompt, fast user switching, screen locked). Screen capture will resume when the action is completed"`. The limitation does not apply to the Windows Server 2003 operating system because that version does not support fast user switching. Earlier versions of Linux do not support *fast user switching* either.

6. Inject Ctrl+Alt+Del

   Users cannot inject **Ctrl+Alt+Del** during a remote control session, except users with Administrator rights on Windows Vista and later. Workarounds for this limitation are detailed in "Ctrl + Alt + Del workarounds." The **Inject Ctrl+Alt+Del** menu option is not available in the **Perform action in target** menu when you are using Windows XP or Windows Server 2003.
7. Full screen text mode

   When a user switches a text mode application to full screen, the following message is displayed on the controller, `"Please wait... Screen capture temporarily interrupted by the target operating system until the end user completes a secure desktop action (UAC prompt, fast user switching, screen locked). Screen capture will resume when the action is completed"`. The full screen text is not displayed in the session window.
8. Detect input from High Integrity level windows

   When input focus is on a window with High Integrity Level, the mouse icon in the controller toolbar does not display the forbidden sign. The controller user cannot see whether the target user is using the mouse or keyboard. Input from the controller is blocked. The limitation does not affect Windows XP, Windows Server 2003, or Linux because these operating systems do not have User Account Control.
9. Logging out

   When a user logs out, all the applications that are running in that user's session are terminated. The on-demand target runs as an application, therefore it is terminated too.

If you transfer files during a remote control session, the following limitations must be noted.

Note: You cannot transfer files to directories on the target that require admin rights for writing, for example, the Program Files directory. You can transfer the file to the user's profile or temp directory, then use local tools to move the file to the correct location, for example, Windows Explorer, cmd.exe, or other tools. However, during this process, UAC prompts might be displayed which you cannot see or control because of the UAC Prompts on Secure Desktop limitation. The same limitation is in effect when you are transferring from the target to the controller.

Ctrl + Alt + Del workarounds

When you click **Ctrl-Alt-Del**, the Windows Security dialog is displayed on the secure desktop. When the dialog is displayed, the on-demand remote control session is paused because the on-demand target is not allowed to capture the secure desktop. The exception is that on Windows XP with the welcome screen enabled, Task Manager is started instead.

The Windows Security dialog provides five options. However, the controller user can select the options in other ways.

Lock workstation

In the controller window, select **Actions** > **Lock Workstation**.

Log off and shutdown
You can select these options from the **Start** menu in the Windows operating system.

Change password
You can access the change password option in Control Panel.

Task Manager
In the controller window, select **Actions** > **Task Manager**. You can also right-click the Windows taskbar.

Installation limitation when you are using Windows XP

The executable file that is used to install the on-demand target might not start in Windows XP and the following message is displayed. `A referral was returned by the server`. To fix this issue, you must install Windows update package KB931125. The package can be installed by using Windows Update and the package, Update for Root Certificates for Windows XP [May 2013] (KB931125). You can also download the package from the Microsoft Download Center.

Chapter 12. Saving a session recording on the on-demand target

As the user on an on-demand target you can save a recording of a remote control session on your computer. You can select to save the recording when you accept the session or start to record and save during the session.

The recording is saved to the target user 's home directory in the `OnDemandRecordings` directory. The format of the file name is as follows:

`trcrecording_`*`YYYYMMDD_HHMMSS`*`.trc`, where *YYYYMMDD_HHMMSS* is the time stamp of when the file was saved.

The recording file is not deleted at the end of the session.

Choose from the following ways to save a recording.

- On the session acceptance window select **Keep local recording**. The **Keep local recording** option is available if the **`Enable user acceptance for incoming connections`** policy is set for the session. The recording starts when the session begins. You can select **Actions** > **Stop local recording** to stop the recording at any point during the session.
- Select **Actions** > **Start local recording** to start recording during the session. The session activity from that point is recorded and saved to the target computer.

  Select **Actions** > **Stop local recording** to stop the recording. Each time that you click **Start local recording** during a session, a new recording file is saved to your computer.

After you save a session recording, you can play back the recording by obtaining a URL from the helpdesk agent. The URL is in the following format.

If you have access to the IBM Endpoint Manager for Remote Control server directly, the URL is `http(s)://`*`server_name:port`*`/trc/ondemand/player.jsp`, where *server_name:port* is the IP address and port of your server.

If you are accessing the page from the internet, the URL is `http(s)://`*`broker_name:port`*`/player.jsp`, where *broker_name:port* is the IP address and port of the reverse proxy.

To play back the recording, complete the following steps:

1. Enter the URL into your browser. The session recording player starts automatically.
2. If the player does not start, click **Run**.
3. Browse to your recording file and click **OK**. Recording files are saved to the `OnDemandRecordings` directory in your home directory.

Chapter 13. Handing over a broker collaboration session

If you are the master controller of a collaboration session, that involves a broker, you can pass full control of the session to another participant.

During a collaboration session, use the **Handover** function to pass full control of the session to one of the other participants in the session. They become the master controller and you can leave the session without having to end it. The availability of this function is determined by the value of the server policy **Allow session handover**.

Set to Yes
The **Hand over** button is displayed in the collaboration control panel.

Set to No
The **Hand over** button is not displayed in the collaboration control panel.

To pass control of a collaboration session to a new master controller, complete the following steps:

1. Select the required controller in the participants list, in the collaboration control panel.
2. Click **Hand over**. The outcome of the handover request is determined by the value that is set for the **`Enable user acceptance for collaboration requests`** server policy.

   If this policy is set to Yes for the session, the target user is asked to accept or refuse your request to hand over control. If they accept the request, full session control is passed to the selected controller. If they refuse, or do not respond in time, a refusal message is displayed on your screen and on the selected controllers screen. You are still the master controller of the session. Click **OK**

   Note: If the target user does not respond in time and the **`Acceptance timeout action`** server policy is set to PROCEED, control is passed to the new master controller.

   If **`Enable user acceptance for collaboration requests`** is set to No, user acceptance is not required by the target user and full session control is passed to the new master controller.

When the session is handed over to the new master controller, the collaboration control panel opens on their system. The list of participants is displayed in the collaboration control panel. You lose input control for the session. The IP address of the new master controller is displayed in the window title of your session window.

The new master controller sees the IP address of the target in the window title of their session window.

Note: The policies for the session remain as they were when the session was started. The policies do not change even although the controller user changed. The initial policies that are set for the session are valid throughout the collaboration session regardless of who is the master controller.

Chapter 14. Ending a session

When you end a session with an IBM Endpoint Manager for Remote Control on-demand target, all related files and directories are deleted.

You can end a remote control session with an on-demand target in the following ways:

- Click the **Connection** icon in the taskbar.
- Click the **X** in the upper right of the controller window.

Click **Yes** to quit the session.

The session ends and the files and directories that are associated with the on-demand target are deleted. The on-demand target binary file, the configuration file, and the installation directory, with all of its contents are deleted. The on-demand target trace file is also deleted unless you selected to save it on the target. For more information about saving the log file, see Chapter 16, “Saving the session log file,” on page 55.

The target user can press **Pause** on their keyboard or click the connection icon to end the session. If the target user closes the session, it ends immediately.

Note: If the session is interrupted by a non-user event, for example, a network failure, the trace file is not deleted. Use the trace file for debugging purposes.

Chapter 15. Ending a collaboration session when you disconnect

When you end a session in which collaboration is started, you can choose to stay in the session or disconnect from the session.

You can end a remote control session in the following ways:

- Click the **Connection** icon in the taskbar.
- Click the **X** in the upper right of the controller window.

If collaboration is started in the session and you are the master controller of the session, you are warned that collaboration is in progress. The following message is displayed. `A Collaboration session is in progress. If you disconnect, the session will end. Keep the session open?`

You can choose to disconnect and end the session or choose to remain in the session as the master controller.

Cancel

When you click **Cancel**, the collaboration session continues and you are still the master controller.

Disconnect session

When you click **Disconnect session**, the collaboration session ends and all participants are disconnected.

Chapter 16. Saving the session log file

You can save the trace log file that is created during a session with an IBM Endpoint Manager for Remote Control on-demand target.

The log file that is created when the on-demand target is installed can be used for debugging purposes. At the end of a remote control session with an on-demand target, the log file is deleted. Use the **Keep Session Log** function to save the file on the target.

In the controller window, click **Perform action in target** > **Keep Session Log** to save the log file.

The log file is saved to the user's home directory on the target computer. The file is saved in the following format:

```
trc_odt_trace_yyyymmdd_hhmmss.log
```

For example, `trc_odt_trace_20130530_095900.log`

Before the session ends, if you selected to save the session log, you can select **Perform action in target** > **Delete Session Log** to delete the log.

Note: If the target user is switched during the session, the log file is saved to the home directory of the target user who started the session.

Chapter 17. Session history for unregistered targets

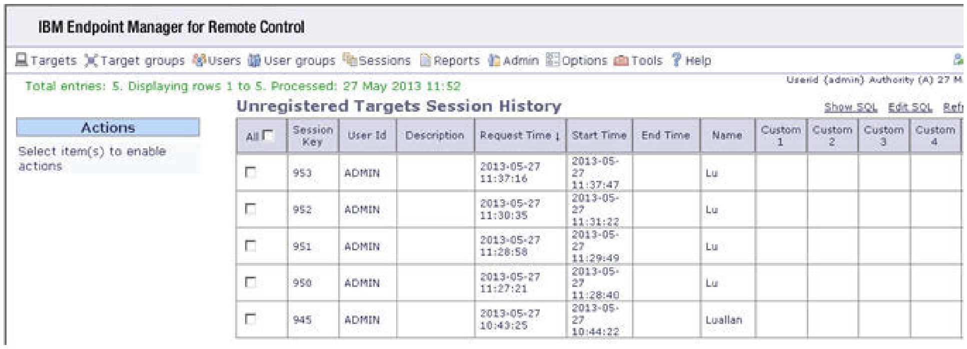
After you have participated in remote control sessions with on-demand targets, you can view the session history. Sessions that involved unregistered targets are listed in the **All Session History** report and **My Session History** report together with the registered target sessions. You can also view a list of the sessions that only involved unregistered targets.

Viewing the session history for unregistered targets

You can view the list of previous sessions by viewing the **All Session History** or **My Session History** reports. These reports contain sessions for registered and unregistered targets. The **Registered Target** column in the reports indicates whether the target in the session was registered on the IBM Endpoint Manager for Remote Control server. To view the list of sessions for unregistered targets only, use the **All Unregistered Targets Sessions** report.

To view the **All Unregistered Targets Sessions** report, complete the following steps:

1. Log on to the IBM Endpoint Manager for Remote Control server with a valid admin ID and password.
2. Select **Sessions** > **All Unregistered Targets Sessions**. The Unregistered Targets Sessions panel is displayed.


IBM Endpoint Manager for Remote Control
Targets
Target groups
Users
User groups
Sessions
Reports
Admin
Options
Tools
Help
Userid (admin) Authority (A) 27 M
Show SQL
Edit SQL
Ref
Actions
Select item(s) to enable actions

Total entries: 5. Displaying rows 1 to 5. Processed: 27 May 2013 11:52

Unregistered Targets Session History

All □	Session Key	User Id	Description	Request Time ↓	Start Time	End Time	Name	Custom 1	Custom 2	Custom 3	Custom 4
□	953	ADMIN		2013-05-27 11:37:16	2013-05-27 11:37:47		Lu				
□	952	ADMIN		2013-05-27 11:30:35	2013-05-27 11:31:22		Lu				
□	951	ADMIN		2013-05-27 11:28:58	2013-05-27 11:29:49		Lu				
□	950	ADMIN		2013-05-27 11:27:21	2013-05-27 11:28:40		Lu				
□	945	ADMIN		2013-05-27 10:43:25	2013-05-27 10:44:22		Luallan				

Note: The custom data column headings reflect the current label name that is defined in the `ondemand.properties` file for the field. The data in a column might not all be in the same format.

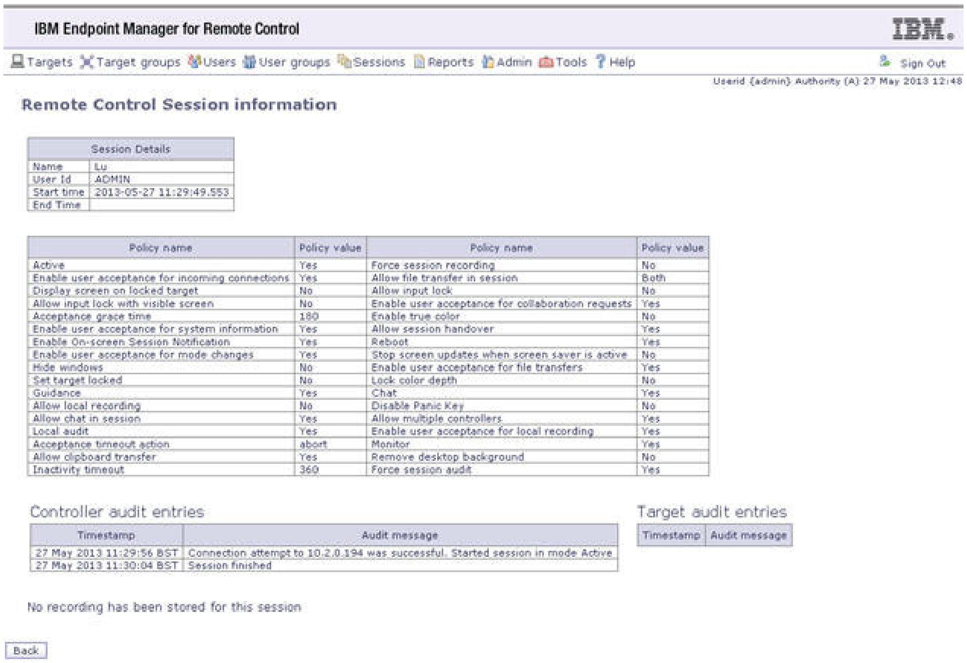
For example, if **`ondemand.custom.field.0.label= Name`** and is then changed to **`ondemand.custom.field.0.label= Email`**, the column with heading email might contain names and email addresses. For more information about the `ondemand.properties` file, see Chapter 19, “Ondemand properties file,” on page 61.

Viewing session details

Use the **Session Details** function to view details about remote control sessions with unregistered targets. You can select a session from the **Unregistered Targets Sessions History** report. Details of the session are displayed.

To view session details for a specific session, complete the following steps:

1. Click **Sessions** > **All Unregistered Targets Sessions**.
2. Select a session from the list.
3. Select **Session details** from the action list on the left.



Userid {admin} Authority (A) 27 May 2013 12:48

Remote Control Session information

Session Details	
Name	Lu
User Id	ADMIN
Start time	2013-05-27 11:29:49.553
End Time	

Policy name	Policy value	Policy name	Policy value
Active	Yes	Force session recording	No
Enable user acceptance for incoming connections	Yes	Allow file transfer in session	Both
Display screen on locked target	No	Allow input lock	No
Allow input lock with visible screen	No	Enable user acceptance for collaboration requests	Yes
Acceptance grace time	180	Enable true color	No
Enable user acceptance for system information	Yes	Allow session handover	Yes
Enable On-screen Session Notification	Yes	Reboot	Yes
Enable user acceptance for mode changes	Yes	Stop screen updates when screen saver is active	No
Hide windows	No	Enable user acceptance for file transfers	Yes
Set target locked	No	Lock color depth	No
Guidance	Yes	Chat	Yes
Allow local recording	No	Disable Panic Key	No
Allow chat in session	Yes	Allow multiple controllers	Yes
Local audit	Yes	Enable user acceptance for local recording	Yes
Acceptance timeout action	abort	Monitor	Yes
Allow clipboard transfer	Yes	Remove desktop background	No
Inactivity timeout	360	Force session audit	Yes

Controller audit entries

Timestamp	Audit message
27 May 2013 11:29:56 BST	Connection attempt to 10.2.0.194 was successful. Started session in mode Active
27 May 2013 11:30:04 BST	Session finished

Target audit entries

Timestamp	Audit message

No recording has been stored for this session

The Remote Control Session information panel is displayed. The **Session Details** section displays the custom data fields in which data was entered on the on-demand portal page, during on-demand target sessions. The user ID of the controller user is also displayed. The policies for the session are displayed and any controller or target audit events, depending on the policies that were set. If the **Force session audit** policy is set to Yes for the session, the saved audit entries are displayed. If the **Force session recording** policy is set to Yes, there is also a link to play back the recording of the session. Click **Play the recording of this session** to open the Session recording player window and play the recording.

Chapter 18. Database table definitions

Description and definition of the database tables that hold data for remote control sessions with on-demand targets. The SESSIONS_DATA table hold the data that is submitted from the default web page that is used by the target user. The SESSIONS table holds session data.

Table 8. SESSION_DATA table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSION_DATA	SESSIONKEY	INTEGER	4	No
	CUSTOM0	VARCHAR	128	Yes
	CUSTOM1	VARCHAR	128	Yes
	CUSTOM2	VARCHAR	128	Yes
	CUSTOM3	VARCHAR	128	Yes
	CUSTOM4	VARCHAR	128	Yes
	CUSTOM5	VARCHAR	128	Yes
	CUSTOM6	VARCHAR	128	Yes
	CUSTOM7	VARCHAR	128	Yes
	CUSTOM8	VARCHAR	128	Yes
	CUSTOM9	VARCHAR	128	Yes

Table 9. SESSIONS table

TABLE NAME	COLUMN NAME	TYPE NAME	LENGTH	NULLS
SESSIONS	SESSIONKEY	INTEGER	4	No
	USERKEY	INTEGER	4	No
	HWKEY	INTEGER	4	No
	REGISTERED_TARGET	CHAR	1	No
	REQUEST_TIME	TIMESTAMP	10	Yes
	START_TIME	TIMESTAMP	10	Yes
	END_TIME	TIMESTAMP	10	Yes
	DESCRIPTION	VARCHAR	512	Yes
	KNOWNUSERNAME	VARCHAR	128	Yes
	KNOWNCOMPUTERNAME	VARCHAR	255	Yes
	SESSION_TOKEN	VARCHAR	256	Yes

Chapter 19. Ondemand properties file

Edit the `ondemand.properties` file to create and configure properties for remote control sessions with on-demand targets.

The `ondemand.properties` file is used to configure properties that are used during remote control sessions with on-demand targets. You can edit the file from the server UI by clicking **Admin** > **Edit properties file**. You can also edit the file manually.

The file is located in the following directory:

Windows operating systems:
[installdir]\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes. Where *[installdir]* is the IBM Endpoint Manager for Remote Control installation directory. For example, `C:\Program Files\IBM\Tivoli\server\wlp\usr\servers\trcserver\apps\TRCAPP.ear\trc.war\WEB-INF\classes`

Linux operating systems:
[installdir]/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes. Where *[installdir]* is the IBM Endpoint Manager for Remote Control installation directory. For example, `/opt/IBM/Tivoli/server/wlp/usr/servers/trcserver/apps/TRCAPP.ear/trc.war/WEB-INF/classes`

After you edit the file, you must click **Admin** > **Reset Application**.

The **`ondemand.url`** property is set to `http://localhost/trc/ondemand/index.jsp?conncode=%c` by default. Replace `localhost` with the address of your remote control server. To use a reverse proxy, replace `localhost/trc/ondemand` with the public fully qualified domain name of the broker that is configured as a reverse proxy. For example, `http://broker.example.com/index.jsp?conncode=%c`. For more information about configuring a reverse proxy, see Chapter 5, "On-demand target portal access for internet users," on page 15. If you do not replace localhost, the value that is defined for the **`ServerURL`** property in the `trc_broker.properties` file is used to create the URL that is displayed to the controller. The *%c* variable is replaced with the session connection code when the URL is displayed in the controller window. The default page requires the session connection code to be entered.

You can also set the property to a URL for your own customized web page.

Table 10. How the URL is displayed to the controller user

ondemand.url=	ServerURL=	URL is displayed as
http://localhost/trc/ondemand/index.jsp	https://mycompany.com/trc	https://mycompany.com/trc/ondemand/index.jsp
http://www.mypage.com/ondemand/index.jsp	https://mycompany.com/trc	http://www.mypage.com/ondemand/index.jsp

Table 10. How the URL is displayed to the controller user (continued)

ondemand.url=	**ServerURL=**	**URL is displayed as**
http://www.mypage.com/ index.jsp?conncode=%c	https://mycompany.com/trc	https://mypage.com/trc/ ondemand/ index.jsp?conncode=1234567 when the connection code is 1234567

`ondemand.url=`

Modifiable field	**`ondemand.url`**
Field Description	URL for a page that the target user can access to start the process to download and temporarily install the target software.
Possible Values	User defined URL. For example, `http://localhost/trc/ondemand/index.jsp`
Value Definition	Default value is `http://localhost/trc/ondemand/index.jsp?conncode=%c`

Properties to add custom fields to the web page that is accessed from the URL that is defined in the **`ondemand.url`** property. There are four custom fields available by default. To add more custom fields, manually edit the `ondemand.properties` file.

Note: After manually editing the file, restart the server service to display the new tools on the screen.

`ondemand.custom.field.x.label=`

Modifiable field	**`ondemand.custom.field.x.label`**

Field Description	Display name that is used for the extra input fields on the default web page that is used to start a session with an on-demand target. x = 1 - 9.
	If you do not set a value for this property, the field is not displayed. For example, the following sample configuration would result in defining a custom **Name** field. The definitions for index 1 are discarded, because there is no **`ondemand.custom.field.1.label`** defined:
	ondemand.custom.field.0.label=Name
	ondemand.custom.field.1.required=true
	ondemand.custom.field.1.label.fr=Numéro de téléphone

Possible Values	User Defined. For example, `ondemand.custom.field.1.label=Name` The text, Name, is displayed on the web page menu.
Value Definition	

`ondemand.custom.field.x.required=`

Modifiable field	**`ondemand.custom.field.x.required=`**
Field Description	Determines whether the custom field is a required field.
Possible Values	True, False.

Value Definition	**True** The target user must enter data in the field. **False** The target user can optionally enter data in the field.

```
ondemand.custom.field.x.label.locale=
```

Modifiable field	**ondemand.custom.field.x.label.locale**
Field Description	Translation for the custom field label name. x=1 - 9
Possible Values	User Defined. For example, `ondemand.custom.field.1.label.fr=Numéro de téléphone`
Value Definition	If no translations are present for the locale of the browser, the value in the **ondemand.custom.field.x.label** property is displayed.

Appendix A. Troubleshooting

When the on-demand target is installed, a log file is created in the target user's home directory. This file can be used for debugging purposes to examine any errors during the installation of the target or during a remote control session.

The log file is created with the following name format:

```
trc_odt_trace_yyyymmdd_hhmmss.log
```

For example, `trc_odt_trace_20130509_143252.log`.

Errors when you are using the Java applet method of installation

When the on-demand target is installed by using the Java applet method, the following errors might be reported. The errors are displayed in the status window and are written also to the log file. The status window is displayed until the target user closes it. For more information about the Java applet installation, see “Downloading the on-demand target by using the Java Applet” on page 40.

Bad URL:{0}
When a malformed URL is entered by the target user. For example, Bad URL:htp://example.com/#123456.

Bad server response for {0}: Response code {1}
When an invalid URL is provided. For example, Bad server response for http://example.com/index.jsp?conncode=0000000:Response code:404.

Unable to determine host architecture
The Java Applet is unable to determine whether the architecture of the target computer is 32-bit or 64-bit.

Error running {0} `-c`={1} `-l`={2}
When the Java Applet fails to start the on-demand launcher. For example, Error running /tmp/trc_odt-abc-123.exe **`-c`**=http://configurl **`-l`**=C:\Users\tgtuser\trc_odt_trace_20130510_131023.log

IO Error downloading from {0}
When a read or write error occurs while downloading the ODL, or the configuration package from the server. For example, IO Error downloading from http://configurl.

Unable to open the log file for writing
When the Java Applet is unable to create its debug log file.

Note: The Java Applet is built with Java version 1.5. Therefore, the target user must have a browser Java plug-in of version 1.5 or later for the Java applet to run correctly.

Errors when using the ActiveX method of installation

When the on-demand target is installed by using the ActiveX method, the following errors might be reported. The errors are written to the log file. For more information about the ActiveX installation method, see “Downloading the on-demand target by using the ActiveX control” on page 39.

The on-demand target application file failed to download
The file required for installing the on-demand target failed to download.

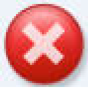
The on-demand target configuration file failed to download
The file required for configuring the on-demand target failed to download.

On-demand target installation and loading status icons

Status icons are displayed during the installation and loading of the on-demand target to indicate success or failure.

The icon that is displayed when the plug-in is being downloaded and installed. It is also displayed when the on-demand target is loading.

The icon that is displayed when the plug-in is successfully installed and the on-demand target is loaded.



The icon that is displayed when the plug-in installation fails or the on-demand target fails to load. Errors are written to the log file in the user's home directory.

Appendix B. Frequently asked questions

What is the definition of an on-demand target?

An on-demand target is a target that is temporarily installed to allow you to start a remote control session with a system that is on the internet. The session is managed by policies that are set on the IBM Endpoint Manager for Remote Control server and the target software is deleted when the session ends.

What is the definition of an unregistered target?

An unregistered target is a target that does not upload its details to the IBM Endpoint Manager for Remote Control server. There are two types of unregistered target.

- An on-demand target.
- A system that has the target software installed, the **`Managed`** property is set to No, and the **`BrokerList`** property is configured with a list of brokers.

I have my own website, how can I provide access to the on-demand target portal?

You can integrate the web page into your own site by creating a static portal or a dynamic portal. For more information about creating a custom portal, see Chapter 4, “Creating a custom landing page,” on page 7.

During a remote control session, why does my screen freeze with a message displayed and the session pauses temporarily?

The message, "`Please wait... Screen capture temporarily interrupted by the target operating system until the end user completes a secure desktop action (UAC prompt, fast user switching, screen locked). Screen capture will resume when the action is completed`" can be displayed for the following reasons.

When Windows is installed on the target system

- A User Access Control prompt is displayed on the target system.
- The target system has **Fast user switching** enabled and another user logs on.
- The target screen is locked and the target user must unlock it.

When Linux is installed on the target system

- The target system has **Fast user switching** enabled and another user logs on.

The remote control session continues after the target user completes the relevant action and the original target desktop that the session was started from, is displayed again. For example, after switching to a different user, you must switch back to the original target user's desktop to continue the session.

I have saved a recording of an on-demand session on my computer, how can I play it back?

You must get a URL for a web page from your helpdesk agent. When you access the web page, the IBM Endpoint Manager for Remote Control player is downloaded and started. Use the player to play your recording file. For more information about saving and playing back a recording, see Chapter 12, “Saving a session recording on the on-demand target,” on page 47.

Appendix C. Support

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

- http://pic.dhe.ibm.com/infocenter/tivihelp/v26r1/topic/com.ibm.tem.doc_9.1/welcome/welcome.html
- IBM Endpoint Manager Support site
- IBM Endpoint Manager wiki
- Knowledge Base
- Forums and Communities

Notices

This information was developed for products and services that are offered in the USA.

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

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

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

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

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

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

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

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

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

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

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

Portions of this code are derived from IBM Corp. Sample Programs.

© Copyright IBM Corp. _enter the year or years_. All rights reserved.

Programming interface information

Trademarks

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

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

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

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

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

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

ITIL is a registered trademark, and a registered community trademark of The Minister for the Cabinet Office, and is registered in the U.S. Patent and Trademark Office.

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

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Personal use

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

Commercial use

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

Rights

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

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

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Index

Printed in USA