

IBM Tivoli Assist On-site  
Version 3.3

*User's Guide*





IBM Tivoli Assist On-site  
Version 3.3

*User's Guide*



**Note**

Before using this information and the product it supports, read the information in "Notices" on page 121.

This edition applies to version 3, release 3 of IBM Tivoli Assist On-site and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2008, 2011.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

## Figures . . . . . v

## Chapter 1. IBM Tivoli Assist On-site. . . 1

Assist On-site components. . . . .	1
Assist On-site process . . . . .	2
New in this release . . . . .	2
Support sessions . . . . .	3
Unattended support sessions . . . . .	3
Assist On-site tunneling and port forwarding . . . . .	3
Session modes . . . . .	4
Host sessions . . . . .	7
Rational Host Access Transformation Services . . . . .	7
Host session architecture . . . . .	8
Collaboration in sessions . . . . .	9
Assist On-site launch-in-context . . . . .	10
Launch-in-context command-line syntax . . . . .	10
IBM Client Diagnostic Data Repository . . . . .	15
Assist On-site security . . . . .	15
Authentication . . . . .	16
Encryption and decryption . . . . .	17
Logging and auditing . . . . .	17

## Chapter 2. Remote Support Console . . . 19

Installing the Remote Support Console . . . . .	19
Remote Support Console Prerequisites . . . . .	19
Downloading and installing the Console. . . . .	19
Starting the Remote Support Console. . . . .	20
Configuring the Remote Support Console . . . . .	20
Console Settings window. . . . .	23
Using the Remote Support Console . . . . .	26
Support session management . . . . .	28
Recording sessions . . . . .	38
Turning on or off local input control . . . . .	38
Chatting with the customer . . . . .	38
Getting the target system information . . . . .	40
Available actions on the target machine . . . . .	41
File transfer functions . . . . .	44
Clipboard functions . . . . .	47
Console tools . . . . .	47
Working in collaborative sessions . . . . .	55
Turning on or off scaled view . . . . .	60
Turning on or off autoscroll . . . . .	61
Turning on or off Truecolor . . . . .	61
Customizing the Remote Support Console . . . . .	62
Extending the Remote Support Console . . . . .	62
Menu mapping XML file . . . . .	63
Customizing the branding of the Remote Support Console. . . . .	63
Common directory locations. . . . .	64

## Chapter 3. Remote Support Utility . . . 65

Installing the Remote Support Utility. . . . .	65
--	----

Remote Support Utility Prerequisites . . . . .	65
Running the Assist On-site connectivity test . . . . .	66
Installing the Utility for external IBM customers . . . . .	69
Installing the Utility for internal IBM customers . . . . .	71
Manually configuring the connection for the proxy server . . . . .	72
Using the Remote Support Utility . . . . .	73
Consenting to support sessions . . . . .	73
Stopping support sessions . . . . .	75
Switching between session modes . . . . .	75
Remote Support Utility actions . . . . .	75

## Chapter 4. Administration Portal. . . . 85

Logging on to the Administration Portal. . . . .	85
Assist On-site users, teams, and BlueGroups . . . . .	85
User functions . . . . .	86
Editing your profile . . . . .	86
Adding favorite URLs. . . . .	88
Viewing session history . . . . .	88
Viewing available installers to download . . . . .	89
Administrator functions . . . . .	89
Creating users . . . . .	89
Searching for users . . . . .	91
Managing users . . . . .	93
Creating teams . . . . .	93
Managing teams. . . . .	95
Adding team URLs. . . . .	96
Running bulk imports . . . . .	98
Viewing lists of recordings . . . . .	100
Viewing administrative reports . . . . .	107
Viewing the audit history for administrators . . . . .	109
Viewing the audit history for selected users or teams . . . . .	109
Server management functions . . . . .	109
Viewing the status of the Relay Server . . . . .	109
Viewing the bandwidth history of the Relay Server . . . . .	110
Viewing the connections history . . . . .	111
Viewing the connectivity problems report . . . . .	111
Uploading branding resource bundles . . . . .	111
Branding resource bundle . . . . .	112

## Chapter 5. Relay Server . . . . . 115

## Chapter 6. Assist On-site Support Service . . . . . 117

Downloading and installing the Support Service . . . . .	117
Configuring the Assist On-site Support Service . . . . .	117
Configuring port forwarding . . . . .	119

## Notices . . . . . 121



---

## Figures

1. Guidance-mode action symbols . . . . .	5	37. Connectivity test results . . . . .	68
2. Guidance-mode mouse button symbols . . . . .	6	38. Online request form. . . . .	70
3. Example of the Paint drawing tool . . . . .	6	39. Session code window . . . . .	71
4. Example of the Highlighting tool. . . . .	6	40. Remote Support Utility interface . . . . .	73
5. Host session architecture . . . . .	9	41. The Assist On-site window . . . . .	74
6. Console Settings window . . . . .	22	42. Information window with the support engineer's details. . . . .	76
7. Advanced Connection Settings window	23	43. Utility Chat window . . . . .	77
8. Remote Support Console interface . . . . .	26	44. Configure Port Forwarding window . . . . .	79
9. Authenticate Session window . . . . .	29	45. Configure Port Forwarding window with examples . . . . .	80
10. Tivoli Assist On-site window. . . . .	30	46. Start Host Session window . . . . .	81
11. Connection Code window. . . . .	30	47. The emulator session running in the Web browser window. . . . .	82
12. Tivoli Assist On-site window. . . . .	32	48. Edit User page . . . . .	87
13. Session for internal customers only confirmation window . . . . .	32	49. View Session History page . . . . .	88
14. Support session details window. . . . .	32	50. Add User page . . . . .	90
15. Connection Code window for internal IBM customers . . . . .	33	51. User and Team Administration page . . . . .	92
16. Tivoli Assist On-site window. . . . .	34	52. Manage Users page. . . . .	93
17. List AOS Targets window . . . . .	34	53. Add Team page . . . . .	94
18. Chat window . . . . .	36	54. Add User Licenses page . . . . .	95
19. Change session mode window . . . . .	36	55. Manage Teams page . . . . .	95
20. Close session confirmation dialog box. . . . .	37	56. View Team URLs page. . . . .	96
21. Chat window . . . . .	39	57. Create Team URL page. . . . .	97
22. E-mail transcript window . . . . .	40	58. User and Team Administration page . . . . .	99
23. Open URL window . . . . .	44	59. Report Options page . . . . .	101
24. Send File to Client window . . . . .	45	60. Video Export page. . . . .	103
25. Choose file to pull window . . . . .	46	61. Run Assist On-site Player applet window	104
26. Quick Text Input window. . . . .	49	62. Assist On-site Player window . . . . .	105
27. Example of the Paint drawing tool. . . . .	50	63. Assist On-site Player window . . . . .	106
28. Example of the Highlighting tool . . . . .	50	64. Report Options page . . . . .	108
29. The emulator session running in the Web browser window. . . . .	52	65. Current Relay Server Status with Recent Session Details page . . . . .	110
30. Port Forwarding window . . . . .	54	66. Assist On-site custom branding page	112
31. Local Port window . . . . .	55	67. Support Service Config window . . . . .	118
32. Local Port window for reverse port forwarding	55	68. Configure Port Forwarding window . . . . .	119
33. Collaboration Control window . . . . .	56	69. Configure Port Forwarding window with examples . . . . .	120
34. Collaboration Control window . . . . .	58		
35. Join a session window . . . . .	59		
36. Welcome page of the Assist On-site Configuration Wizard . . . . .	64		





---

## Chapter 1. IBM Tivoli Assist On-site

IBM® Tivoli® Assist On-site is a lightweight remote support program intended primarily for help desks and support engineers to diagnose and fix problems without the need of any external dependencies. Assist On-site is based on the IBM Tivoli Remote Control technology.

Assist On-site has been developed specifically to meet functionality, security, and privacy requirements of IBM and IBM customers. Support engineers and their customers can run it on various platforms. It currently has a native version for the 32 bit Windows environment and generic Linux compatible operating systems. Assist On-site uses IBM AES MARS encryption, NTLM authentication, and IBM intranet authentication for IBM support engineers. Assist On-site can also support lightweight Rational® Host Access Transformation Services emulator sessions for computers running z/OS® and Power i.

Assist On-site provides a launch-in-context feature such that support engineers can start Assist On-site from within the session of the third-party support tool. For restricted use only, Assist On-site supports IBM diagnostic tools to function over the Assist On-site connection for the purpose of debugging hardware devices and IBM software.

---

### Assist On-site components

Assist On-site has several primary components: Remote Support Console, Remote Support Utility, Relay Server, Administration Portal, and Assist On-site Support Service.

- Remote Support Console

It is a Java application that is installed on the machine of the support engineer and is used to communicate with the Remote Support Utility. The Remote Support Console has many functions to assist the support engineer in resolving customer issues within a support session.

- Remote Support Utility

It is a lightweight Java application that communicates with the Remote Support Console. The Remote Support Utility has many functions that provides the customer with various privacy functions while the support engineer can take control of the customer's machine when allowed. After support session stops, the Remote Support Utility deletes itself from the customer's machine.

- Relay Server

It is an application server that handles the data transmissions for support sessions between the Remote Support Console and the Remote Support Utility. There is a network of servers across several geographic regions, with support engineers and customers connecting to those servers within their geographic regions where possible.

- Administration Portal

It is a single, secure point of access to information, applications, teams, and users that can be administered and managed to support Assist On-site.

- Assist On-site Support Service

It is an applicative service that has features similar to the Remote Support Utility and runs on target machines. It registers itself with the Relay Server and sends

HTTPS heartbeats as status updates. Assist On-site Support Service configuration uses customer policies that determine when and how the support engineer can run unattended support sessions.

---

## Assist On-site process

The components of Assist On-site (AOS) interact together to start and maintain a support session between the support engineer and the customer.

The Assist On-site process can be summarized as follows:

1. The customer contacts the support team and opens a PMR with an issue or question.
2. In the Remote Support Console, the support engineer starts a support session to determine the problem.
3. The Relay Server generates a connection code that is displayed in the Remote Support Console. The connection between the Relay Server and the Remote Support Console is established. The one-time-use connection code is seven digits, with a default timeout of 15 minutes.
4. The support engineer refers the customer to an Assist On-site URL and the customer can enter details such as name, PMR number, and customer number.
5. The support engineer can extend the connection code timeout for an additional 10 minutes to accommodate slow network connectivity.
6. The Remote Support Utility plug-in downloads automatically through the customer's Web browser and is less than 780 KB. The customer enters the connection code.
7. The Remote Support Utility starts and the initialize support session and session mode window opens.
8. The customer must select the session mode and thereby accept the request from the support engineer to start the support session. The connection between the Relay Server and the Remote Support Utility is established.
9. After the customer accepts, the support engineer is connected to the customer's machine through the Relay Server.
10. The support engineer attempts to resolve the problem during the support session and uses the functions of the Remote Support Console.
11. During the session, the customer can retake control of the mouse and keyboard at any time.
12. Either the support engineer or customer can stop the session.
13. After the session ends, the Remote Support Utility is deleted from the customer's machine.

---

## New in this release

Version 3.3 provides new features and enhancements to Assist On-site Version 3.2. They support tunneling, launch-in-context, and IBM Client Data Diagnostic Repository.

Version 3.3 contains the following new features and enhancements:

- **Assist On-site launch-in-context**  
Assist On-site provides a launch-in-context feature such that support engineers can start Assist On-site from within the session of the third-party support tool.
- **Assist On-site tunneling and port forwarding**

For restricted use only, Assist On-site supports IBM diagnostic tools to function over the Assist On-site connection for the purpose of debugging hardware devices and IBM software. During a Assist On-site tunneling session, the set of forwarded ports is saved to a CSV file on the support engineer's machine. Connections to multiple devices from the same port on the support engineer's machine and collaborative sessions are also supported. The Assist On-site administrator can turn on this feature for teams that have specific permission to use it for remote diagnostics.

- **Support for the exchange of diagnostic data**

Assist On-site provides support for the IBM Client Diagnostic Data Repository (CDDR) strategy in the exchange of data through the propagation of team URLs and file transfer functions.

---

## Support sessions

Support engineers can troubleshoot issues with the machine of a customer during a support session. A support session is a lightweight remote-control and interactive exchange between the support engineer's controller machine running the Remote Support Console and the customer's target machine running the Remote Support Utility.

The support engineer establishes an authenticated connection to the Relay Server and creates the support session, requesting a unique connection code from the Relay Server. The support engineer gives this connection code to the customer, who downloads the Remote Support Utility and joins the support session using the connection code.

Support sessions can run in various modes that determine the level of access the support engineer has to the target machine. With the customer's permission, the support engineer can view the target desktop and shares control of the target mouse and keyboard. The customer has overriding control of the mouse and keyboard and can stop the support session at any time.

## Unattended support sessions

The support engineer can run lights-out or unattended support sessions, including port forwarding sessions, during which the customer is not in attendance. The support engineer establishes an authenticated connection between the Remote Support Console and the Relay Server. The Remote Support Console displays a list of target machines on which the Assist On-site Support Service runs. Assist On-site Support Service configuration uses customer policies that determine when and how the support engineer can run unattended support sessions and port forwarding sessions.

## Assist On-site tunneling and port forwarding

A customer might have issues on a storage device or another IT device that does not have a GUI and want a support engineer to troubleshoot the issues by using debug tools such as Telnet or SSH during a port forwarding session. A port forwarding session is a tunneled session that routes debugging or diagnostic traffic between the configured local port on the support engineer's machine and the port on the remote host machine. It runs over an existing Assist On-site connection, ensuring secure end-to-end connections.

For restricted use only, Assist On-site supports IBM diagnostic tools to function over the Assist On-site connection for the purpose of debugging hardware devices

and IBM software. The Assist On-site administrator can turn on this feature for teams that have specific permission to use it for remote diagnostics.

After the customer explicitly configures permission for port forwarding in the Remote Support Utility, the support engineer can begin the attended, port forwarding session to the authorized ports. During an Assist On-site tunneling session, the set of forwarded ports is saved to a CSV file on the support engineer's machine.

The support engineer and the customer can use the Assist On-site chat function to communicate during this session or change to another session mode. The customer or support engineer can stop the port forwarding session at any time.

The support engineer can set which local ports on the support engineer's machine to forward to which remote host machines and ports. Connections to multiple devices from the same port on the support engineer's machine and collaborative sessions are also supported.

Alternatively, the customer can use Assist On-site Support Service to configure remote host machines for unattended, port forwarding sessions. The support engineer can start and run multiple unattended, port forwarding sessions in the Remote Support Console.

## Session modes

Assist On-site can establish remote connections for support sessions in different modes. The customer chooses the session mode after joining the support session or the support engineer can request that the customer changes the mode during the support session. The type of session or the permissions associated with the support engineer also determine the session modes that are available during sessions.

When Assist On-site administrators create a team or a user, they can select the default permissions for that team or user including the set of session modes that are available. For example, a team might have default permissions to run sessions in View Only and Chat Only session modes. Customers can further restrict the session mode when they consent to sessions.

### Chat Only mode

This session mode allows the support engineer to chat with the customer in the Chat window, but does not allow the support engineer to view the target system or have any control of the target mouse or keyboard.

**Note:** The Chat window allows the support engineer to chat to the customer within another session mode and provides an additional form of contact.

The support engineer can also request or the customer can change to the Chat Only mode during a support session.

### View Only mode

This session mode the support engineer to view the target system, but does not allow the support engineer to have any control of the target mouse or keyboard.

In the View Only mode, the support engineer can select and mark areas of the target desktop using the Remote Support Console tools.

The support engineer can also request or the customer can change to the View Only mode during a support session.

## Guidance mode

This session mode allows the support engineer to view the target system and direct the customer to perform tasks on the target system, but does not allow the support engineer to have any control of the target mouse or keyboard. The support engineer can use the Guidance mode symbols, Remote Support Console tools, and the chat function to direct the customer through any task to perform on the target.

The Guidance mode is often used in training situations and in workplaces of very high sensitivity.

**Note:** Your administrator might have disabled the Guidance mode and therefore it is disabled in the Session mode window.

The support engineer can request or the customer can change to the Guidance mode during a support session.

### Legend for the Guidance mode symbols

There are five action symbols that the support engineer can display on the target desktop as follows:

- **Move**  
Move the target cursor to the position of the symbol.
- **Single Click**  
Click the target mouse button once.
- **Double Click**  
Click the target mouse button twice.
- **Drag Start**  
Click the target mouse button and start to drag the mouse in the direction of the symbol.
- **Drag End**  
Continue to drag the target mouse in the direction of the symbol and then release the target mouse button at the final position of the symbol.

Figure 1 shows examples of the action symbols.



Figure 1. Guidance-mode action symbols

The support engineer can also specify the mouse button with which to perform the action. Figure 2 on page 6 shows examples of the action symbols for the target mouse buttons.

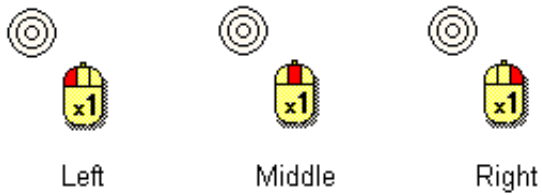


Figure 2. Guidance-mode mouse button symbols

### Other tools

The support engineer can use the Remote Support Console drawing tools to paint colored lines or highlight areas on the target desktop to direct the customer.

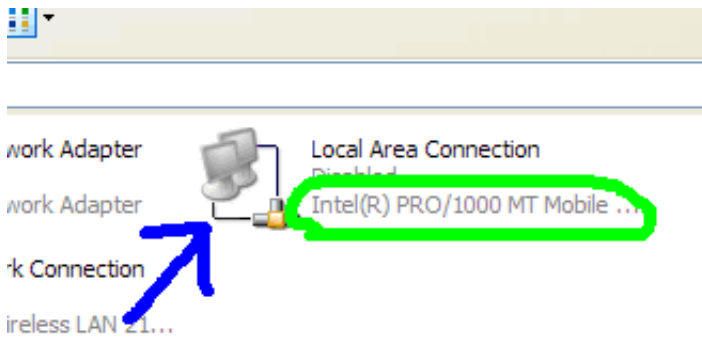


Figure 3. Example of the Paint drawing tool

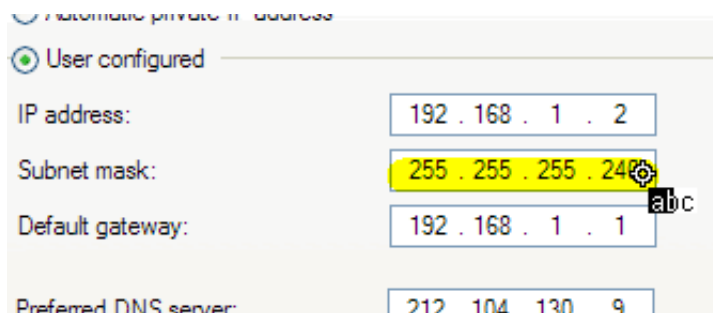


Figure 4. Example of the Highlighting tool

### Shared Control mode

This session mode allows the support engineer to view the target system and to have input control of the target mouse and keyboard.

During a support session, the support engineer can turn on local input control to perform actions on the support engineer's machine rather than the target machine.

The actions of the customer take precedence over the actions performed through the Remote Support Console. When the customer uses the mouse or the keyboard,



the input control icon changes to  to indicate that input control in the Remote Support Console is temporarily blocked until the customer stops using the mouse or the keyboard.

The support engineer can use the Remote Support Console tools, such as the drawing tools, to select and mark areas of the target desktop.

The support engineer can request or the customer can change to the Shared Control mode during a support session.

---

## Host sessions

A customer might have issues on a computer running z/OS or Power i and want a support engineer to troubleshoot the issues during a host session. A host session is lightweight IBM Rational Host Access Transformation Services emulator session simultaneously running in the Web browsers on both the customer's target and support engineer's machines. It runs over an existing Assist On-site connection, ensuring secure end-to-end connections.

Either the customer or the support engineer can start the host session. Only the customer logs on to the host machine without the support engineer seeing the host User ID and password. The support engineer can run commands on the host while the customer views these commands and maintains control of the target machine.

The support engineer and the customer can use the Assist On-site chat function to communicate during the host session. Other support engineers can collaborate and join the host session without using Assist On-site if they obtain the host session URL and ID code.

The customer can stop the host session at any time.

## Rational Host Access Transformation Services

IBM Rational Host Access Transformation Services (HATS) transforms terminal applications quickly and easily. With Rational Host Access Transformation Services, you can create Web applications, including portlets, and rich client applications that provide an easy-to-use graphical user interface (GUI) for your 3270 applications running on IBM System z<sup>®</sup> platforms and your 5250 applications running on IBM Power i platforms.

These character-based 3270 and 5250 applications are referred to as host applications.

Assist On-site uses Rational Host Access Transformation Services to manage a host session over an existing and secure Assist On-site connection. Rational Host Access Transformation Services converts the host application data streams to HTML for lightweight emulator host sessions. The emulator host session runs simultaneously in the Web browsers on both the customer's target and support engineer's machines. The customer can monitor the work that the support engineer performs during the host session and can intercede as required. No additional Rational Host Access Transformation Services software needs to be downloaded to the target machine and host machine or the support engineer's machine. The customer does not have to open any ports in the firewalls on the customer's network.

## Host session architecture

The components of Assist On-site (AOS) interact together and with the Rational Host Access Transformation Services (HATS) server to start and maintain a host session.

The process to start and maintain the host session is shown in Figure 5 on page 9 and can be summarized as follows:

1. The customer uses the Remote Support Utility **Start a Host Session** function to initiate a session with the host computer.
2. Remote Support Utility prepares a packet-forwarding thread and port to establish a host connection.
3. Assist On-site sends the packet over the existing Assist On-site connection to request a new host connection.
4. The Relay Server opens a new port and a bidirectional packet-forwarding thread within the Assist On-site network to be ready to accept a Rational Host Access Transformation Services connection for the new host session.
5. The Relay Server opens a HTTP or HTTPS URL connection to the Rational Host Access Transformation Services server. It passes the newly-opened local port, server, and connection type for the new connection, for example:  
`https://localhost:9443/hatsproj1/index.jsp?host=aosrelay1&sessionType=1&port=9101;`
6. The Rational Host Access Transformation Services server begins a TN3270 or a TN5250 host session to the requested port.
7. The packet-forwarding thread within the Relay Server forwards the TN3270 data packet to the Remote Support Utility.
8. The Remote Support Utility routes the TN3270 or TN5250 packet to the host computer, and the packet-forwarding thread routes all packets from the host computer across the Assist On-site connection.
9. The Relay Server receives the new session ID from the Rational Host Access Transformation Services server for the Web browser clients. It sends a new packet to both endpoints informing them of this secure session ID to which to connect to the Rational Host Access Transformation Services emulator session.
10. Assist On-site launches the same emulator session in Web browser clients at both endpoints.
11. The emulator session remains active and synchronized, with either the customer or support engineer running commands. This session functions independently of the Assist On-site connection. The customer can select the Chat Only mode and monitor the support engineer without relinquishing control of the customer's target machine.
12. When either the customer or support engineer ends the Assist On-site session, the host session also ends.



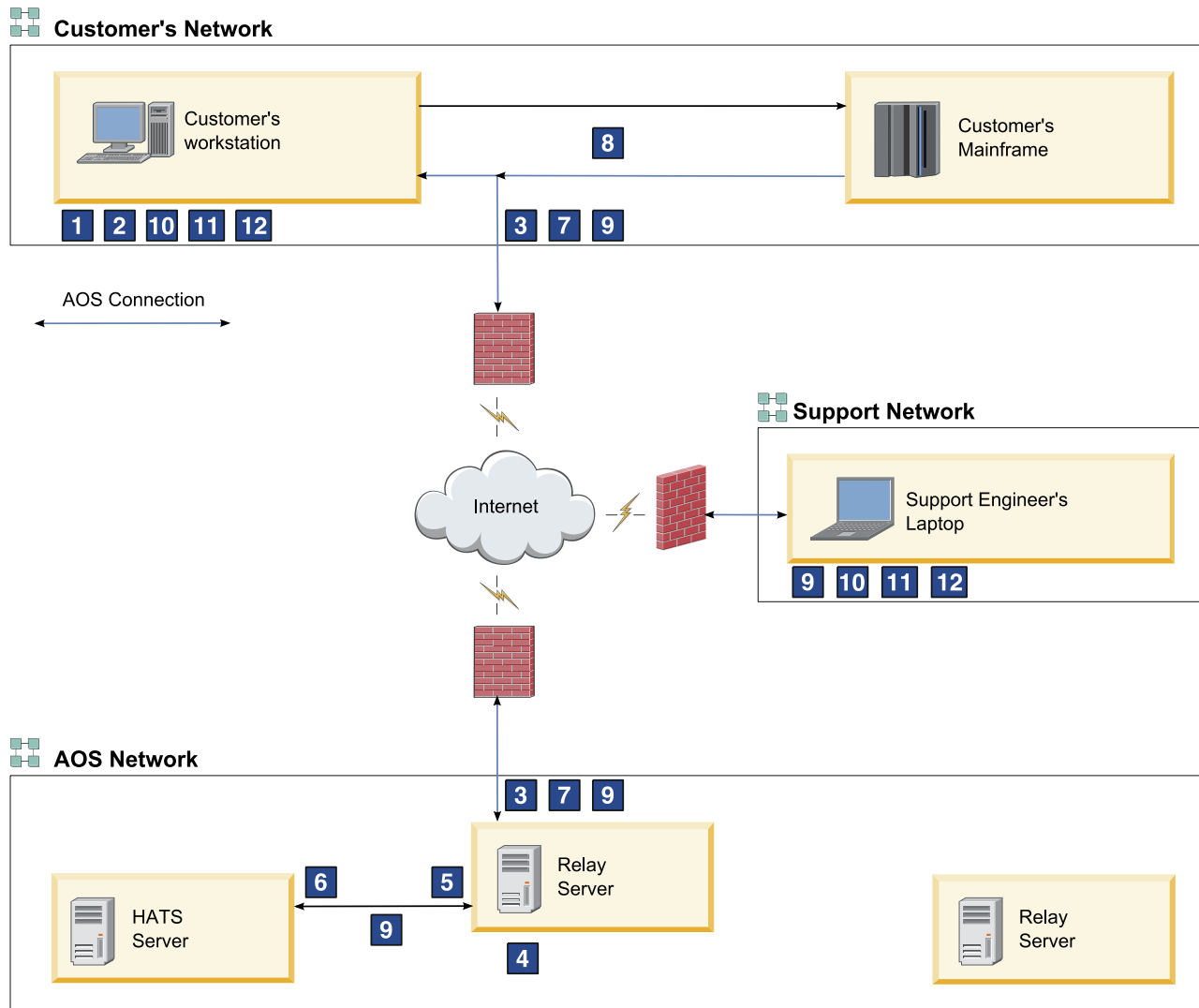


Figure 5. Host session architecture

## Collaboration in sessions

Assist On-site has the Collaboration function to let multiple participants (support engineers and the customer) to connect, view the target desktop, and chat during the same support session. The original or primary support engineer starts the collaboration for the existing support session and provides a collaboration code to the other participating support engineers. The customer must accept each participating support engineer's request to join the support session.

The secondary support engineer can join an existing support session using the collaboration code or the secure URL if the Remote Support Console is not installed. The primary support engineer provides the secondary support engineer with the secure URL that launches the Remote Support Console from a Relay Server using a Java Web Start Launcher.

The primary support engineer can assign and return control of the support session, disconnect other participating support engineers, and leave the support session while the other participants continue. All participants can send messages in a shared chat session.

Collaboration can also occur during a host session, although the other participating support engineers do not need to use Assist On-site. The primary support engineer can send the host session URL and ID to the other participants, and they can participate using their Web browsers.

---

## Assist On-site launch-in-context

Support engineers might start troubleshooting customers' issues by first using other support tools such as Technical Support Chat. Rather than starting Assist On-site independent of other support tools, Assist On-site provides a launch-in-context feature such that support engineers can start Assist On-site from within the session of the third-party support tool.

The Assist On-site launch-in-context feature has the following functions:

- Command-line interface to start Assist On-site from the third-party support tool. It opens the Remote Support Console on the support engineer's machine, creates a support session, and obtains the connection code. Assist On-site also creates a connection file that contains the instructions for the customer to download the Remote Support Utility from the specified Assist On-site URL.

**Note:** The third-party support tool provides the launch mechanism, for example, a menu item in the support tool that executes the command-line interface and runs Assist On-site.

- Command-line launch-in-context parameters to specify details of the customer, support engineer, and PMR, flags to write values to standard output, and paths to use the Assist On-site connection and template URL files.
- Template URL file to contain the launch-in-context parameters and the instructions for the customer to download the Remote Support Utility as specified by Assist On-site URL launch-in-context parameter.

When Assist On-site is started in context, Assist On-site generates the connection file with contents of the template URL file and replaces the launch-in-context parameters by their runtime values.

To use this feature, you must perform the following tasks:

1. Build the launch mechanism in the third-party tool.
2. Add the Assist On-site command with the launch-in-context parameters to the launch mechanism.
3. Create the template URL file with the launch-in-context parameters and the instructions for the customer to download the Remote Support Utility as specified by Assist On-site URL launch-in-context parameter.
4. Display the contents of the connection file to the customer.

## Launch-in-context command-line syntax

Support engineers can launch Assist On-site in context from the command-line interface based on the set of parameters that are specified at launch time. Administrators can create the template URL file with the launch-in-context parameters and the instructions for the customer to download the Remote Support Utility as specified by Assist On-site URL launch-in-context parameter.

## Syntax

There are a set of launch-in-context parameters that are mandatory. If you do not set these parameters correctly, some or all of the functions of the feature might not work. Table 1 outlines the special characters that are used in the syntax for the command to specify whether the launch-in-context parameters are mandatory and the valid values.

Table 1. Special characters for command-line interface

Special Character	Description
<>	Identifies a placeholder name.
[]	Identifies an optional parameter. Parameters not enclosed in brackets are required.
...	Indicates that you can specify multiple values for a parameter.
	Indicates mutually exclusive parameters. Specify either the parameter to the left of the separator or the parameter to the right of the separator, but not both.
{}	Encloses a set of mutually exclusive parameter separated by  .

Remote Support Console must be installed on the support engineer's machine. To run the AOSConsole.jar file, use the Java command.

**Note:** Ensure that you set Java home directory in the Path environment variable to run the Java command from any working directory. You can use a relative path to the AOSConsole.jar file or an absolute path, which must be enclosed by double quotes if using the feature on a Windows system.

```
java -jar rsc_root/AOSConsole.jar --script startnewsession
customername="<customer_name>"
ibmcustnumber="<customer_number>"
geo="{americas|ap|emea}"
aosconnectionfile=<path_to_connection_file>
templateurlfile=<path_to_template_url>
[usesavedcredentials=true|false]
[licenseagreement="<url_for_license_agreement>"]
[rename="<support_engineer_name>"]
[pmrnumber1="<pmr_number>"]
[pmrnumber2="<branch_code>"]
[pmrnumber3="<country_code>"]
[returnurltostdout=true|false]
[returnconnectioncodetostdout=true|false]
```

**Important:** Ensure that you do not remove any characters such as double quotes, full stops and forward slashes for relative paths, and so forth. Removing any of these characters might cause incorrect parsing of the parameters, processing of the template URL file, and saving of the contents to the connection file.

## Parameters

### **--script startnewsession**

Mandatory flag to determine which connection mode to use to start Assist On-site.

**customername**="*<customer\_name>*"

Mandatory parameter that represents the name of the customer, enclosed by double quotes.

**geo**="{americas|ap|emea}"

Mandatory parameter that represents the geography associated with the customer and the relay server to which the customer connects. It is a single geography, enclosed by double quotes.

**ibmcustnumber**="<customer\_number>"

Mandatory parameter that represents the number associated with the IBM customer, enclosed by double quotes.

**Note:** If you do not know the customer number, use "99999".

**templateurlfile**="<path/file\_name>"

Mandatory parameter to the path and name of the template URL file, for example, `templateURL.txt`. Administrators can create the template URL file with the launch-in-context parameters and the instructions for the customer to download the Remote Support Utility as specified by Assist On-site URL launch-in-context parameter. When Assist On-site is started in context, Assist On-site generates the connection file, as specified by the **aosconnectionfile** parameter, with contents of the template URL file and replaces the launch-in-context parameters by their runtime values.

You can use the absolute paths or relative paths to the template URL file.

Table 2. Absolute and relative paths

Operating System	Absolute Path	Relative Path
Windows	"C:\Program Files\IBM\Assist On-site\Console\"	Relative to the current working directory. For example: <ul style="list-style-type: none"><li>• C:\AOS is the working directory</li><li>• \templates or ./templates is the relative path</li><li>• C:\AOS\templates is the absolute path</li></ul>
UNIX	./opt/ibm/Assist On-site/Console/	Relative to the current working directory. For example, ./templates

**aosconnectionfile**=<path\_to\_connection\_file>

Mandatory parameter to the path and name of the connection file, for example, `aoslaunchurl.txt` that contains the instructions for the customer to download the Remote Support Utility as specified by Assist On-site URL. The contents are determined by the template URL file and the runtime values for the launch-in-context parameters that the administrator specifies within that file. Assist On-site creates the text file if it is not already created, or it overwrites the file if it exists.

You can use the absolute paths or relative paths to the connection file.

**licenseagreement**="<url\_to\_license\_agreement>"

Optional parameter to the URL that contains the custom license agreement. You can create a landing page with your custom license agreement and terms and conditions that replaces the Assist On-site standard landing page. Use the internal test page as an example:

<https://aos.us.ihost.com/AssistOnSite/InternalTest.jsp>

**repname**="*<support\_engineer\_name>*"

Optional parameter that represents the name of the support engineer, enclosed by double quotes.

**usesavedcredentials**=*true|false*

Optional flag to determine whether to use the saved credentials of the support engineer.

**pmrnumber1**="*<pmr\_number>*"

Optional parameter that represents the number associated with the PMR for the customer issue, enclosed by double quotes.

**pmrnumber2**="*<branch\_code>*"

Optional parameter that represents the branch code associated with the PMR, enclosed by double quotes.

**pmrnumber3**="*<country\_code>*"

Optional parameter that represents the country code associated with the PMR, enclosed by double quotes.

**returnurltostdout**=*true|false*

Optional flag to determine whether the Assist On-site URL to download the Remote Support Utility is passed to standard output, for example, the command-line interface.

**returnconnectioncodetostdout**=*true|false*

Optional flag to determine whether the connection code is passed to standard output, for example, the command-line interface.

## Example on Windows systems

This example for Windows systems starts Assist On-site with the following values for the launch-in-context parameters:

```
java -jar "C:\Program Files\IBM\Assist On-site\Console\AOSConsole.jar"  
--script startnewsession  
customername="John Doe"  
geo="americas"  
ibmcustnumber="99999"  
templateurlfile="C:\Program Files\IBM\Assist On-site\Console\templateURL.txt"  
aosconnectionfile=./aoslaunchurl.txt  
licenseagreement="https://aos.us.ihost.com/AssistOnSite/InternalTest.jsp"  
repname="Jane Smith"  
usesavedcredentials=true  
pmrnumber1="111111"  
pmrnumber2="111"  
pmrnumber3="111"
```

## Example on UNIX systems

This example for UNIX systems starts Assist On-site with the following values for the launch-in-context parameters:

```
java -jar /opt/ibm/Assist On-site/Console/AOSConsole.jar  
--script startnewsession  
customername="John Doe"  
ibmcustnumber="99999"  
templateurlfile=./opt/ibm/Assist On-site/Console/templateURL.txt  
geo="americas"  
aosconnectionfile=./aoslaunchurl.txt  
licenseagreement="https://aos.us.ihost.com/AssistOnSite/InternalTest.jsp"  
repname="Jane Smith"
```

```

usesavedcredentials=true
pmrnumber1="111111"
pmrnumber2="111"
pmrnumber3="111"

```

## Template for the Assist On-site URL

Administrators can create the template URL file with the launch-in-context parameters and the instructions for the customer to download the Remote Support Utility as specified by Assist On-site URL launch-in-context parameter. When Assist On-site is started in context, Assist On-site generates the connection file with contents of the template URL file and replaces the launch-in-context parameters by their runtime values.

Each launch-in-context parameter must be enclosed by < and >. Table 3 outlines the launch-in-context parameters to use and two parameters for the generated connection code and generated URL from which to download the Remote Support Utility.

*Table 3. Launch-in-context parameters in the template URL file*

Launch-in-context parameter	Description
<customername>	Assist On-site replaces it with the value that was specified for the customer's name.
<ibmcustnumber>	Assist On-site replaces it with the value that was specified for the IBM customer number.
<pmrnumber1>	Assist On-site replaces it with the value that was specified for the PMR.
<pmrnumber2>	Assist On-site replaces it with the value that was specified for the branch code.
<pmrnumber3>	Assist On-site replaces it with the value that was specified for the country code.
<repname>	Assist On-site replaces it with the value that was specified for the support engineer. It does not use the name associated with the credentials that the support engineer uses to initiate the support session.
<licenseagreement>	Assist On-site replaces it with the value that was specified for the URL of the custom license agreement.
<geo>	Assist On-site replaces it with the value that was specified for the geography.
<aosconnectioncode>	Assist On-site replaces it with the generated connection code. <b>Note:</b> This parameter is not a command-line parameter. It is only used in the template URL file.
<aosurl>	Assist On-site replaces it with the generated URL from which to download the Remote Support Utility. <b>Note:</b> This parameter is not a command-line parameter. It is only used in the template URL file.

**Important:** If you do not specify the launch-in-context parameter in the command, but you specify it in the template URL file, an error occurs when Assist On-site processes the template URL file.

An example of the template URL file is as follows:

```
Hello <customername>,  
Please read the license and agree to it on this page:  
<licenseagreement>  
Download the Remote Support Utility from <aosurl>  
When prompted, enter this connection code: <aosconnectioncode>
```

```
Thank you,  
<repname>
```

When Assist On-site is launched in context, Assist On-site replaces the parameters enclosed by < and > with the relevant values and saves this content to the connection file.

```
Hello John Doe,  
Please read the license and agree to it on this page:  
https://aos.us.ihost.com/AssistOnSite/InternalTest.jsp  
Download the Remote Support Utility from  
https://aos.us.ihost.com:80/AssistOnSite/download.jsp?connCode=1234567  
When prompted, enter this connection code: 1234567
```

```
Thank you,  
Jane Smith
```

---

## IBM Client Diagnostic Data Repository

Often IBM support engineers need to analyze customer data to diagnose customers' issues or they need to provide customers with utilities to debug the issues. Assist On-site provides support for the IBM Client Diagnostic Data Repository (CDDR) strategy in the exchange of data through the propagation of team URLs and file transfer functions. Administrators can add team URLs to the relevant URLs associated with CDDR and propagate those URLs to subteams. During Assist On-site sessions, support engineers can open these URLs on the customers' machines and transfer diagnostic data.

The CDDR strategy uses the Enhanced Customer Data Repository (ECuRep) as the consolidated back end data repository for exchanging information with IBM Software Technical Support. The strategy also means that customers can exchange data by using the fastest method based on geographic location, for example, by connecting to the Testcase FTP server or by connecting to ECuRep directly. For more information, see the following address:

<http://www-01.ibm.com/software/support/exchangeinfo.html>

---

## Assist On-site security

Security and privacy are fundamental concerns when granting remote access to corporate IT assets. Assist On-site uses the latest security technology to ensure that the data exchanged between support engineers and customers is completely secure. Identities are verified and protected with industry-standard authentication technology. Assist On-site support sessions are kept secure and private using randomly generated session keys and advanced encryption.

Assist On-site allows support engineers to remotely access customers' machines to identify and resolve technical issues in real time. Assist On-site has a powerful suite of tools for problem determination and remediation that support engineers can use to quickly complete root cause analysis and take appropriate corrective action.

No permanent installation of software on the customer's machine is required. The Remote Support Utility plug-in downloads automatically through the customer's Web browser and is less than 780 KB. The plug-in is kept secure and virus free on the Relay Server and must be downloaded each time a support session is established.

Only customers can initiate support sessions unless they are unattended support sessions. During the initiation of an attended support session, the customer can refuse receipt of the Remote Support Utility plug-in, thus refusing the download. When the customer accepts the connection to the support session, the customer can choose a session mode. During the support session, the customer can retake control of the mouse and keyboard at any time.

After a support session starts, the support engineer is connected to the customer's machine through the Relay Server. Large, randomly generated session keys are issued to both participants; thus, only the designated parties are connected. During the support session, all transferred data is encrypted, including screen views, file transfer data, and identities. Encryption and decryption are from end to end; therefore, data cannot be intercepted during transit and can only be viewed through the Remote Support Console.

The support engineer can also troubleshoot problems on the customer's machine running z/OS or Power i by using a host session over an existing Assist On-site connection to ensure secure end-to-end connections. No Rational Host Access Transformation Services emulators must be installed on the customer's target machine, the host machine, or the support engineer's machine. Either the customer or support engineer can start a host session, but only the customer can log on to the host machine. The support engineer can run commands on the host machine and the customer can monitor this work and maintain control of the customer's target machine.

Either the customer or support engineer can stop the support session or host session. After the support or host session stops, the support engineer can no longer connect to the customer's computer or the host machine. Any future support sessions require new session keys and only the customer can initiate them.

The support engineer can troubleshoot problems on a customer's IT device by using debug tools such as Telnet or SSH during a port forwarding session. A port forwarding session is a tunneled session that routes debugging or diagnostic traffic between the configured local port on the support engineer's machine and the port on the remote host machine. It runs over an existing Assist On-site connection, ensuring secure end-to-end connections. No emulator or diagnostic software needs to be installed on the remote host machine. The Assist On-site administrator can turn on this feature for teams that have specific permission to use it for remote diagnostics. The customer configures the remote host machines and ports for port forwarding sessions whether attended by using the Remote Support Utility or unattended by using the Assist On-site Support Service.

## Authentication

Support sessions are protected by strong password authentication. Support engineers are authenticated using a challenge and response password exchange, or IBM support engineers can be authenticated using their IBM intranet IDs and passwords through IBM Intranet Password eXternal. Customers can select basic or NTLMv2 authentication for Assist On-site connections through their proxy servers.



Administrators can view audit reports detailing logon failures associated with incorrect IDs or passwords through the Administration Portal.

## **NTLMv2**

NTLMv2 is a Microsoft challenge-response authentication protocol, that is used with the SMB protocol. It sends two 16-byte responses to an 8-byte server challenge. The protocol hashes the client and server challenges by using HMAC-MD5 that hashes the proxy password and other data including the proxy user name and domain name.

Assist On-site detects the customer's proxy server through the customer's Web browser settings or registry keys. Proxy settings are evaluated through a JavaScript parser if available. The Remote Support Utility opens a window to allow the customer to select basic or NTLM proxy authentication. If the customer selects NTLM, the customer enters the domain, user ID and password to authenticate using the NTLMv2 protocol.

## **IBM intranet ID and password authentication**

IBM Intranet Password eXternal is an authentication tool that uses leading edge open standards to allow IBM employees on the intranet to securely use the existing intranet password system to log on to third-party vendor Web sites. The open standards include the RSA Public Key Cryptography Standard (PKCS) 7, XML, and SOAP-based Web services.

IBM Intranet Password eXternal utilizes web service technology to adopt the intranet password system regardless of their operating system or server platform and to remotely validate digitally-signed authentication tokens.

Assist On-site adopts IBM Intranet Password eXternal to allow support engineers to log on to the Remote Support Console and Administration Portal using their IBM intranet ID and passwords, without Assist On-site compromising the passwords. Using IBM BlueGroups, IBM Intranet Password eXternal can manage support engineers' membership of support teams and thereby access to Assist On-site. Assist On-site migrates the details from the BlueGroups to the Administration Portal database.

## **Encryption and decryption**

Assist On-site implements outbound connections that are protected by state-of-the-art 128-bit MARS encryption over an HTTPS browser session. This form of advanced encryption prevent intruder access to the information exchanged during all support sessions. Chat, screen viewing, screen sharing, and file transfer data is encrypted end to end. Packets are never decrypted in transit by the Relay Server.

## **Logging and auditing**

Assist On-site writes to log files on the Relay Server and can also write to log files on the customer's target machine if the customer selects the option when initiating the support session.

Relay Server logs the following support session data: the customer name and number; the support engineer name and number; the customer's and support engineer's IP and MAC addresses; and the connection and disconnection time stamps. Administrators can view reports of these log files through the Administration Portal.

The customer can choose to audit the support session locally and must explicitly activate it upon accepting the support session. Assist On-site events are written to the target system's application log. Written events include:

- Connection and disconnection
- Initial session mode and subsequent changes to other session modes
- Details about port forwarding session including the user name of the support engineer and a date and time stamp about when the connection was started and stopped
- Names of the files that have been received and transferred
- Any requests for system information from the Remote Support Console

---

## Chapter 2. Remote Support Console

The Remote Support Console is one of the main components of Assist On-site. It is a lightweight Java application that is installed on the controller machine of the support engineer and is used to communicate with the Remote Support Utility. The Remote Support Console has many functions to assist the support engineer in resolving customer issues within a support session.

---

### Installing the Remote Support Console

You can download the Remote Support Console for your platform from the Administration Portal and install using the executable file or the binaries.

#### Remote Support Console Prerequisites

Remote Support Console requires that you have installed Java Runtime Environment (JRE) version 1.6 or higher. Assist On-site also requires that you can connect to the Americas Relay Server and another server located in your geographical region. Your firewall and proxy server must allow traffic to and from the Relay Server.

Open a command-line interface, and run the following command:

```
java -version
```

The output displays either the current version of the JRE, or it displays an error if it is not installed.

The summary of requirements for the Remote Support Console is as follows:

- One of the following supported platforms:
  - Pentium-class computer running Windows starting with Windows 95 and above, including all variants of Windows 2000, Windows XP, Windows Vista, and Windows 7
  - Red Hat Enterprise and Desktop Linux 5 for Intel 32-bit and 64-bit
  - SUSE Linux Enterprise Server 11 for Intel 32-bit and 64-bit
  - Mac OS X 10.0 or later

You can configure the Remote Support Console to connect to a specific Relay Server for your geographical region. For more information, see “Configuring the Remote Support Console” on page 20.

Your firewall might deny the Assist On-site connection. If your firewall logs show that it has blocked Assist On-site traffic, configure your firewall according to the associated firewall documentation to allow traffic to and from the Relay Server in the Americas on the relevant ports and any other Relay Server in your region. For more information about the IP addresses and port numbers for each Relay Server, see Chapter 5, “Relay Server,” on page 115.

#### Downloading and installing the Console

You can log on to the Administration Portal and download the installer for Windows operating systems only or binaries for multiple platforms from the Downloads page. The executable file or binaries files contain the Assist On-site

Configuration Wizard. The Assist On-site Configuration Wizard configures the Remote Support Console to use your team's default resource branding bundle.

## Before you begin

Ensure that you have Java Runtime Environment version 1.6 or higher. You also need your Assist On-site user account details to log on to the Administration Portal.

## Procedure

1. Log on to the Administration Portal.
2. Click **User Options > Downloads**. The Downloads page opens.
3. Choose one of the following options:

Option	Description
Executable file (Windows only)	<ol style="list-style-type: none"><li>1. Click <code>aos_console_setup.exe</code>.</li><li>2. When prompted, click <b>Open</b> or <b>Run</b>.</li><li>3. Run the installer and follow the onscreen instructions to install the Console to the default location or a location that you choose.</li></ol>
Binaries files	<ol style="list-style-type: none"><li>1. Click <code>AOSConsole_ver.zip</code>.</li><li>2. When prompted, click <b>Save</b> to download the compressed file to your local machine.</li><li>3. Extract the contents of the compressed file to your preferred location, maintaining the directory structure of the contents.</li><li>4. Create a shortcut to the script file (<code>run.sh</code> or <code>run.bat</code>) to quickly open the Console.</li></ol>

4. You can run the Assist On-site Configuration Wizard after your first download the Remote Support Console installation package. For more information, see "Customizing the branding of the Remote Support Console" on page 63.

## Starting the Remote Support Console

You can start the Remote Support Console using a shortcut or script file.

## Procedure

Choose one of the following options:

- (On **Windows systems**) Click **Start > All Programs > IBM > AOS Console**.
- (On **Linux systems**) Run the script file, `run.sh`, in `rsc_root`.

---

## Configuring the Remote Support Console


You can configure the Remote Support Console to use default values for auditing, transferring files, and establishing connections in the Console Settings window. You can also set the details for the preferred Relay Server to which to connect.

## About this task

For more information about Console Settings window and the Advanced connection settings window that opens when you click **Advanced settings** in the **Relay Settings** area, see “Console Settings window” on page 23.

**Note:** You cannot configure the Remote Support Console during a support session.

## Procedure

1. Click  and select **Configuration**. The Console Settings window opens.

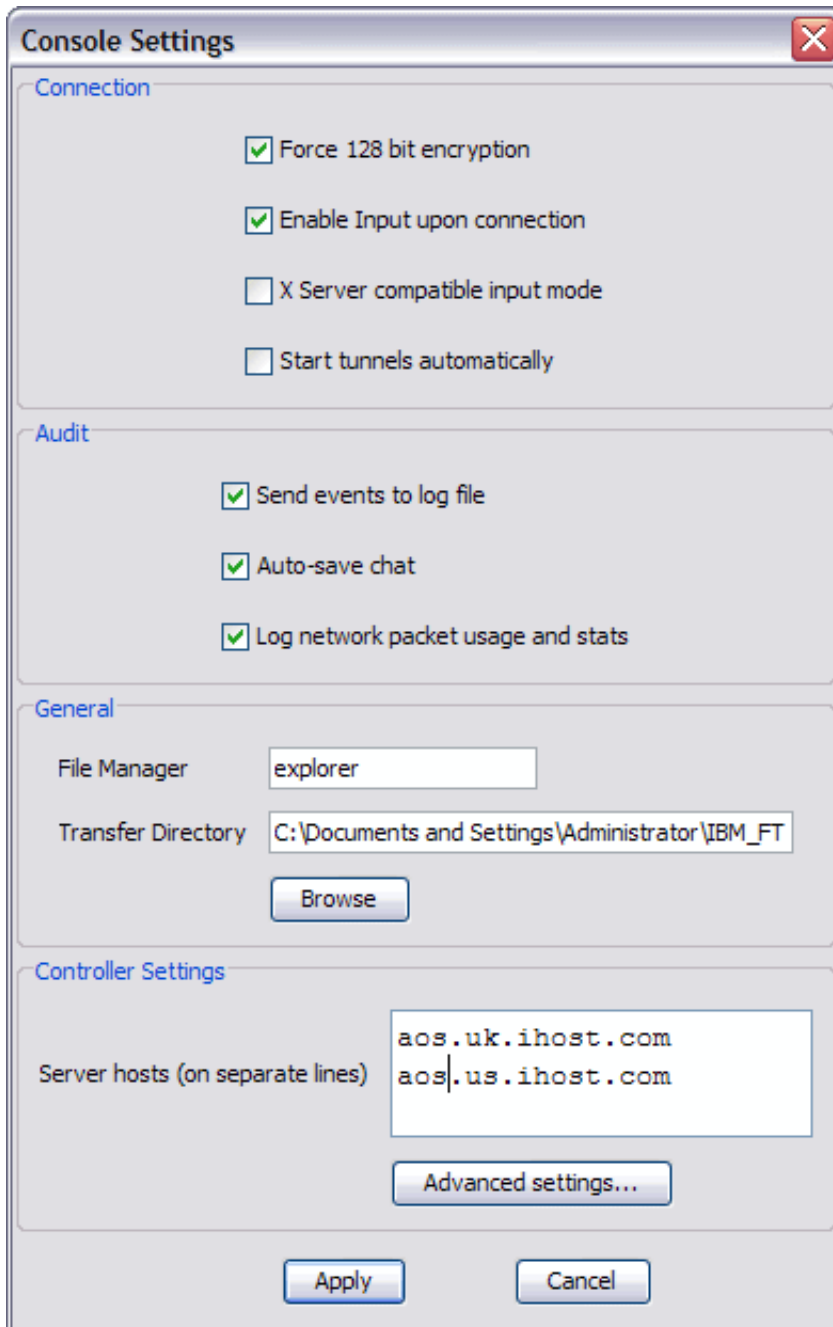


Figure 6. Console Settings window

2. Select the check boxes and enter the details that you want to set as the default settings.
3. In **Relay hosts** text area, enter the IP address or fully qualified host name for each Relay Server on a separate line. For example, for the Americas region, enter `aos.us.ihost.com` and then `aosback.us.ihost.com` on the next line. For the EMEA region, enter `aos.uk.ihost.com` and for the AP region, enter `203.141.90.53`.

**Important:** You must enter the details of the Relay Server for your geographical region on the first line. For more information about the IP addresses, see Chapter 5, “Relay Server,” on page 115.

- To set the preferred ports for the Relay Server and details for a proxy server that connects to the Relay Server, click **Advanced settings**. The Advanced Connection Settings window opens.

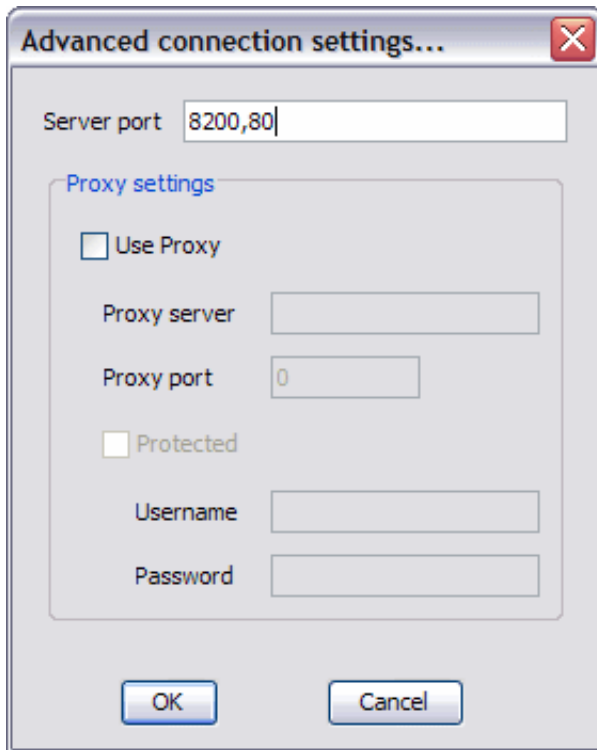


Figure 7. Advanced Connection Settings window

- In the **Relay ports** field, type the port numbers for the Relay Server, separated by commas.
- Enter the proxy server configuration details if the connection to the Relay Server must be routed through a proxy server. Click **OK**.
- Click **Apply** to save the configuration settings.

## Console Settings window

The Console Settings window lets you configure default settings for the Remote Support Console.

### Elements of the Console Settings window

Table 4. Console Settings window elements

Element	Description
<b>Connection settings</b>	
Force 128 Bit Encryption	Select this check box to force every support session to use 128-bit session encryption. <b>Important:</b> Assist On-site uses 128-bit encryption in all support sessions regardless of this setting.

Table 4. Console Settings window elements (continued)

Element	Description
Enable Input upon connection	Select this check box to turn on input control of the local mouse and keyboard automatically after each connection is established. This setting activates the <b>Enable/Disable local input</b> toggle icon in the toolbar.
X server compatible input mode	Select this check box to ensure that text characters are properly input in an X-terminal session on the target machine.
Start tunnels automatically	Select this check box to automatically start port forwarding sessions for the local ports configured to be forwarded to the remote host machines and ports. <b>Note:</b> The Assist On-site administrator must assign the port forwarding permissions to you before you can start port forwarding sessions.
<b>Audit settings</b>	
Send events to log file	Select this check box to write auditing and events to a log file on your local system. The log file is stored in the operating system's home directory, within the .AOSConsole directory.
Auto-save chat	Select this check box to write chats to log files on your local system. The log file is stored in the operating system's home directory, within the .AOSConsole directory and has a file name based on the name of the customer and the IP address.
Log network packet usage and stats	Select this check box to write diagnostics and statistics about the network connection to a log file on your local system. The log file is stored in the operating system's home directory, within the .AOSConsole directory.
<b>General settings</b>	
File Manager	Enter the application that overrides the Console's default file manager, which it uses for operations such as opening the file transfer directory.
Transfer Directory and Browse	Enter or click <b>Browse</b> to select the default transfer directory that is used in file transfers.
<b>Relay settings</b>	
Relay hosts (on separate lines)	Enter the IP address of the Relay Server to use to establish the connection for the support session.  <b>CAUTION:</b> <b>Changing these settings might affect the ability to successfully establish a connection.</b>



Table 4. Console Settings window elements (continued)

Element	Description
Advanced settings	Click to set the port number and proxy server details for the Relay Server in the Advanced connection settings window. For more information about the elements of this window, see Table 5.
Apply	Click to save the configuration settings.
Cancel	Click to close the window without saving any changes.

## Elements of the Advanced Connection Settings window

Table 5. Advanced Connection Settings window elements

Element	Description
Relay port	Enter the port numbers for the Relay Server that you entered in the <b>Relay hosts</b> text area.
<b>Proxy settings</b>	
Use Proxy	Select this check box if you need to use a proxy server for the Relay Server.
Proxy server	Enter the IP address of the proxy server.
Proxy port	Enter the port number for the proxy server.
Protected	Select this check box if the proxy server requires user authentication.
Username	Enter the user name for authentication on the proxy server.
Password	Enter the password for the user name.
OK	Click to save the advanced connection settings.
Cancel	Click to close the window without saving any changes.

## Using the Remote Support Console

Support engineers can connect to target machines and provide support by performing certain functions on that target system using the Remote Support Console.

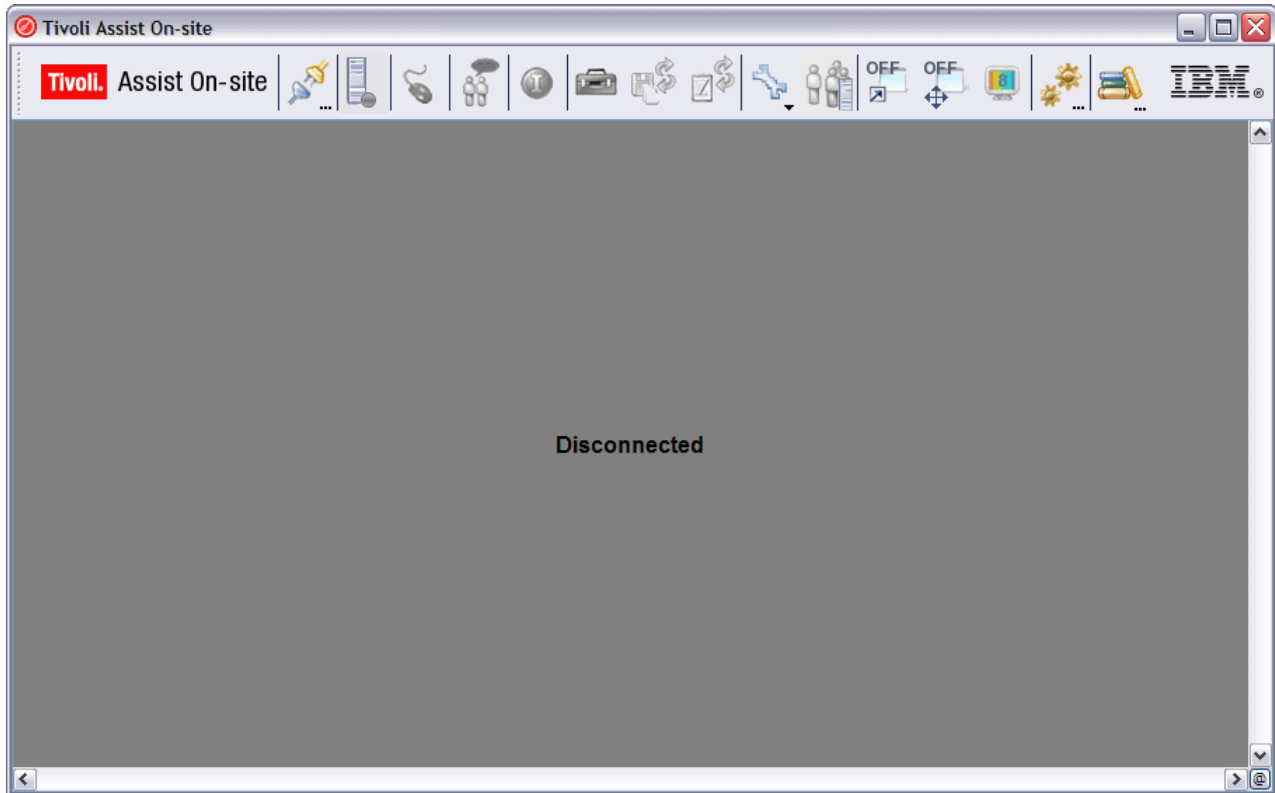


Figure 8. Remote Support Console interface

### Remote Support Console functions

Table 6 describes the main functions of the Remote Support Console that you can access from the toolbar.

Table 6. Remote Support Console functions


Function and toolbar icon	Description
Open or close session 	Establish a connection to the Relay Server upon first usage. Create or join a support session. For more information, see “Support session management” on page 28.

Table 6. Remote Support Console functions (continued)




















Function and toolbar icon	Description
<p>Start recording</p> 	<p>Record all or part of the support session for playback and potential export afterwards. Stop recording the support session using the toggled icon. For more information, see “Recording sessions” on page 38.</p>
<p>Stop recording</p> 	
<p>Enable/Disable local input</p>  	<p>Forward mouse movements and keyboard strokes between the controller and target machines. With inputs enabled, you can perform operations on your local machine without affecting the mouse or keyboard status of the target machine. For more information, see “Turning on or off local input control” on page 38.</p>
<p>Chat</p> 	<p>Open the Chat window for real-time communication with the customer. You can request to change the session mode in the Chat window regardless of the current session mode. For more information, see “Chatting with the customer” on page 38.</p>
<p>Target system information</p> 	<p>Gather information about the target system. For more information, see “Getting the target system information” on page 40.</p>
<p>Actions menu</p> 	<p>Contains dynamic menu items to perform common operations or to quickly open specific applications. For more information, see “Available actions on the target machine” on page 41.</p>
<p>File Transfer menu</p> 	<p>Contains menu items to transfer files between the local and target machines. For more information, see “File transfer functions” on page 44.</p>
<p>Clipboard menu</p> 	<p>Contains menu items to transfer local clipboard information (text only) between the local and target machines. For more information, see “Copying clipboard text from the local machine” on page 47.</p>
<p>Collaboration</p> 	<p>Turn on collaboration between many support machines and the target machine. For more information, see “Working in collaborative sessions” on page 55.</p>

Table 6. Remote Support Console functions (continued)

Function and toolbar icon	Description
Console Tools menu 	Contains menu items to use the drawing or highlighting tools, to save screen shots of the remote system, and to manually set the optimal video settings for the support session. For more information, see “Console tools” on page 47.
Turn on or off scaled view  	Turn on or off the reduction in size of the target desktop to fit within the Remote Support Console window. For more information, see “Turning on or off scaled view” on page 60.
Turn on or off autoscroll  	Turn on or off automatic scrolling of the support session view. For more information, see “Turning on or off autoscroll” on page 61.
Switch between 8-bit and 24-bit color  	Switch between 8-bit and 24-bit color for the target session view. For more information, see “Turning on or off Truecolor” on page 61.
Configure Console 	Configure the Remote Support Console settings. For more information, see “Configuring the Remote Support Console” on page 20.
Help menu 	View the Assist On-site help, information about the Remote Support Console version, get support, and open the Administration Portal.

## Support session management

When you first open and use the Remote Support Console, you must establish and authenticate yourself on the Relay Server. You can run one or many support sessions while you have the Remote Support Console open, but you must request a new connection code for each support session. You can also request that the customer change the session mode during a support session. Either you or the customer can end a support session.

## Connecting to a Relay Server

Before you can create a support session, you must connect to and authenticate your User ID on the Relay Server. If you are an IBM support engineer and a member of an Assist On-site BlueGroup, you can use your IBM intranet ID to authenticate on the Relay Server.

### Before you begin

Ensure that you have configured connection to the preferred Relay Server. For more information, see “Configuring the Remote Support Console” on page 20.

**Note:** You only need to successfully connect to the Relay Server once while you have the Remote Support Console opened.

### About this task

When you connect, you can also save your user ID and password to avoid typing them again at future logons. The Console saves these details to your local machine, and displays them in the fields when you next view the Authenticate Session window.

### Procedure

1. Click  . The Authenticate Session window opens.

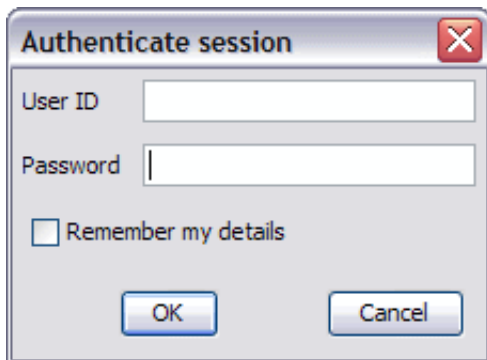


Figure 9. Authenticate Session window

2. In the **User ID** field, type your Assist On-site User ID that might also be your IBM intranet ID.
3. In the **Password** field, type your password.
4. To save your user ID and password to your local machine, select **Remember my details**.

### Creating support sessions for external customers

When the Remote Support Console is in disconnected status, either because it just has been loaded or because a previous support session has finished, you can create another support session. You follow the standard Assist On-site security protocols for an external customer. The external customer downloads the Remote Support Utility from the Assist On-site Support Web site.

## Before you begin


The Remote Support Console attempts to establish a connection with the Relay Server that has been configured in the Console Settings window. If it is the first connection since the Console was loaded or a previous authentication attempt was unsuccessful, you must enter your user details to authenticate your connection to the Relay Server. While the Remote Support Console is running in any successive session after a successful authentication, the Console uses the same authentication details for each support session.

Ensure that you have connected to a Relay Server. For more information, see “Connecting to a Relay Server” on page 29.

## About this task

**Note:** All support sessions in Assist On-site are forced to use 128 Bit encryption.

## Procedure

1. Click  . The Tivoli Assist On-site window opens.

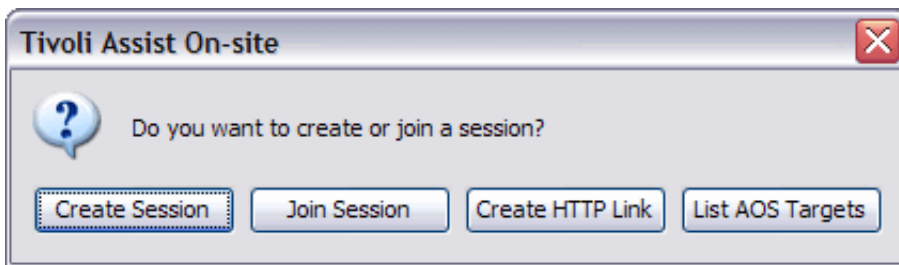


Figure 10. Tivoli Assist On-site window

2. Click **Create new session**.

**Important:** Do not use **Create HTTP Link** to create a session for an external IBM customer.

The Connection Code window opens.

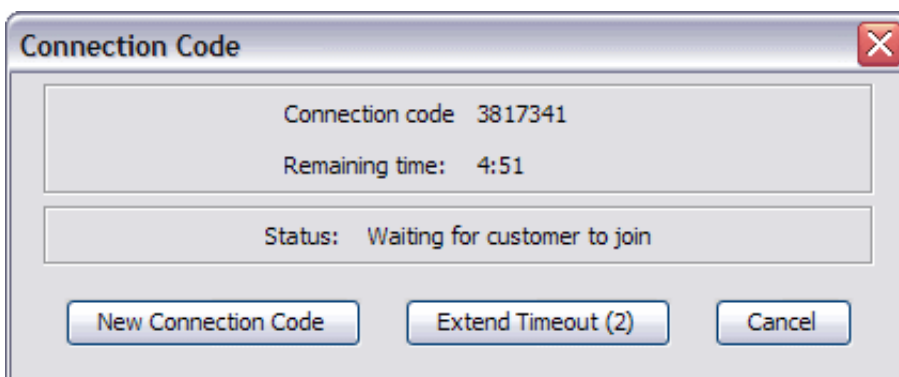


Figure 11. Connection Code window

3. The customer enters the connection code in the Assist On-site Support Web site and uses the downloaded Remote Support Utility to connect to the Relay Server. A Waiting for user acceptance message is displayed in the Console.
4. After the customer initiates the support session and selects the session mode, the Console displays the target system view, or if the customer selects the chat mode, a chat window replaces the main window of the Remote Support Console.

## Results

The support session starts with an established connection to the Relay Server.

While the support session is active,  replaces  to indicate that a secure connection is in progress.

## Creating support sessions for internal IBM customers

When the Remote Support Console is in disconnected status, either because it just has been loaded or because a previous support session has finished, you can create another support session. You can bypass the standard Assist On-site security protocols for an internal IBM customer. You can provide a URL to download the Remote Support Utility from it.

## Before you begin


The Remote Support Console attempts to establish a connection with the Relay Server that has been configured in the Console Settings window. If it is the first connection since the Console was loaded or a previous authentication attempt was unsuccessful, you must enter your user details to authenticate your connection to the Relay Server. While the Remote Support Console is running in any successive session after a successful authentication, the Console uses the same authentication details for each support session.

Ensure that you have connected to a Relay Server. For more information, see “Connecting to a Relay Server” on page 29.

## About this task

**Note:** All support sessions in Assist On-site are forced to use 128 Bit encryption.

## Procedure

1. Click  . The Tivoli Assist On-site window opens.

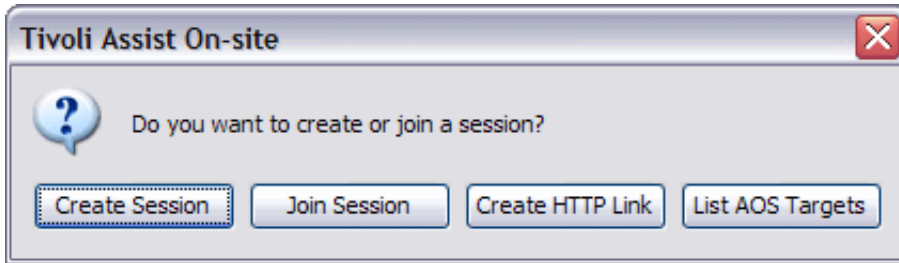


Figure 12. Tivoli Assist On-site window

2. Click **Create HTTP Link** and click **OK** in the confirmation window to confirm that the session is for an internal IBM customer or a customer with a separate license agreement.

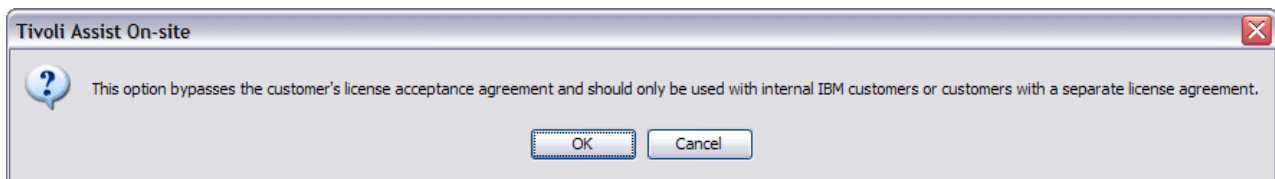


Figure 13. Session for internal customers only confirmation window

**Important:** Do not use **Create HTTP Link** to create a session for an external IBM customer.  
The Support session details window opens.

Figure 14. Support session details window

3. Enter the following details:
  - a. In the **Customer Name** field, type the name of the IBM customer.
  - b. In the **Case Number** field, type the case number.
  - c. From the **Geography** list, select the location of the IBM customer and the Relay Server to which the customer connects.
  - d. In the **Customer Number** field, type the IBM customer number.
  - e. Click **OK**.



The Connection Code window opens.

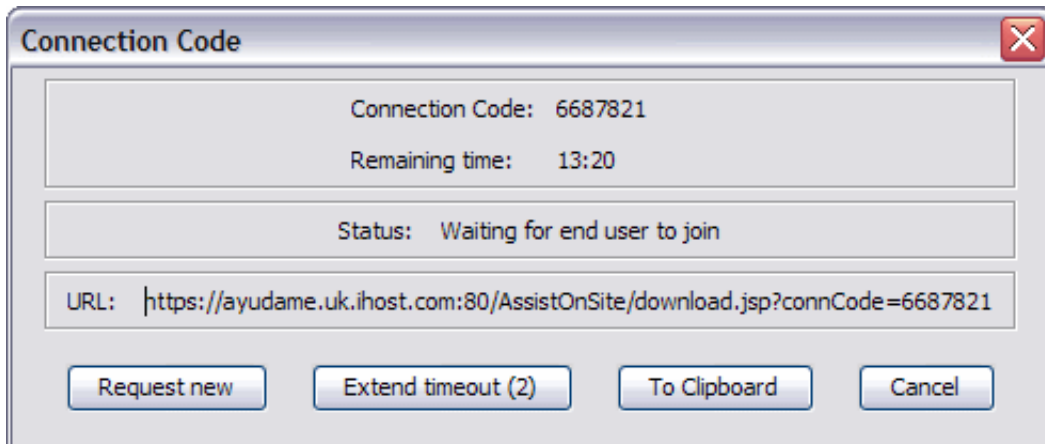


Figure 15. Connection Code window for internal IBM customers

4. Click **To Clipboard** to copy the URL to your clipboard. You can send the URL to the customer
5. The customer opens the URL, enters the connection code, and uses the downloaded Remote Support Utility to connect to the Relay Server. A *Waiting for user acceptance* message is displayed in the Console.
6. After the customer initiates the support session and selects the session mode, the Console displays the target system view, or if the customer selects the chat mode, a chat window replaces the main window of the Remote Support Console.

## Results


The support session starts with an established connection to the Relay Server.

While the support session is active,  replaces  to indicate that a secure connection is in progress.

## Creating unattended support sessions

The support engineer can run lights-out or unattended support sessions, including port forwarding sessions, during which the customer is not in attendance. The Remote Support Console displays a list of target machines on which the Assist On-site Support Service runs. It also displays the set of remote host machines on which unattended port forwarding sessions are configured and authorized.

## Procedure

1. Click  . The Tivoli Assist On-site window opens.

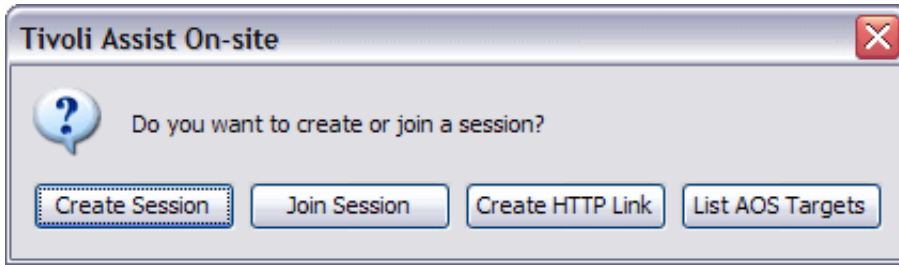


Figure 16. Tivoli Assist On-site window

2. Click **List AOS Targets**.

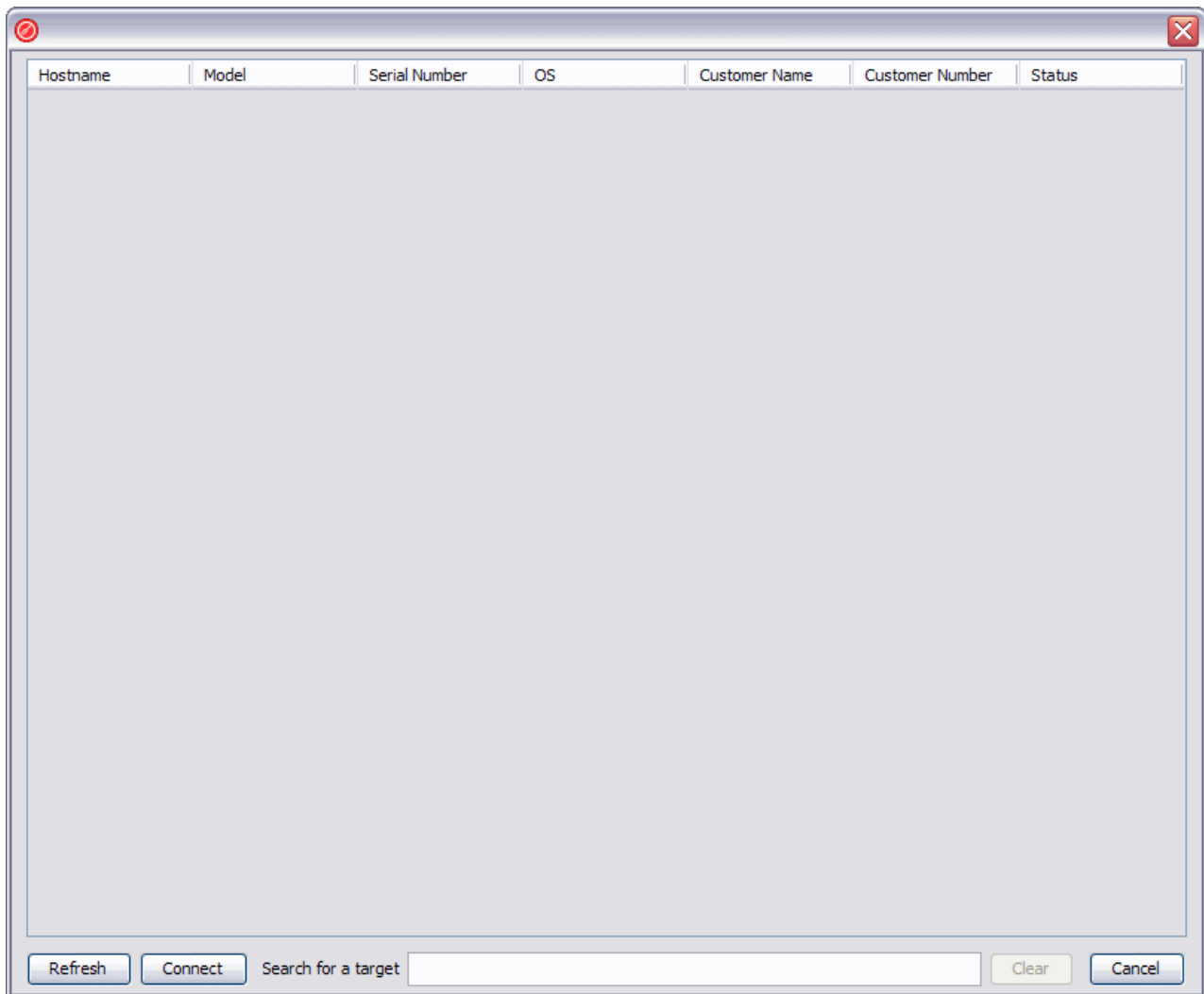


Figure 17. List AOS Targets window

3. Choose one of the following options:

Option	Description
Standard lights-out or unattended session	Select the remote host name and click <b>Connect</b> .

Option	Description
Unattended port forwarding session	<p>Select the remote host name and click <b>Connect</b>. You can configure port forwarding and set which local ports to forward to which remote host machines and ports on the Configure Port Forwarding window. See “Configuring and starting port forwarding sessions in the Console” on page 53.</p> <p><b>Note:</b> The Assist On-site administrator must assign the port forwarding permissions to you before you can start port forwarding sessions.</p>

## Starting Assist On-site in context

You can start Assist On-site from within the session of the third-party support tool such as Technical Support Chat.

### Procedure

From the third-party support tool, you can start Assist On-site. It opens the Remote Support Console on the support engineer's machine, creates a support session, and obtains the connection code. Assist On-site also creates a connection file that contains the instructions for the customer to download the Remote Support Utility from the specified Assist On-site URL.

**Note:** The third-party support tool provides the launch mechanism, for example, a menu item in the support tool that executes the command-line interface and runs Assist On-site.

## Changing between session modes

You can request that the customer change between session modes during a support session. The customer can then accept the session mode change.

### Procedure



1. Click  to open the Chat window on your machine.

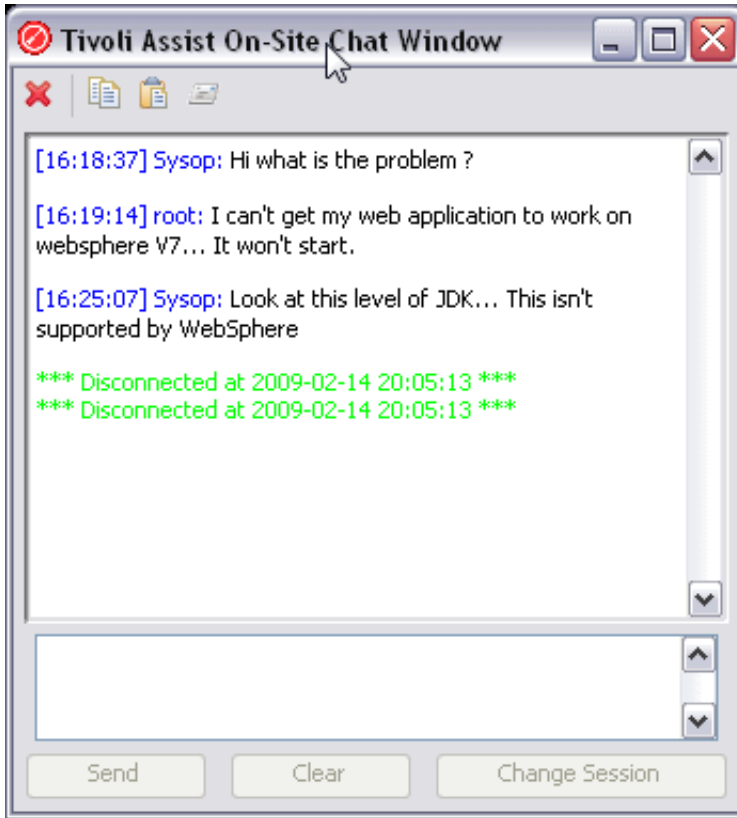


Figure 18. Chat window

2. Click **Change Session** to request to the customer to change to another session mode. The Change session mode window opens on your machine.

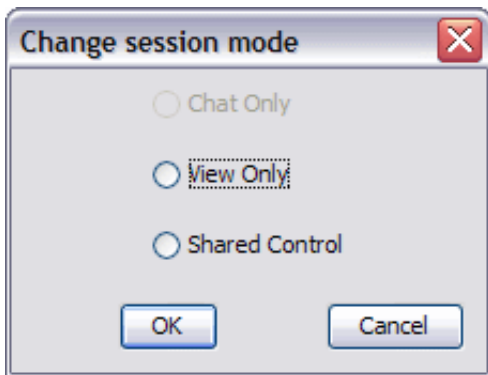


Figure 19. Change session mode window

**Important:** The choice of session modes is dependent on the default permissions of the team to which the support engineer belongs, the permissions of the support engineer, and the type of session. The current session mode is a disabled option.

Table 7. Session modes and options

Option	Description
Guidance	Select to change the support session to Guidance mode.

Table 7. Session modes and options (continued)

Option	Description
Shared View	Select to change the support session to View Only mode.
Shared Control	Select to change the support session to Shared Control mode.
Port Forwarding	Select to change the support session to a port forwarding session. <b>Note:</b> Ensure that your customer has configured port forwarding. The Assist On-site administrator must assign the port forwarding permissions to you before you can start port forwarding sessions.

3. Select the mode to change, and click **OK**. A message is displayed on the target machine:

'Allow user <username> to change session to <new mode> '

4. The customer must click **Yes** to allow the change. An acceptance message is displayed on your machine. A similar message is displayed on the target desktop to notify the customer that the session mode has changed.

When the session mode changes to port forwarding, the Port Forwarding window opens in the Console. For more information, see “Configuring and starting port forwarding sessions in the Console” on page 53.


## Ending support sessions

You can end the support session in the Remote Support Console.

### Procedure

1. Choose one of the following options:



- Click .
- Close the Remote Support Console, for example, in Windows systems click the X in the Console.
- In the Session in Progress window, click **End Session**.

The confirmation dialog box opens.

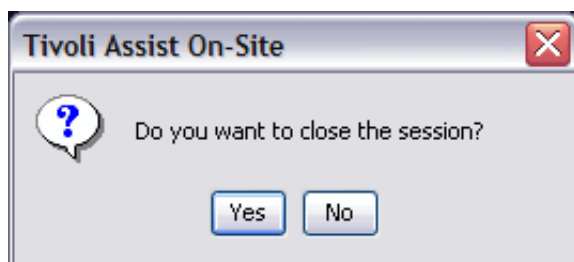



Figure 20. Close session confirmation dialog box

2. Click **Yes**. The support session ends and the target desktop is no longer shared.

## Recording sessions

The Remote Support Console has a recording function to let support engineers record all or part of a support session, providing that the customer allows the support session to be recorded.

### Procedure

1. At any stage during a support session, you can click  to start recording.

2. Click  to stop recording.

**Note:** The customer is advised of both actions.

Recorded sessions are stored and accessible through the Administration Portal, which also provides playback and export functions. You can view the recorded session using the Assist On-site Player.

## Turning on or off local input control


When a support session is in the **Shared Control** mode, you can turn on or off input control of your local mouse and keyboard using the **Enable/Disable Input** toggle icon on the toolbar.


### About this task

**Note:** You can turn on local input control by default in the configuration settings of the Remote Support Console. For more information, see “Configuring the Remote Support Console” on page 20.

### Procedure

Depending upon the current status of the local input control, click one of the following icons:

- To turn on local input control, click  .


- To turn off local input control, click  .

## Chatting with the customer

You can chat with the customer during a Chat Only session or during another session mode. During a Chat Only session, the Remote Support Console is replaced with the Chat window. For other session modes, the Remote Support Console and the Chat window can be minimized.

### Procedure

1. To open the Chat window, choose one of the following options:

- In session modes other than Chat Only, click  .

- Have the customer start a support session in Chat Only mode.  
The Chat window opens.

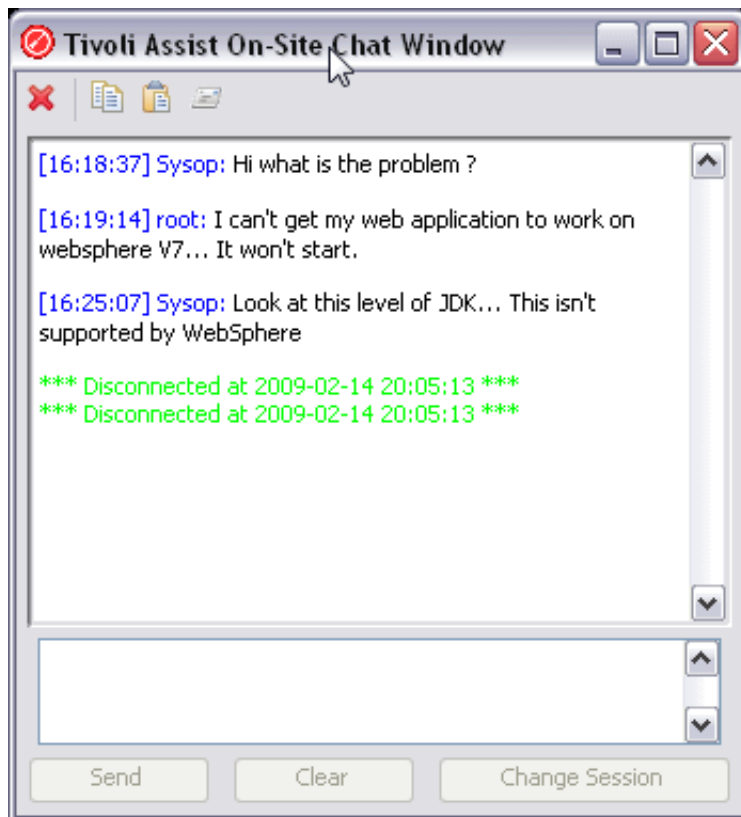



Figure 21. Chat window

2. Type the text message that you want to send, and click **Send** or press **Enter**.
3. If you need to request a change in the session mode while chatting, click **Change Session**. For more information, see "Changing between session modes" on page 35.
4. During or at the end of the chat, you can e-mail the transcript of the chat to the customer or another support engineer. Click . A new e-mail window opens, with the chat transcript automatically attached to the e-mail.

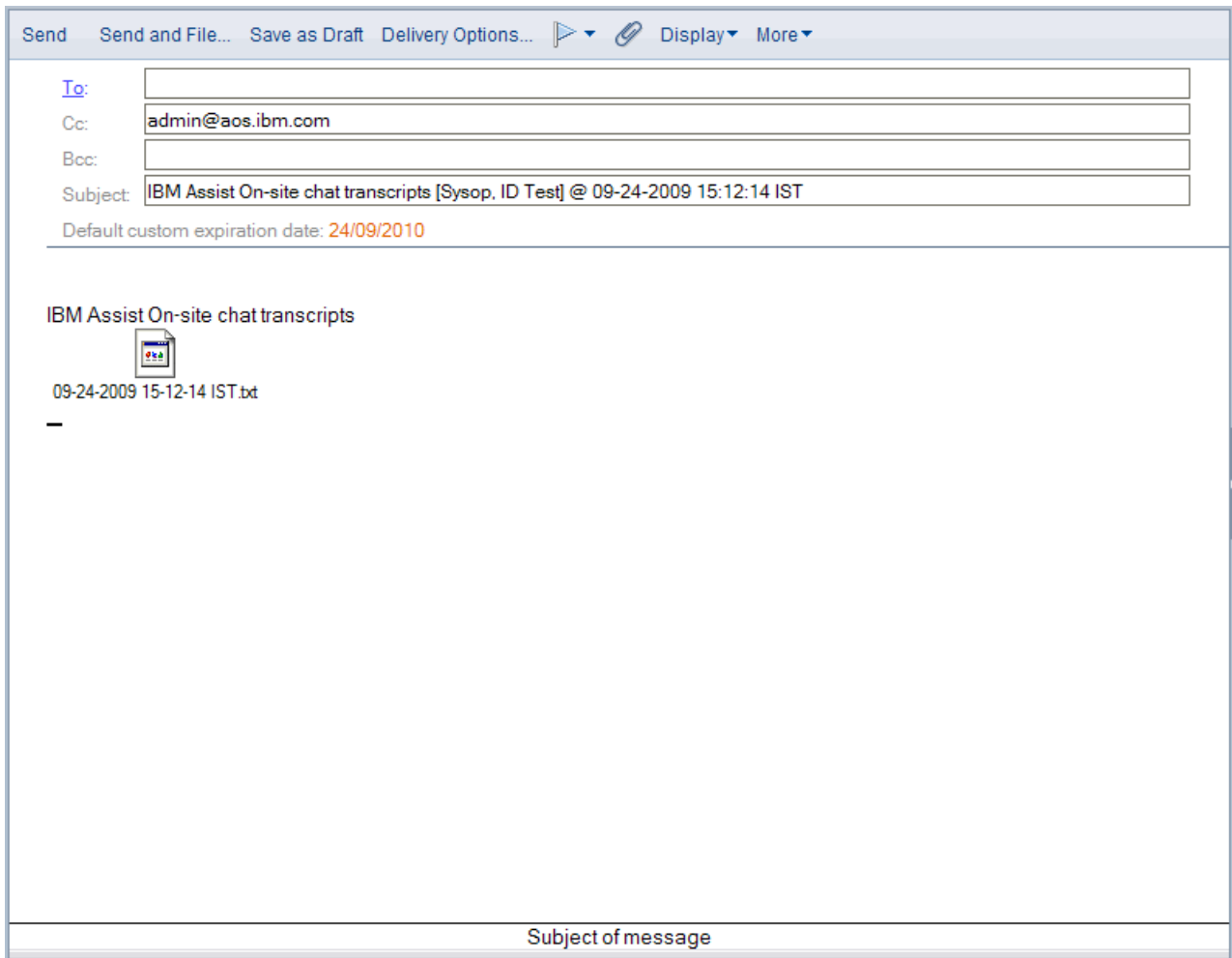


Figure 22. E-mail transcript window


5. You can close or minimize the Chat window.

## Getting the target system information

During a support session, you can retrieve information about the target system using the IBM System Information Gatherer to support troubleshooting. This very small, powerful, and highly configurable program obtains information such as the target system's details, network devices and status, and a list of running processes.

### Procedure



Click . A text file is automatically created on the target machine and sent back to be displayed in the Console.

### Results

The file is saved in the file transfer directory of the Console for further reference, but it is overwritten the next time that you run this function in the same or a new support session.



## Available actions on the target machine

You can perform certain actions on the target machine during a session using the **Perform actions on client** dynamic menu. The set of available actions is dependant on the operating system of the target machine and the session mode.



You can access the **Perform actions on client** dynamic menu using the .

Table 8 outlines the available actions for each operating system and session mode.

*Table 8. Available actions on the target machine*

Actions	Description	Operating systems	Session modes
<b>Guidance Tool</b>	Turns on or off the Guidance tool. For more information, see “Guiding the customer to perform actions” on page 42.		Guidance
<b>Drawing Tool</b>	Turns on or off the drawing tool. For more information, see “Drawing on the target desktop” on page 49.		Guidance <b>Note:</b> This tool is available in Shared Control mode in the Console Tools menu.
<b>Highlighting Tool</b>	Turns on or off the highlighting tool. For more information, see “Drawing on the target desktop” on page 49.		Guidance <b>Note:</b> This tool is available in Shared Control mode in the Console Tools menu.
<b>Clear Instructions</b>	Clears the guidance symbols and drawings from the target desktop.		Guidance <b>Note:</b> This tool is available in Shared Control mode in the Console Tools menu.
<b>Lock Workstation</b>	Locks the target workstation.		Shared control
<b>Inject ALT+F4</b>	Closes the active window on the target machine.		Shared control
<b>Inject ALT+TAB</b>	Switches between active windows on the target machine.		Shared control
<b>Inject CTRL+ALT+DEL</b>	Opens the Windows Security Center window depending on the Windows configuration.	Windows	Shared control
<b>Open URL</b>	Opens the Open URL window. For more information, see “Opening URLs on the target” on page 43.	Windows	Shared control

Table 8. Available actions on the target machine (continued)

Actions	Description	Operating systems	Session modes
<b>Device Manager</b>	Opens the Device Manager window for the target machine.	Windows	Shared control
<b>Control Panel</b>	Opens the Control Panel window for the target machine.	Windows	Shared control
<b>Command Prompt</b>	Opens the command-line interface on the target machine.	Windows	Shared control
<b>On-screen Keyboard</b>	Opens the On-Screen Keyboard window on the target machine.	Windows	Shared control
<b>System Settings</b>	Opens the Windows Systems Properties window on the target machine.	Windows	Shared control
<b>Computer Management</b>	Opens the Windows Computer Management window on the target machine.	Windows	Shared control
<b>Add/Remove Programs</b>	Opens the Windows Add or Remove Programs window on the target machine.	Windows	Shared control

## Sending commands to the target machine

You can perform certain actions on the target machine during a support session using the **Perform actions on client** dynamic menu.

### Procedure



Click  and select the action that you want to perform.

**Note:** It is a dynamic menu that changes depending upon the operating system on the target machine and the session mode.

### Guiding the customer to perform actions

When in Guidance mode, you can guide the customer on which actions to perform on the target system using the Guidance tool. You can select the action symbol and use your local mouse to position the action symbol in the area of the target desktop where the customer should perform the action. The customer must then use the target mouse to mimic the action symbol and perform the correct action.

### Before you begin


Ensure that the session mode is Guidance; otherwise, the Guidance tool is disabled.

## About this task

**Tip:** You can also use the drawing and highlighting tools to guide the customer. For more information, see “Drawing on the target desktop” on page 49.

### Procedure



1. Click  and select **Guidance Tool**.
2. Click and select one of the following options:

Option	Description
Cancel	Cancel the last action symbol that you selected.
Move	Direct the customer to move the target cursor to the position of the symbol.
Single Click	Direct the customer to click the target mouse button once.
Double Click	Direct the customer to click the target mouse button twice.
Drag Start	Direct the customer to click the target mouse button and start to drag the mouse in the direction of the symbol.
Drag End	Direct the customer to continue to drag the target mouse in the direction of the symbol and then release the target mouse button at the final position of the symbol.

**Note:** You can direct the customer to click the relevant left or right button of the target mouse when you select the left or right button of your mouse after selecting **Single Click** or **Double Click**.

3. After the customer performs the actions, you can clear the action symbols from



the target desktop. Click  and select **Clear Instructions**.

### Opening URLs on the target

You can open a URL in the default Web browser on the target machine in the Open URL window. You can manually enter the URL or you can select the URL from the favorites lists.

### Procedure



1. Click , and select **Open URL**. The Open URL window opens.

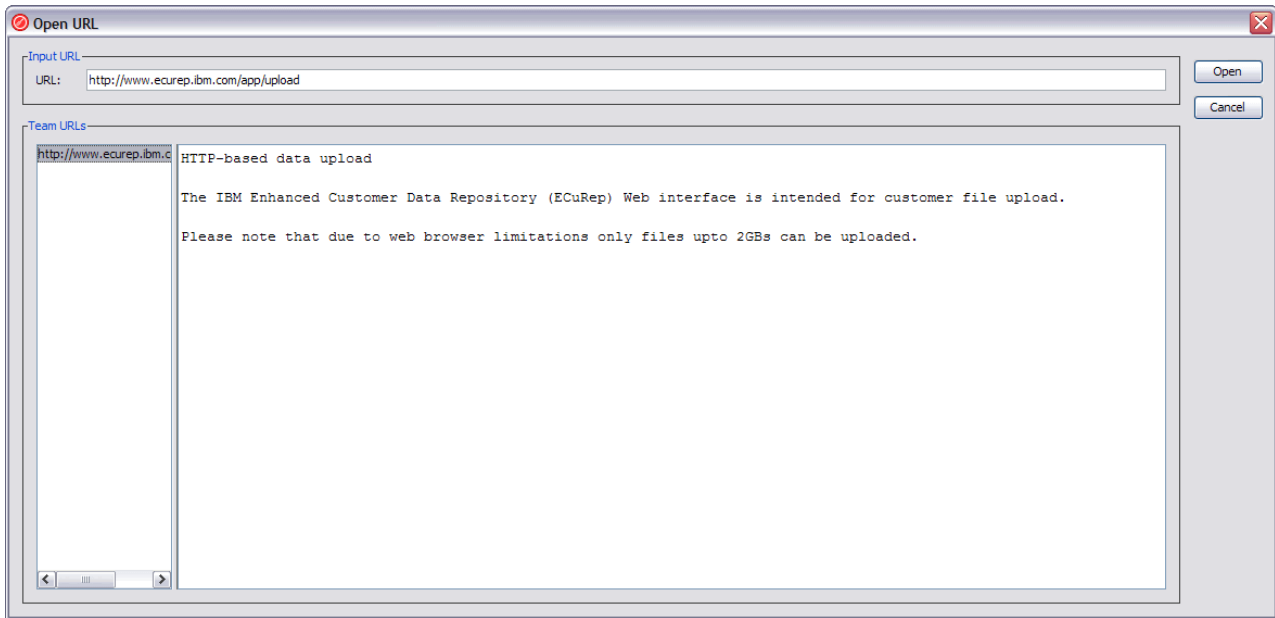


Figure 23. Open URL window

2. Do one of the following options:
  - In the **URL** field, type the URL for the Web site that you want to open.
  - In the **Team URLs** list, select the URL that you want to open.
3. Click **Open**.


### Propagation of parent team URLs to subteams

When Assist On-site administrators add team URLs, they can choose to propagate the URLs to the teams of the parent team. Support engineers, who are members of these subteams, can also open these URLs. Administrators can turn on this function by selecting the **Propagate to subteams** check box on the Create team URL or Edit team URL pages in the Assist On-site Administration Portal. This function is useful when support teams want to use a standard URL to upload files from customers' machines to a support web site for further diagnostic checking.

Assist On-site provides support for the IBM Client Diagnostic Data Repository (CDDR) strategy in the exchange of data through the propagation of team URLs and file transfer functions. For example, during an Assist On-site session, an IBM Support engineer can open the URLs for ECuRep or Testcase FTP server that have been propagated from the parent team and upload the files by using the URL that is fastest for the geography of the customer.

### File transfer functions

The Remote Support Console has File Transfer functions such as send and receive files, and open the file transfer directory on your machine.

You can access these functions from the File Transfer menu, , on the toolbar.

## Sending files to the target

You can send a file to the target machine during a support session using the **Send file** menu item in the **File Transfer** menu.

### About this task

**Note:** The file is transferred to the default file transfer directory on the target machine.

### Procedure



1. Click  and select **Send file**. The Send File to Client window opens.

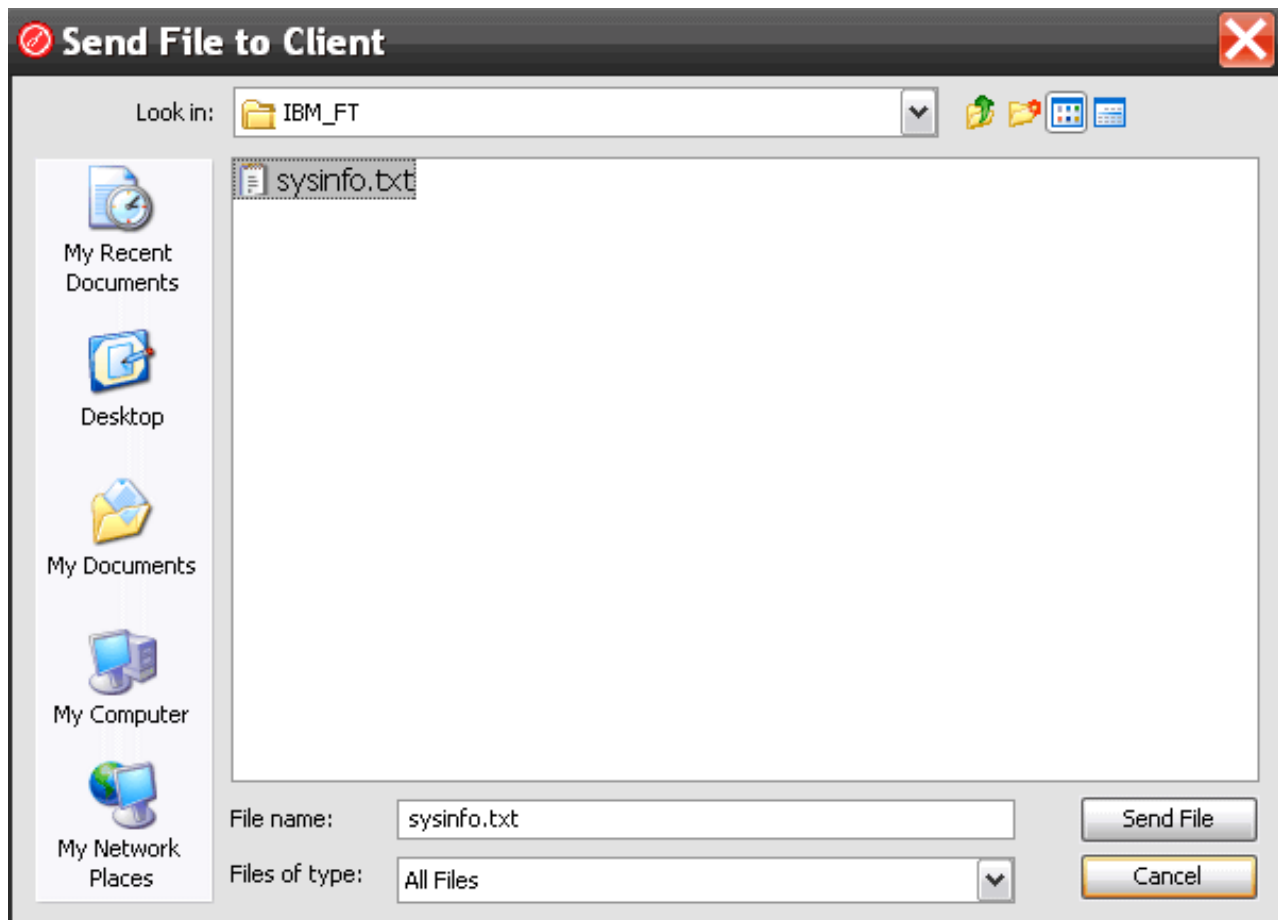


Figure 24. Send File to Client window

2. Browse to and select the file that you want to send, and click **Send File**. A progress bar indicates how much of the file is transferred. When the file transfer is complete, a confirmation message is displayed.

## Receiving files

You can retrieve a file from the target machine during a support session using the **Pull file** menu item in the **File Transfer** menu.

## About this task

**Note:** The file is transferred to the default file transfer directory on your local machine.

## Procedure



1. Click  and select **Pull file**. The Choose file to pull window on the target machine opens.

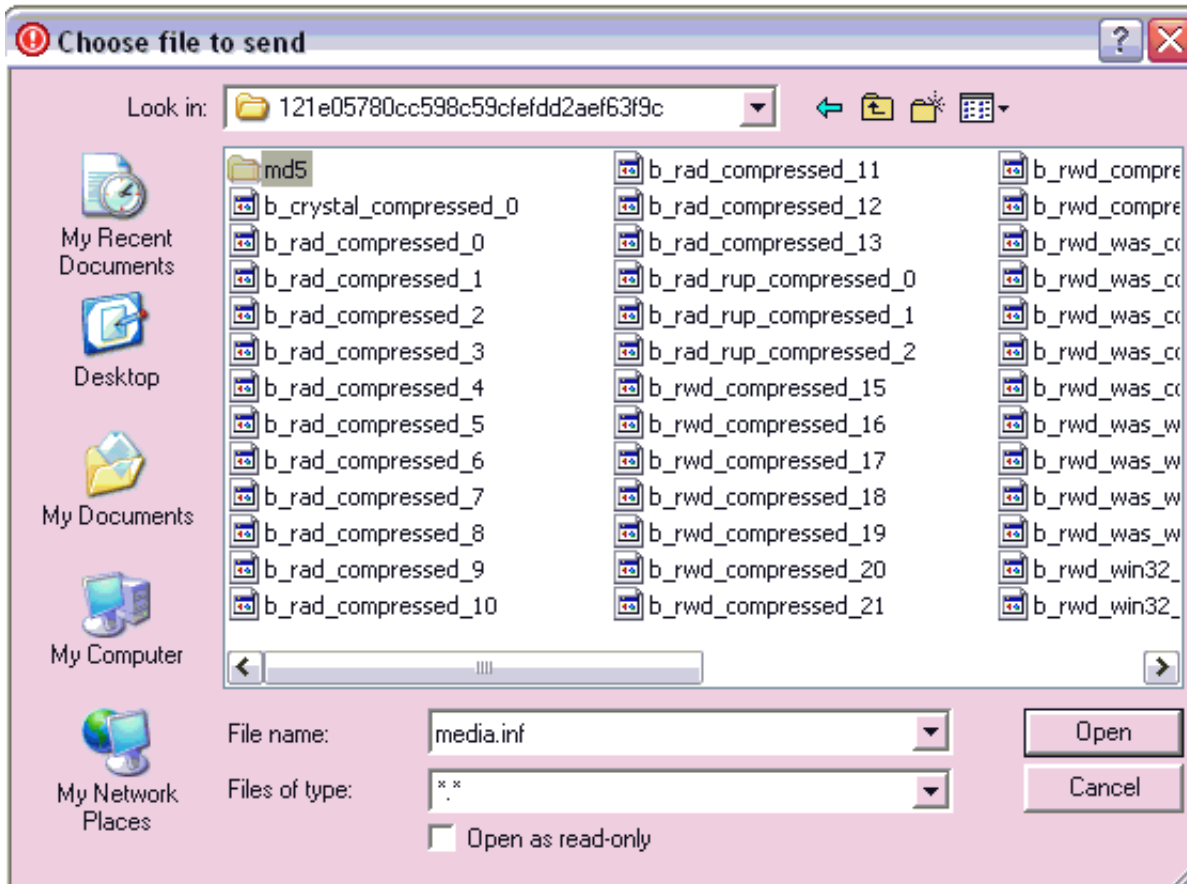


Figure 25. Choose file to pull window

2. Browse and select the file that you want to receive and click **Open**. A progress bar indicates how much of the file is transferred. When the file transfer is complete, a confirmation message is displayed.

## Opening the file transfer directory

You can open the file transfer directory that contains the retrieved file from the remote machine using the **Open transfer folder** menu item in the **File Transfer** menu.


## About this task

The Remote Support Console uses the most appropriate file manager for the operating system on which it is running. You can override the file manager and the file transfer directory in the console configuration settings. For more information,

see “Configuring the Remote Support Console” on page 20.

### Procedure



Click  and select **Open transfer folder**. A file manager window opens showing the file transfer directory. The default directory is named *IBM\_FT*.

## Clipboard functions

The Remote Support Console has clipboard functions such as copy and paste files between your local machine and the target machine.



You can access these functions from the Clipboard menu, , on the toolbar.

### Copying clipboard text from the local machine

You can copy the text contents of your local clipboard in a support session using the **Clipboard transfer** menu.

### Procedure



Click  and select **Send clipboard text**.

### Copying clipboard text from the target machine

You can copy the text contents of the remote clipboard in a support session using the **Clipboard transfer** menu.

### Procedure



Click  and select **Pull clipboard text**.

## Console tools

The Remote Support Console provides additional tools for a support session. These tools include entering text quickly; using drawing and highlighting tools to draw attention to areas of the target desktop; storing an image with the current status of the target desktop; and optimizing the target video settings.



You can access these tools from  on the toolbar.

### X Server compatible input mode

Assist On-site supports multiple operating systems including UNIX-based. The Remote Support Console has a X Server compatible input mode to let you correctly enter text characters during an X-terminal session on the target machine.


### Turning on or off X Server compatible input mode:

You can turn on or off X Server compatible input using the Console tools or Console configuration settings. You can toggle between turning on or off the mode using either option.


### Procedure

Choose one of the following options:



- Click  and select **X Server compatible input**. This option enables the mode for all support sessions.



- Click  and select **Configuration**. In the Console Settings window, select the **X Server compatible input mode** check box, and click **Apply**. This option enables the mode for this support session only.

**Note:** You can turn off the mode by clearing your choice in either the **X Server compatible input** menu item or the **X Server compatible input mode** check box in the Console Settings window.

### Quick Input Text tool

The Remote Support Console has a Quick Input Text tool to let you type text on your local machine and send it to the target machine when the local control input function is enabled. This tool compensates for differences in the local and target keyboard mappings that make it difficult to type certain characters or to type long sequences of text where considerable latency occurs.

The quick text input window keeps a limited history of recently typed lines of text. You can also store common text strings as favorites in slots that are assigned to the keyboard digits 1 to 0. You can scroll through the history, or you can press **CTRL+digit** to retrieve a favorite text string. These strings are stored in the Console settings directory on your local hard drive, so both the history and the favorites are available between different Console sessions.

### Handling text sent to the target:

When you have local control input enabled, you can type characters and text in the quick text input window and then send the text to the target machine after you press **ENTER**.

### Before you begin

Ensure you have turned on local control input. For more information, see “Turning on or off local input control” on page 38.

### Procedure



1. Click  and select **Quick Text Input**. The quick text input window opens at the current position of your local mouse pointer.



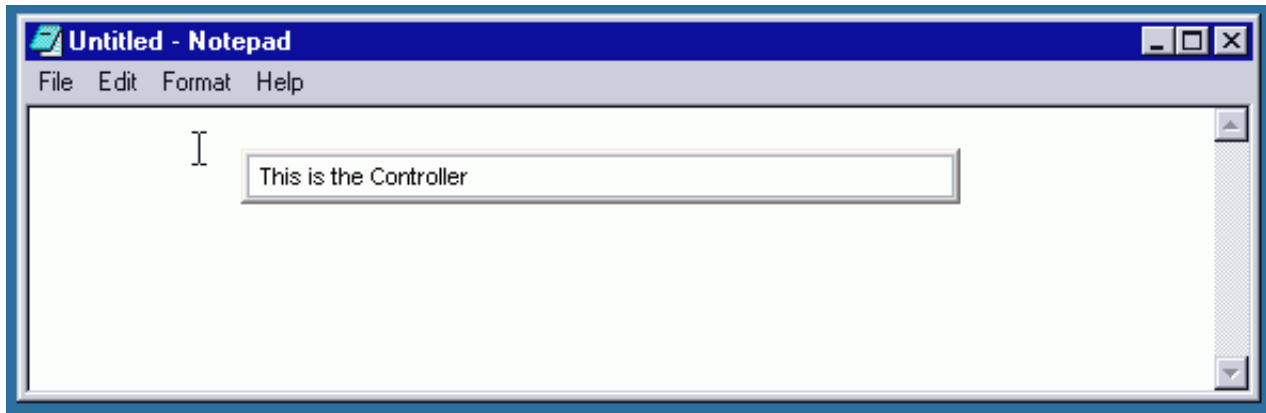



Figure 26. Quick Text Input window

2. Choose one of the following options:

Option	Description
New text string	Type the text string in the quick text input window.
Text string in history	Press <b>Up arrow</b> or <b>Down arrow</b> to scroll up or down the history in the quick text input window to select the text string.
Favorite text string	Press <b>CTRL+digit</b> associated with the slot that is assigned to the favorite text string. For example, if you assigned the favorite text string to slot five, press <b>CTRL+5</b> .

3. If you want to set the new text string as a favorite text string, press **CTRL+SHIFT+digit**. For example, to store the text string as favorite and assign it to slot 7, press **CTRL+SHIFT+7**.
4. After you have typed or selected the text string, press **ENTER**. The text string is sent to the target machine.

5. After you have finished sending text strings to the target machine, click  and select **Clear Instructions** .

### Drawing tools

The Remote Support Console has a set of drawing tools to let you draw and highlight areas on the target desktop to draw the customer's attention to those areas. The drawing tool is a solid color brush that you control with the target mouse. The highlighting tool is a transparent pen that you can drag over text on the target desktop. You can clear any drawings from the target desktop using the **Clear Instructions** function.

#### Drawing on the target desktop:


You can draw lines or highlight areas on the target desktop using the drawing and highlighting tools.

## About this task

**Tip:** If the session mode is Guidance, you can also use the Guidance tool to guide the customer in performing actions on the target system. For more information, see “Guiding the customer to perform actions” on page 42.

## Procedure

1. Click  and select either **Drawing Tool** or **Highlighting Tool**.

**Note:** If the session mode is Guidance, you can also click  and select either **Drawing Tool** or **Highlighting Tool**.

2. If you chose the **Drawing Tool**, use your mouse to draw on the target desktop. Figure 27 is an example of the drawing tool.

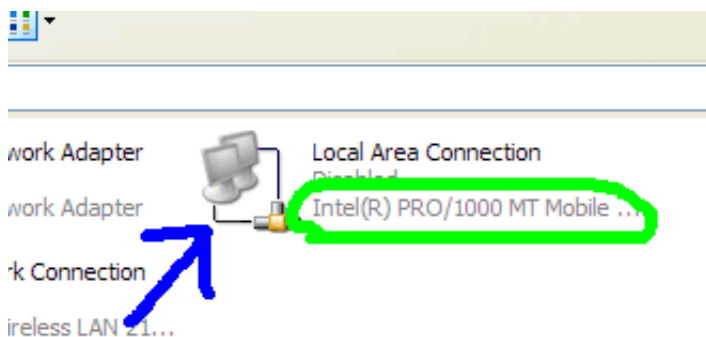


Figure 27. Example of the Paint drawing tool

3. If you chose the **Highlighting Tool**, use your mouse to highlight an area on the target desktop. Figure 28 is an example of the highlighting tool.

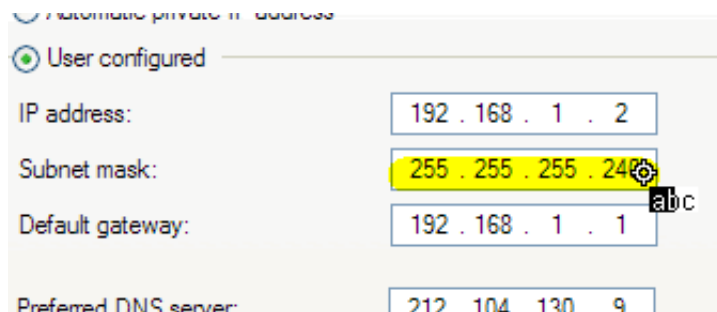



Figure 28. Example of the Highlighting tool

4. To remove the drawings from the target desktop, click  and select **Clear Instructions**.

## What to do next

After you have finished, you can turn off the tools. Click  and select either **Drawing Tool** or **Highlighting Tool**.


### Capture screen tool

The Remote Support Console has a capture screen tool to capture an image of the target screen. Assist On-site saves the screen capture in JPEG format. You can set the path and file name for the screen capture.

#### Capturing the screen of the target desktop:

You can capture the target screen using the Screen Capture tool.

#### Procedure

1. Click  and select **Screen Capture**. Assist On-site captures the screen and opens the Capture Screen to File window.
2. Browse and select the path and name for the JPEG file. Click **Save**.

### Optimal Video Settings tool


The Remote Support Console has an Optimal Video Settings tool to turn on or off the optimal video acceleration settings of the target operating system. The optimal settings improve the performance of the connection and reduce the resources that the Remote Support Utility uses.

When the connection starts, the Remote Support Utility attempts to set the optimal video settings. This automatic attempt might not succeed, so you can use the Optimal Video Settings tool in the Console to manually turn them on or off. After the session finishes, the Remote Support Utility resets the video settings to their status before the support session started.

#### Turning on or off the optimal video settings:

You can turn on or off the optimal video acceleration settings of the target operating system using the Optimal Video Settings tool.

#### Procedure

Click  and select one of the following menu items:


- **Optimal Video Settings** to turn on the optimal video settings
- **Restore Video settings** to turn off the optimal settings and return to the original settings

### Launching host sessions

You can reopen a host session on the host machine over an existing Assist On-site connection using the **Launch host session** function.

## Procedure



Click  and select **Launch host session**. A Web browser window opens on your machine and the customer's machine, running the same Rational Host Access Transformation Services emulator session.

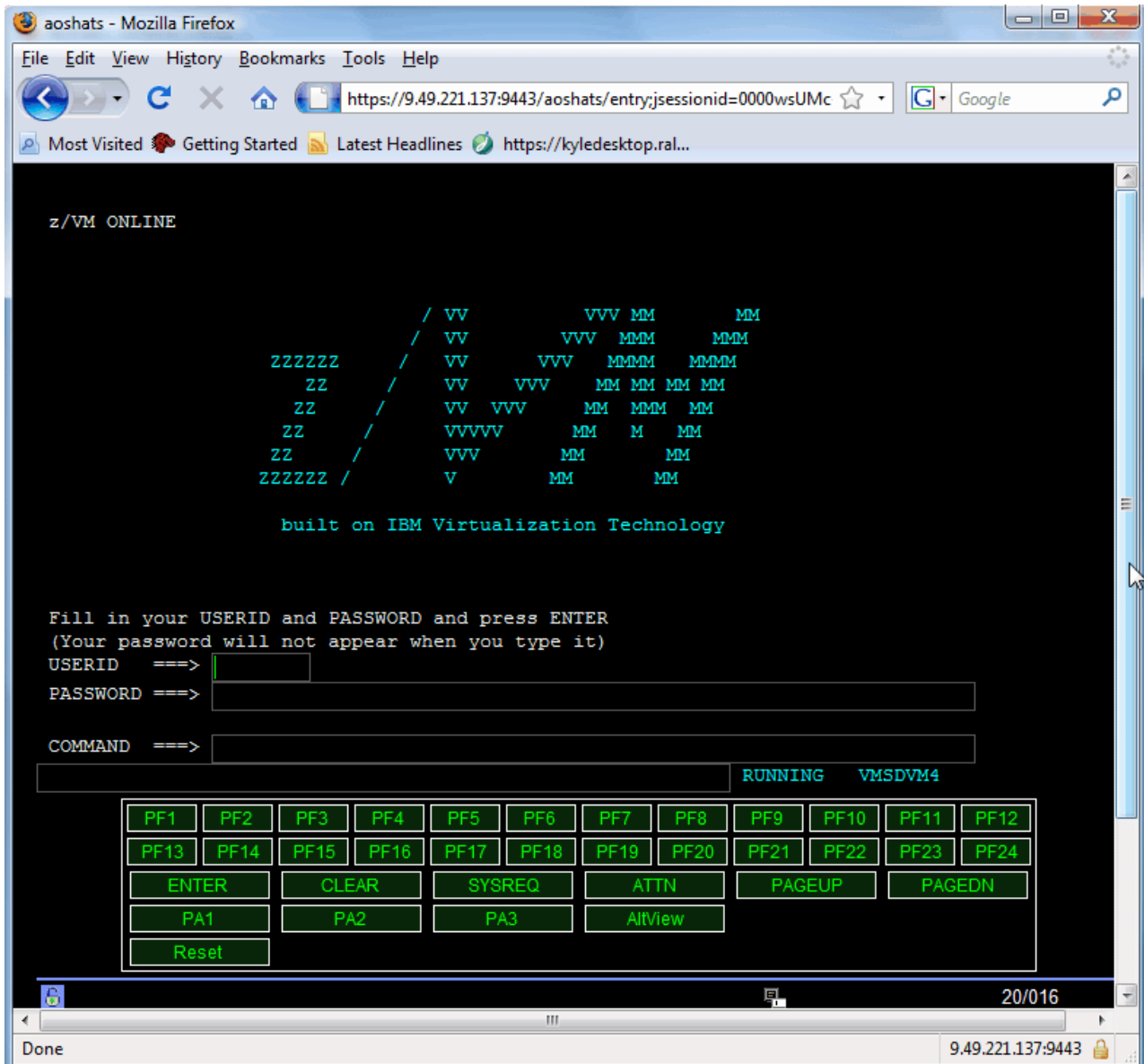


Figure 29. The emulator session running in the Web browser window

## What to do next

Either you or the customer can run commands on the host machine using the emulator session in the Web browser window. You can also stop the host session at any time.

## Configuring and starting port forwarding sessions in the Console

After the customer explicitly configures permission for port forwarding in the Remote Support Utility or the Assist On-site Support Service, you can begin a port forwarding connection from your local machine to an authorized port on the remote host machine. You can configure port forwarding and set which local ports to forward to which remote host machines and ports on the Port Forwarding window.

### Before you begin

During a Assist On-site tunneling session, the set of forwarded ports is saved to a CSV file on the support engineer's machine. The `portfwd.csv` file is stored in the operating system's home directory, within the `.AOSConsole` directory. For example, on a Windows system, the file is stored: .

```
C:\Documents and Settings\<support_engineer>\.AOSConsole
```

**Note:** The Assist On-site administrator must assign the port forwarding permissions to you before you can start port forwarding sessions.

### Procedure

1. When the session mode changes to port forwarding, the Port Forwarding window opens in the Console.

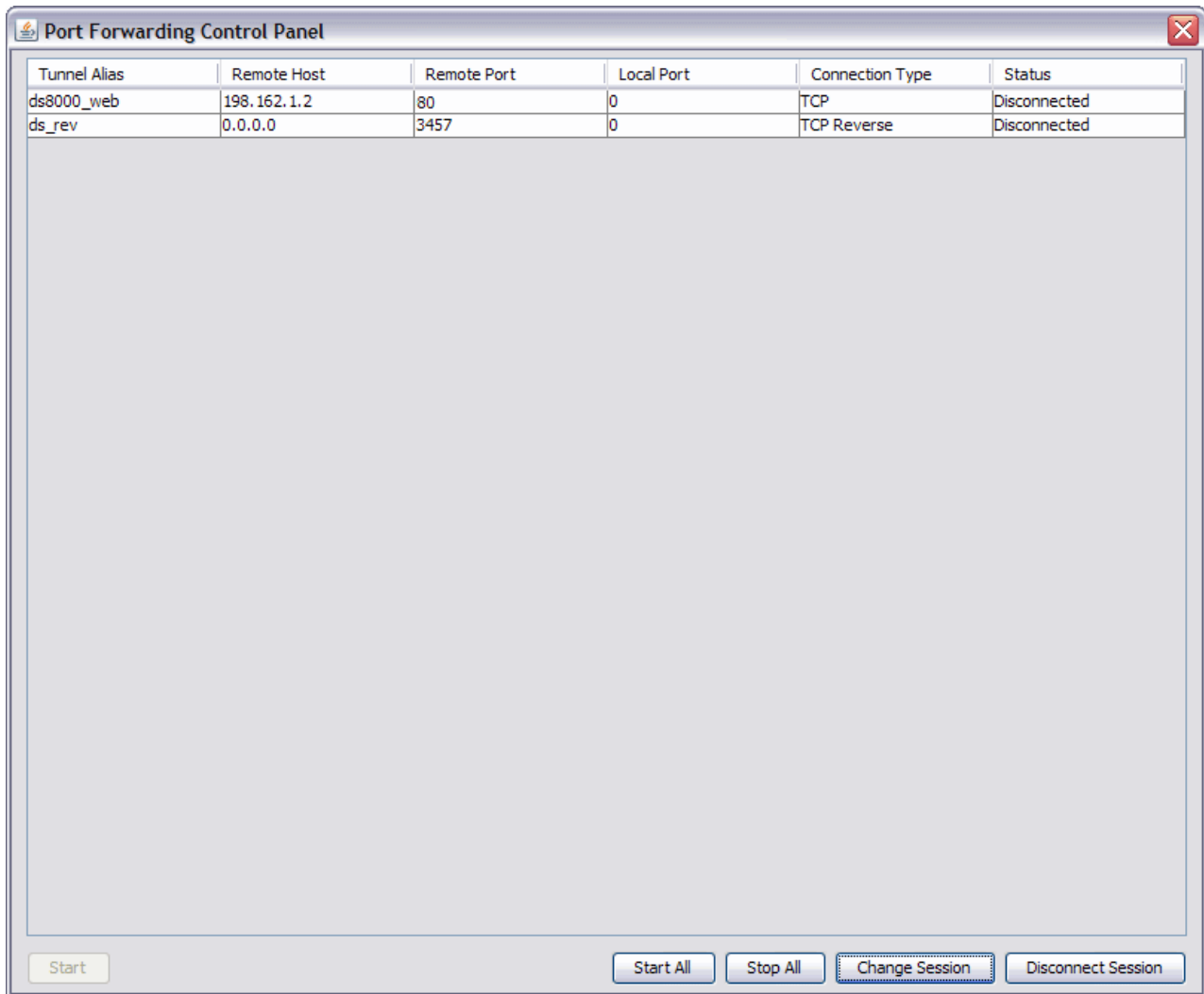


Figure 30. Port Forwarding window

2. You can connect to multiple machines during a port forwarding session, click **Start All**.

**Note:** Connections to multiple devices from the same port on the support engineer's machine are also supported.

3. To configure port forwarding to connect to a single machine, complete the following substeps:
  - a. Select a host machine in the grid and click **Start**.

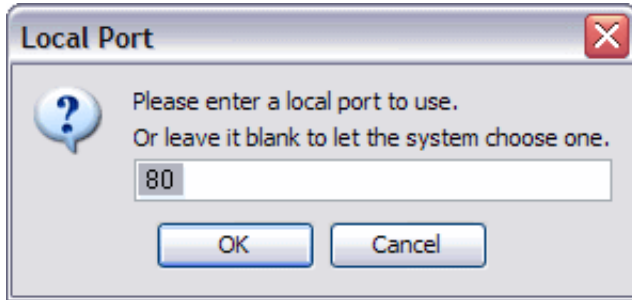


Figure 31. Local Port window

- b. In the field, enter the number of the port to forward to the remote host machine; click **OK**.

**Important:** Leave the field blank to have Assist On-site set the local port.

4. To configure reverse port forwarding to connect to a single machine, complete the following substeps:
  - a. Select a host machine in the grid and click **Start**.

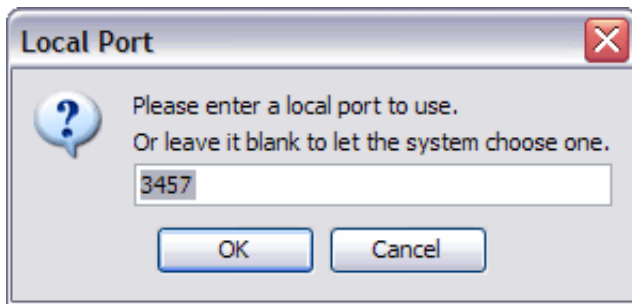


Figure 32. Local Port window for reverse port forwarding

- b. In the field, enter the number of the port for port redirection from the remote host machine to your machine; click **OK**.

Assist On-site starts the port forwarding session for the selected host machine and port.

### What to do next

You can stop the connection to a single remote host machine at any time by clicking **Disconnect Session** or to all remote host machines by clicking **Stop All**. You can also change to another type of session mode; click **Change Session**.

## Working in collaborative sessions

You can either start a collaboration for a support session or join one. Depending upon whether you created or joined the support session, your set of available functions differ.

### Starting collaborations for support sessions

You can start a collaboration between multiple participants that can join an existing support session to troubleshoot the customer's issue in the Collaboration Control Panel window.

## Before you begin

You must start a support session with the customer, and the customer must have accepted the connection and initiated the support session before you can start a collaborative session.

## Procedure



1. Click . The Collaboration Control window opens.

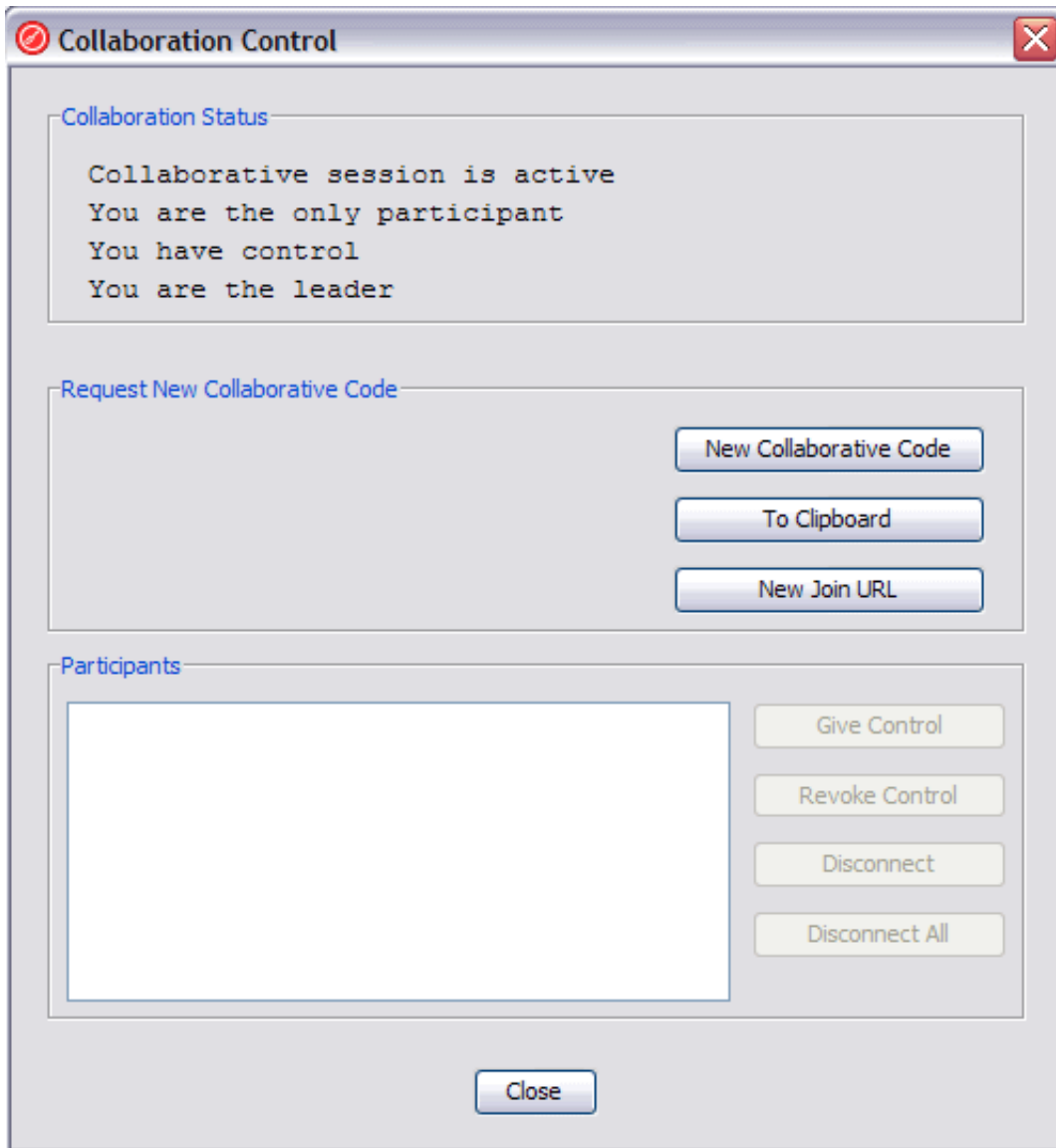


Figure 33. Collaboration Control window

2. Click **Get new code** to generate a collaborative session code that you must supply to the other participants to join the collaborative session.
3. Before you provide the collaborative session code to the other participants, ensure the customer grants permission to the start the collaborative session. If



the customer refuses permission, you get notification of the refusal and the Collaboration Control window displays the Stopped status.

4. Click **To Clipboard** to copy the collaborative session code to the clipboard. Send the collaborative session code to the participants. After a participant joins, the participant's name is added to the **Participants** list in the Collaboration Control window.

**Note:** After you start the collaborative session, you can close the Collaboration Control window without affecting the ongoing support session. You can open



the window again by clicking .

### What to do next

You can perform actions in the collaborative session. For more information, see “Collaboration actions” on page 60.

### Starting collaborations and generating secure URLs

You can start a collaboration between multiple participants that can join an existing support session to troubleshoot the customer's issue in the Collaboration Control Panel window.

### Before you begin

You must start a support session with the customer, and the customer must have accepted the connection and initiated the support session before you can start a collaborative session.

### Procedure



1. Click . The Collaboration Control window opens.

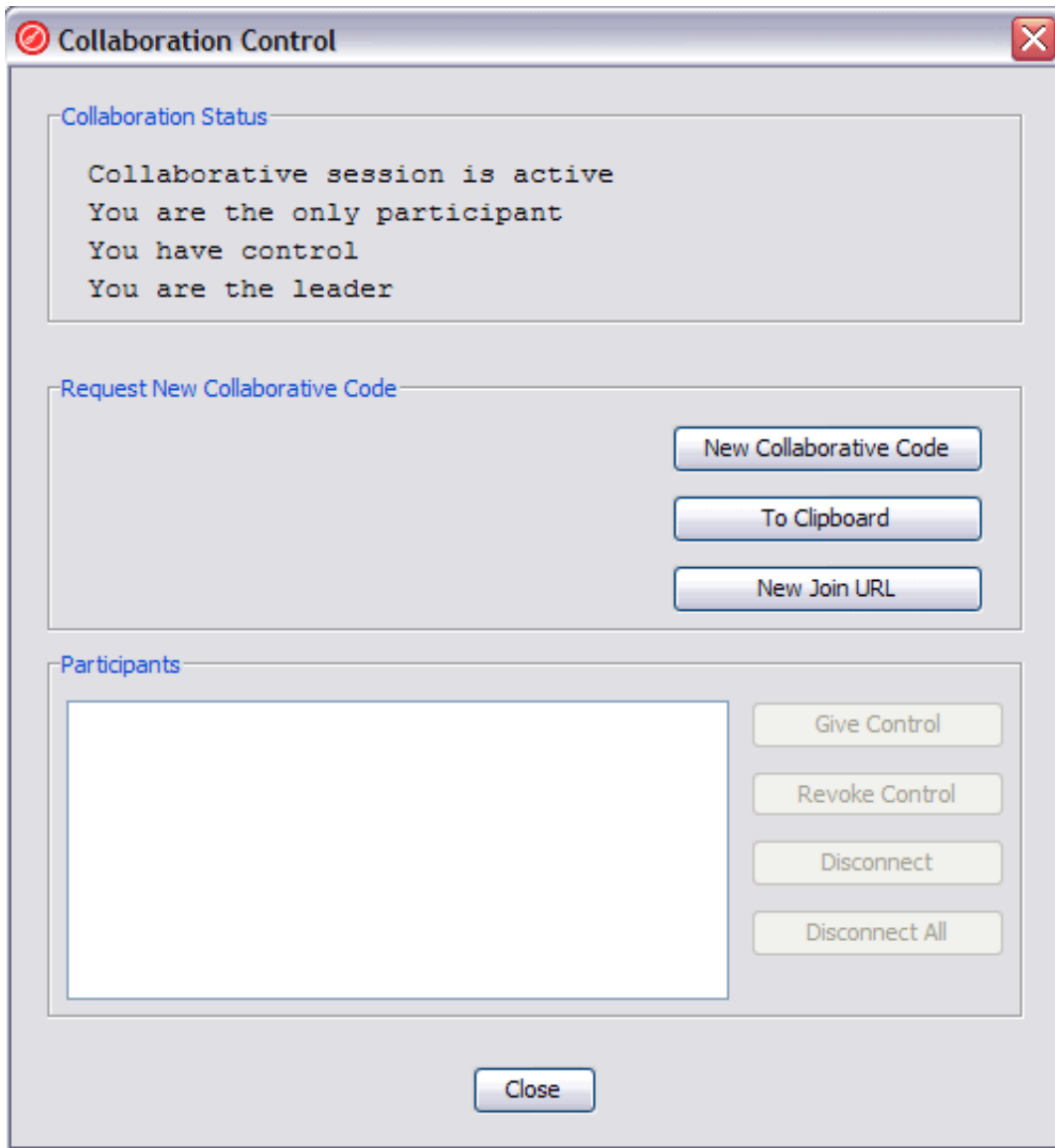



Figure 34. Collaboration Control window

2. Click **New Join URL** to generate a secure URL. The primary support engineer provides the secondary support engineer with the secure URL that launches the Remote Support Console from a Relay Server using a Java Web Start Launcher.
3. Click **To Clipboard** to copy the URL to your clipboard. After a participant joins, the participant's name is added to the **Participants** list in the Collaboration Control window.

**Note:** After you start the collaborative session, you can close the Collaboration Control window without affecting the ongoing support session. You can open

the window again by clicking  .

## What to do next

You can perform actions in the collaborative session. For more information, see “Collaboration actions” on page 60.

## Joining collaborative sessions

You can join and collaborate in an existing support session that the primary support engineer started in the Collaboration Control window. After you join an existing support session, the updates from the target desktop are displayed in the Console's window. You cannot have control of the target machine until the primary support engineer gives you control.

## Before you begin

Ensure that the primary support engineer has sent you the collaborative session code and that you have connected to a Relay Server. For more information, see “Connecting to a Relay Server” on page 29.

## Procedure

1. Choose one of the following options:

- Click 

- Click  . In the Tivoli Assist On-site window, click **Join Session**.

The Join a session window opens.

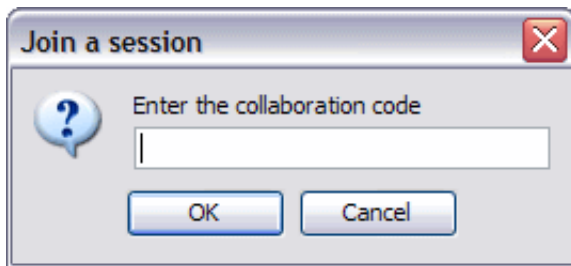



Figure 35. Join a session window

2. In the **Enter the collaboration code** field, type the collaborative session code that you obtained from the primary support engineer and click **OK**.

**Note:** After you join the collaborative session, you can close the Collaboration Control window without affecting the ongoing support session. You can open

the window again by clicking  .

## What to do next

You can perform actions in the collaborative session. For more information, see “Collaboration actions” on page 60.

## Joining collaborative sessions using secure URLs

The primary support engineer provides the secondary support engineer with the secure URL that launches the Remote Support Console from a Relay Server using a Java Web Start Launcher.

### Procedure

1. Open the secure URL.
2. Click **Launch**.
3. When prompted, select **open with Java Web Start Launcher**.
4. Click **OK**.

### What to do next

You can perform actions in the collaborative session. For more information, see “Collaboration actions.”

### Collaboration actions

Depending upon whether you started (primary support engineer) or joined (participating support engineer) the collaboration for a support session, you can perform different collaboration actions in the Collaboration Control window.

Table 9 outlines the collaboration actions available to the primary support engineer in the Collaboration Control window.

*Table 9. Primary support engineer's available collaboration actions*

Action	Description
Give control	Passes control of the target machine to the participating support engineer selected in the Participants list.
Retake control	Retakes control of the target machine from the participating support engineer selected in the Participants list.
Disconnect	Disconnects the participating support engineer selected in the Participants list from the collaborative session.
Disconnect all	Disconnects all participating support engineers in the Participants list from the collaborative session.

Table 10 outlines the collaboration actions available to the participating support engineer in the Collaboration Control window.

*Table 10. Participating support engineers available collaboration actions*

Action	Description
Give control	Passes control of the collaborative session to the selected support engineer.
Request control	Requests control of the collaborative session from the current support engineer with control.

## Turning on or off scaled view

During a support session, you can turn on or off the screen reduction of the target desktop using the **Enable/Disable scaled view** toggle icon in the toolbar. When you turn on this function, you can resize the Console window and the target

desktop resizes accordingly. This function uses slightly more processing power and is only recommended when target or local resolutions prohibit view of the full screen.



## About this task


**Note:** The default mode of the scaled view function is disabled by default upon opening the Console. You can switch it on or off at any time during the support session.

Subsequent support sessions remain in the mode last selected unless you open and close the Remote Support Console.

## Procedure

Depending upon the current status of the scaled view, click one of the following icons:

- To turn on scaled view, click  .
- To turn off scaled view, click  .



When you turn off this function, you can resize the Console window to the size of the target desktop by clicking  in the bottom right corner of the Console. When you right click the scroll bars during a support session, you can select from a set of functions to view sections of the screen that are not visible in the Console window.

## Turning on or off autoscroll

You can turn on or off the Console window automatically scrolling vertically and horizontally using the **Enable/Disable autoscroll** toggle icon in the toolbar. When the mouse pointer approaches either the top, bottom, left or right side of the Console window, it automatically scrolls if the target window is bigger than the area displayed.

## Procedure

Depending upon the current status of the autoscroll function, click one of the following icons:

- To turn on automatic scrolling, click  .
- To turn off automatic scrolling, click  .

## Turning on or off Truecolor

You can turn on or off 24-bit Truecolor view of the target desktop using the **Enable/Disable True Color** toggle icon in the toolbar. The default view is 8-bit, with the Truecolor function disabled upon opening the Remote Support Console.

This function conserves bandwidth that reduces the data being passed across the connection while generally providing enough color quality.

### About this task

**Note:** Subsequent sessions remain in the mode last selected unless you close and open the Remote Support Console.

### Procedure

Depending upon the current status of the Truecolor function, click one of the following icons in the toolbar:



- To turn on 24-bit Truecolor, click  .

**Note:** There might be a short delay before the Console displays the target desktop in 24-bit color.



- To turn off 24-bit Truecolor and return to 8-bit, click  .

---

## Customizing the Remote Support Console

You might want to run a Java application or executable during a support session. You can extend **Console tools** menu and add this application as an Extensions menu item.

### Extending the Remote Support Console

You can add your Java application as an menu item extension to the **Console tools** menu. Before building your Java application, you must adhere to and use a directory structure for your Java class files that supports Remote Support Console extensions. You must also add your menu item extension to a menu mapping XML file. After you build your Java application, you put the Jar file in the Remote Support Console extensions directory.

### Before you begin

Ensure you understand how to create a menu mapping XML file. For more information, see “Menu mapping XML file” on page 63.

### Procedure

1. Create the Assist On-site directory at the root level of your Java code, with the name `ayudame`.
2. Create a menu item mapping XML file, `ayudame.xml`, at the root level, and add mapping nodes for each menu item extension to add.
3. Build your Java application.
4. Copy your Jar file to the extensions directory, `rsc_root/extensions`
5. Start the Remote Support Console. Click **Console tools Extensions > *Menu\_item\_extension\_name***.

## Menu mapping XML file

You can add your Java application as a menu item extension to the **Console Tools** menu using the menu mapping XML file.

### Purpose

For each menu item extension, add a mapping node to the menu mapping XML file associated with your Java application.

### ayudame-extension node

This node is the parent node for the XML file. It contains the child menu-mappings node.

### menu-mappings node

This node is the parent node for the menu item extensions. It contains the child mapping nodes.

### mapping node

This node represents menu item extension. It can contain the following elements:

- `<caption>`  
The menu item label.
- `<accessible-name>`  
The label to support accessibility.
- `<parameters>`  
Any parameters that need to be passed to the Java application.

### Clock menu item extensions

This example creates two menu item extensions, one extension for the digital clock Java application and another one for the analog clock.

```
<ayudame-extension>
  <menu-mapping>
    <mapping>
      <caption>Digital Clock </caption>
      <accessible-name>Digital clock</accessible-name>
      <parameters>digital</parameters>
    </mapping>
    <mapping>
      <caption>Analog Clock </caption>
      <accessible-name>Analog clock</accessible-name>
      <parameters>analog</parameters>
    </mapping>
  </menu-mapping>
</ayudame-extension>
```

## Customizing the branding of the Remote Support Console

You can run the Assist On-site Configuration Wizard after your first download the Remote Support Console installation package. The Assist On-site Configuration Wizard configures the Remote Support Console to use your team's default resource branding bundle.

## About this task

To customize the branding of the Remote Support Console:

### Procedure

1. Browse to the location of the installation package, and run one of the following files:
  - Executable file: `aos_console_setup_ver.exe`
  - Batch or script file from the binaries file: `run.bat` or `run.sh`

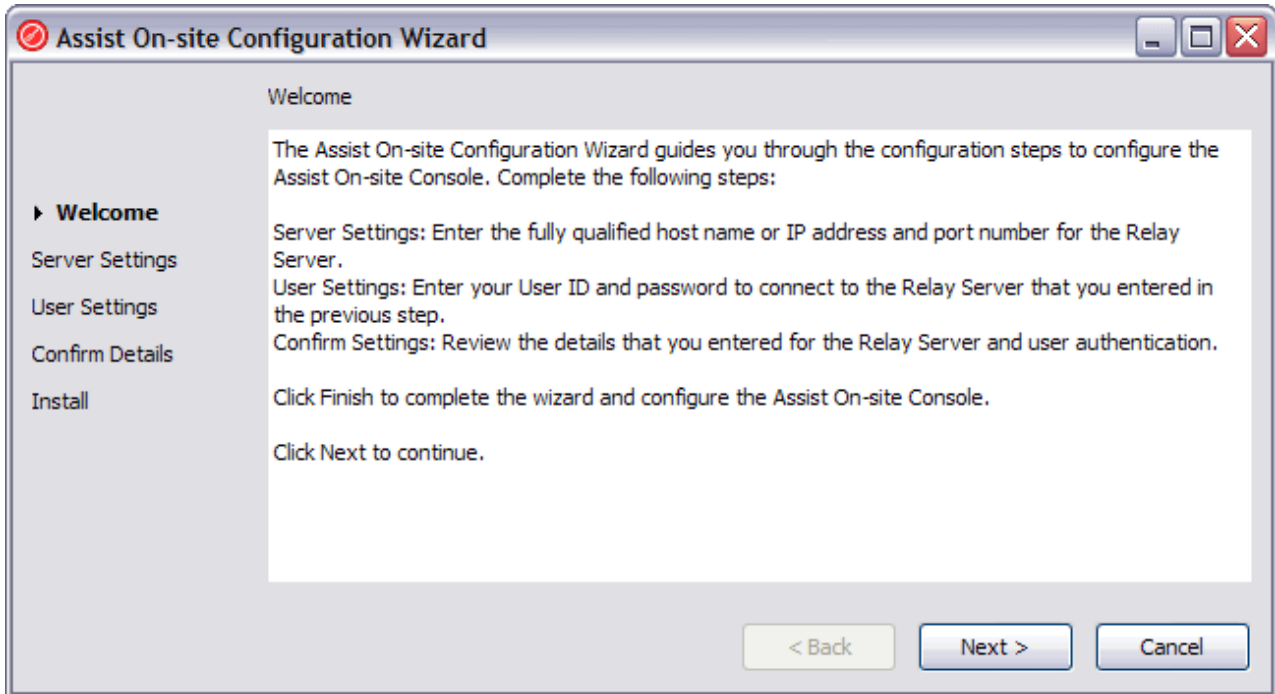


Figure 36. Welcome page of the Assist On-site Configuration Wizard

2. Click **Next**, and follow the onscreen instructions.

---

## Common directory locations

The Assist On-site use path name variables for common directories.

### Remote Support Console installation directory

`rsc_root` describes the location where Remote Support Console is installed. If not specified, the following default locations are used:

- On **Linux systems**: `/opt/ibm/Assist On-site/Console`
- On **Windows systems**: `C:\Program Files\IBM\Assist On-site\Console`



---

## Chapter 3. Remote Support Utility

The Remote Support Utility is one of the main components of Assist On-site. It is a lightweight Java application that communicates with the Remote Support Console. The Remote Support Utility has many functions which, whilst allowing the support engineer to take control, provides you, the customer, with various privacy functions.

After you or the support engineer stops the support session, the Remote Support Utility deletes itself from your machine.

---

### Installing the Remote Support Utility

You can download and automatically install the Remote Support Utility through the Assist On-site Web site or from a URL that you obtained from your support engineer if an internal IBM customer. It is a small Utility (`ibmaos.exe`).

The Utility includes the following files:

- `ibmaos.bat`

This batch file calls the main Utility. It deletes the main Utility from your machine and itself after the Utility deletes the auxiliary files.

- `forthook.dll`

This library places hooks on the mouse and keyboard. These hooks ensure that the Remote Support Utility is aware of the mouse position coordinates and shape, has the ability to inject or reject events in the operating system's event queue, and detect when you press **Pause** to stop the support session. The main Utility deletes this file.

- `tgrab.sys`

This Windows system file stores system settings and variables to support full screen, text mode windows. The main Utility deletes this file.

- `egathdrv.sys`

This driver is copied to the `system32` directory if the customer is an administrator and the support engineer requests system information. It is loaded to gather system information such as the serial number of the target machine. It is automatically unloaded and deleted from the machine after this operation finishes.

### Remote Support Utility Prerequisites

Assist On-site requires that you can connect to the Americas Relay Server and another server located in your geographical region. Your firewall and proxy server must allow traffic to and from the Relay Server.

Assist On-site provides a connectivity test executable that checks whether you can connect to the Relay Server in each geographical region. For more information about running the test, see "Running the Assist On-site connectivity test" on page 66.

Your firewall might deny the Assist On-site connection. If your firewall logs show that it has blocked Assist On-site traffic, configure your firewall according to the associated firewall documentation to allow traffic to and from the Relay Server in

the Americas on the relevant ports and any other Relay Server in your region. For more information about the IP addresses and port numbers for each Relay Server, see Chapter 5, “Relay Server,” on page 115.

The summary of requirements for the Remote Support Utility is as follows:

- 28.8Kbps or greater Internet connection (56K recommended)
- One of the following supported platforms:
  - Pentium-class computer running Windows starting with Windows 2000 Service Pack 4 and above, including all variants of Windows XP, Windows Vista, and Windows 7
  - Red Hat Enterprise and Desktop Linux 4 for Intel 32-bit and 64-bit
  - Red Hat Enterprise Linux 4.0 for z/Series 31-bit
  - Red Hat Enterprise Linux 4.0 for z/Series 64-bit
  - Red Hat Enterprise and Desktop Linux 5 and above for Intel 32-bit and 64-bit
  - Red Hat Enterprise Linux 5.0 and above for z/Series 31-bit
  - Red Hat Enterprise Linux 5.0 and above for z/Series 64-bit
  - SUSE Linux Enterprise Server 9 for Intel
  - SUSE Linux Enterprise Server 9 for zSeries® 31-bit
  - SUSE Linux Enterprise Server 9 for zSeries 64-bit
  - SUSE Linux Enterprise Server 10 for Intel
  - SUSE Linux Enterprise Server 10 for zSeries 64-bit
  - SUSE Linux Enterprise Server 11 for Intel
  - SUSE Linux Enterprise Server 11 for zSeries 64-bit
- Internet Explorer 4.0 or later, Netscape Navigator 4.0 or later, or Mozilla Firefox 1.0 or later
- Access to ports 80, 443, and 8200
- Recommended: Ability to make direct outgoing TCP connections, or availability of a SOCKS server or an HTTP proxy

## Running the Assist On-site connectivity test

You can run the Assist On-site connectivity test to check whether you can successfully connect to the Relay Server in each geographical region. The connectivity test uses an executable that you download to your local machine and run.

### Procedure

1. Open the following URL:  
<http://www-01.ibm.com/support/assistsite/>
2. Click **Assist On-site Connectivity Test**.
3. When prompted, click **Open** to temporarily save the executable to your local machine.
4. When prompted, click **Run**.
5. If prompted by your firewall, allow the executable to connect to the Internet.

## Results

The connectivity test runs and displays the results in your Web browser. You must be able to connect to at least one Relay Server in the Americas and to realize improved throughput, you should be able to connect to a Relay Server in your geographical region.

**Important:** If you cannot connect to any Relay Server in the Americas, you might not be able to use Assist On-site. Check that your firewall is configured to allow traffic to and from Relay Server in the Americas.

# Assist On-site Tester results

Mozilla Firefox Settings : Available

Internet Explorer Settings : Not Detected

Mozilla Firefox Settings : Selected

Proxy Type: DIRECT

List is ordered by connection response speed (fastest to slowest)

Region	Server	Port	SSL	Proxy	Result	Comments
Relay1	72.15.223.60	80	No	Yes	Failed to connect	Failed to connect
AP	203.141.90.53	80	No	Yes	Failed to connect	Failed to connect
AMERICA	72.15.208.234	80	No	Yes	Failed to connect	Failed to connect
EMEA	81.144.208.229	80	No	Yes	Failed to connect	Failed to connect
Backup	72.15.223.61	8200	No	Yes	Success. It is a relay	Success. It is a relay
Relay1	72.15.223.60	8200	No	Yes	Success. It is a relay	Success. It is a relay
EMEA	81.144.208.229	8200	No	Yes	Success. It is a relay	Success. It is a relay
AMERICA	72.15.208.234	8200	No	Yes	Success. It is a relay	Success. It is a relay
EMEA	81.144.208.229	443	Yes	Yes	Success. It is a relay	Success. It is a relay
Relay1	72.15.223.60	443	Yes	Yes	Success. It is a relay	Success. It is a relay
AP	203.141.90.53	8200	No	Yes	Success. It is a relay	Success. It is a relay
AP	203.141.90.53	443	Yes	Yes	Success. It is a relay	Success. It is a relay
Backup	72.15.223.61	80	No	Yes	Failed to connect	Failed to connect

If you have any issues connecting to any of the relays, please refer to [this](#) Knowledge Document for detailed help.

For improved performance you must be able to connect to a relay in your geographic region:

- AMERICA** : North, Central and South America
- EMEA** : Europe, Middle East and Africa.
- AP (Asia-Pacific)** : East Asia, Southeast Asia, Australasia
- Backup** : Backup Server
- Relay1** : Backup Relay One

## LOG DETAILS

```

profile {4196}

[2011.02.02-13:51:25.468 (GMT)]-->PROXY set to DIRECT {4196}

[2011.02.02-13:51:25.468 (GMT)]-->IMPORTING INTERNET EXPLORER PROXY SETTINGS {4196}

[2011.02.02-13:51:25.468 (GMT)]-->PROXY set to AUTO-DISCOVERY {4196}

[2011.02.02-13:51:25.468 (GMT)]-->AUTO-DISCOVERING PROXY... {4196}

[2011.02.02-13:51:28.062 (GMT)]-->Proxy Auto Discovery FAILED {4196}

[2011.02.02-13:51:28.093 (GMT)]-->PROXY AUTODISCOVERY FAILED. Ignoring Explorer proxy settings {4196}

[2011.02.02-13:51:28.093 (GMT)]-->Relay [0] = aos.us.ihost.com : 8200 (DIRECT) {4196}

[2011.02.02-13:51:28.109 (GMT)]-->Relay [1] = aos.us.ihost.com : 80 (DIRECT) {4196}

[2011.02.02-13:51:28.109 (GMT)]-->Relay [2] = aos.uk.ihost.com : 8200 (DIRECT) {4196}

[2011.02.02-13:51:28.109 (GMT)]-->Relay [3] = aos.uk.ihost.com : 443 (DIRECT) {4196}

[2011.02.02-13:51:28.109 (GMT)]-->Relay [4] = aos.uk.ihost.com : 80 (DIRECT) {4196}

```

Figure 37. Connectivity test results

## Example

In Figure 37 on page 68, the customer can connect to the Relay Server on port 8200 in the Americas, Relay Server on ports 8200 and 443 in EMEA, and the Relay Server on ports 8200 and 443 in AP. Thus the customer can download the Remote Support Utility and choose to connect to any Relay Server , though the customer should choose to connect to the server that is located in the same geographic region.

## What to do next

If the connectivity test is successful, you can download and install the Remote Support Utility.

## Installing the Utility for external IBM customers

You must complete the online request form on the Assist On-site Support Web site and agree to the terms and conditions for using Remote Support Utility before you can download and install the Utility, `ibmaos.exe`.

## Before you begin

Ensure that you have successfully connected to the Relay Server. The support engineer must also give you a connection code, otherwise you cannot install the Utility after you download it.

**Note:** If your support engineer started Assist On-site during a session of a third-party support tool such as Technical Support Chat, the URL that is provided might be different to the URL provided in the following procedure. If it is, accept the license agreement and proceed to step 9 on page 70.

## About this task

You are prompted to install the Utility that is less than 780 KB.

## Procedure

1. Open the following URL:  
`http://www-01.ibm.com/support/assistsite/`
2. Click **IBM Assist On-site request form**. The page with online request form opens.

United States [ change ]

Search

Home Solutions Services Products Support & downloads My IBM Welcome [ IBM Sign in ] [ Register ]

## Support & downloads

- Downloads and drivers
- Troubleshooting
- Product publications
- Open a service request
- Warranties and maintenance
- Feedback

# IBM Assist On-site

**How it works:**

1. Once you are on the phone with a member of our support team, you will be directed back to this page after your support representative provides you with a unique connection code. You will then enter the code in the field below and click the **I Agree** button to initiate the screen-sharing session.
2. You are prompted to download a small 500kb plug-in.
3. With your permission, your support representative can view your screen and share control of your mouse and keyboard.
4. You are in full control of your computer at all times. You always have overriding control of your mouse and keyboard, and you can end the screen-sharing session at any time.

**Personalized support**  
Visit [My support](#) for fast access to your favorite features.

**Related resources**

- Global Technical Support
- Software support
- Systems Technology Group

**Translate my page**  
Select Language

By clicking on "I agree" below, you are agreeing to allow IBM and its subcontractors to remotely access, manipulate and/or control your systems in order to assist you in isolating potential errors in your IBM software. You are responsible for backing up your systems prior to granting IBM access and for taking all other measures necessary to adequately protect your systems and all data, materials and other information contained therein. IBM shall not be liable for any loss of, or damage to, any data, materials and/or other information contained on or accessed through your systems. You are responsible for securing any necessary consents or approvals that may be required to permit IBM and its subcontractors to remotely access, manipulate and/or control your systems and to have access to the data, materials or other information contained on your systems. You agree to defend and indemnify IBM from and against any third party claims arising from your failure to secure all necessary consents and/or approvals. These services are being provided to you in accordance with and subject to the terms and conditions of your services agreements; (e.g., Passport Advantage, Software Maintenance, SoftwareXcel agreement) as well as any other support agreement you have with IBM applicable to the IBM software. These terms may be superceded or supplemented by the terms of separate agreements which you may have with IBM addressing support and/or the remote access of your systems.

Please complete the form below with your name and click the **I Agree** button to proceed.

Name:

IBM Customer Number:

PMR number, branch code, country code:  ,  ,

Geography: Americas

About IBM Privacy Contact Terms of use IBM Feeds Jobs

Figure 38. Online request form

3. In the **Name** field, type your name.
4. In the **IBM Customer Number** field, type your customer number. If you do not know it, type all zeros.
5. **PMR number, branch code, country code** fields, type the PMR number and associated codes for your issue.
6. In the **Connection code** field, type the connection code that you obtained from the support engineer if required.
7. From the **Geography** list, select your geographical region.

**Important:** Ensure that you select a geographical region that contains a Relay Server to which you successfully connected when you ran the connectivity test.

8. Click **I Agree**.
9. When prompted, click **Open** or **Run** to download the Utility.

**Note:** You might need to temporarily allow popup windows in your Web browser depending upon your Web browser security settings.

- The Utility detects any proxy server settings and if necessary, it opens a proxy authentication window to enter the proxy user name and password. Enter some or all of the following details, and click **OK**:

Options	Description
User name (basic proxy authentication)	Enter the proxy user name and password for your proxy server.
Domain\User (NTLM proxy authentication)	Enter the domain controller and user name for your proxy server.
Password	Enter the password for the proxy user.

- If prompted by your firewall, allow the Utility to connect to the Internet. The Session code window opens.

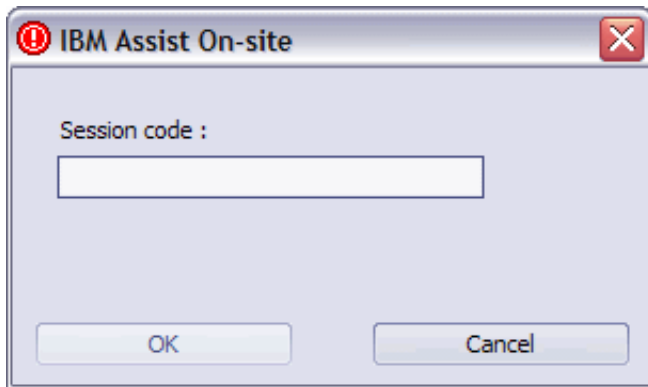


Figure 39. Session code window

- In the **Session code** field, type the connection code that you obtained from the support engineer. Click **OK**.

### What to do next

After you install the Remote Support Utility, you must consent to running the support session. For more information, see “Consenting to support sessions” on page 73.

## Installing the Utility for internal IBM customers

As an internal IBM customer, you can bypass the agreement of terms, and download and run the install the Utility using the URL that you obtained from the support engineer. This URL is secure and contains the unique connection code for your support session.

### Before you begin

Ensure that you have successfully connected to the Relay Server.

### About this task

You are prompted to install the Utility that is less than 780 KB.

## Procedure

1. Open the URL that you obtained from the support engineer.
2. You are prompted to download and run the Utility. Click **Run** or **Open**.

**Note:** You might need to temporarily allow popup windows in your Web browser depending upon your Web browser security settings. Otherwise, you need to click the download link on the page.

3. The Utility detects any proxy server settings and if necessary, it opens a proxy authentication window to enter the proxy user name and password. Enter some or all of the following details, and click **OK**:

Option	Description
User name (basic proxy authentication)	Enter the proxy user name and password for your proxy server.
Domain\User (NTLM proxy authentication)	Enter the domain controller and user name for your proxy server.
Password	Enter the password for the proxy user.

4. If prompted by your firewall, allow the Utility to connect to the Internet.

## What to do next

After you install the Remote Support Utility, you must consent to running the support session. For more information, see “Consenting to support sessions” on page 73.

## Manually configuring the connection for the proxy server

Assist On-site detects the customer's proxy server through the customer's Web browser settings including the Proxy Autoconfiguration file (PAC), or registry keys. It evaluates the proxy settings through a JavaScript parser if available; otherwise, Assist On-site supports manual proxy configuration using a configuration file, `proxy_ibm.txt`.

### Before you begin

Ensure that you obtained the proxy server settings from your administrator before you create the configuration file.

### Procedure

1. Create a text file using a text editor.
2. In the text file, enter your proxy server details using the following syntax:  
`Proxy=myproxy.mycompany.com:myproxy_port`  
  
`myproxy.mycompany.com` is the fully qualified host name or IP address for your proxy server and `myproxy_port` is the port number on the proxy server for outbound connections.
3. Save the text file with the name `proxy_ibm.txt` in your home directory or at the root level of your C:\ drive.

## What to do next

If you cannot establish a connection to a Relay Server, ensure that you configure your proxy server to allow encrypted non-SSL outbound traffic to the Americas



Relay Server and to a relevant Relay Server in your geographic region. For more information about the IP addresses and port numbers, see Chapter 5, “Relay Server,” on page 115.

If you still cannot establish a connection, Assist On-site creates a diagnostic report in the `connrpt.html` file that you can submit to Assist On-site Support.

## Using the Remote Support Utility

A customer can accept connections from a support engineer's machine, obtain support, and interact with the support engineer using various functions of the Remote Support Utility.

When a session is active, Remote Support Utility opens a small window for the duration of the support session. You can minimize it to the taskbar.

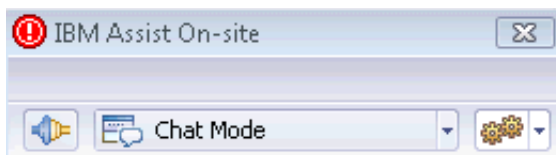




Figure 40. Remote Support Utility interface

### Remote Support Utility functions

Table 11 describes the main functions of the Remote Support Utility that you can access from the toolbar.

Table 11. Remote Support Utility functions

Function	Description
Disconnect from a session 	Disconnect from a session. For more information, see “Stopping support sessions” on page 75.
Session mode drop-down list	Contains the session mode options to switch to during a session. For more information, see “Switching between session modes” on page 75.
Actions menu 	Contains menu items to perform common actions on your host machine. For more information, see “Remote Support Utility actions” on page 75.

### Consenting to support sessions

When an support engineer starts a support session and attempts to connect to your target machine, the Remote Support Utility displays a message on your machine. You must accept the connection and choose the session mode before it times out. At no point is the session activated until you accept the connection. If the request times out after the default or extended timeout period, the Remote Support Utility automatically refuses the connection.

## About this task

**Note:** You can stop the support session at any time. For more information, see “Stopping support sessions” on page 75.

## Procedure

1. The support engineer starts a support session and attempts to connect to your target machine. The Assist On-site window opens.

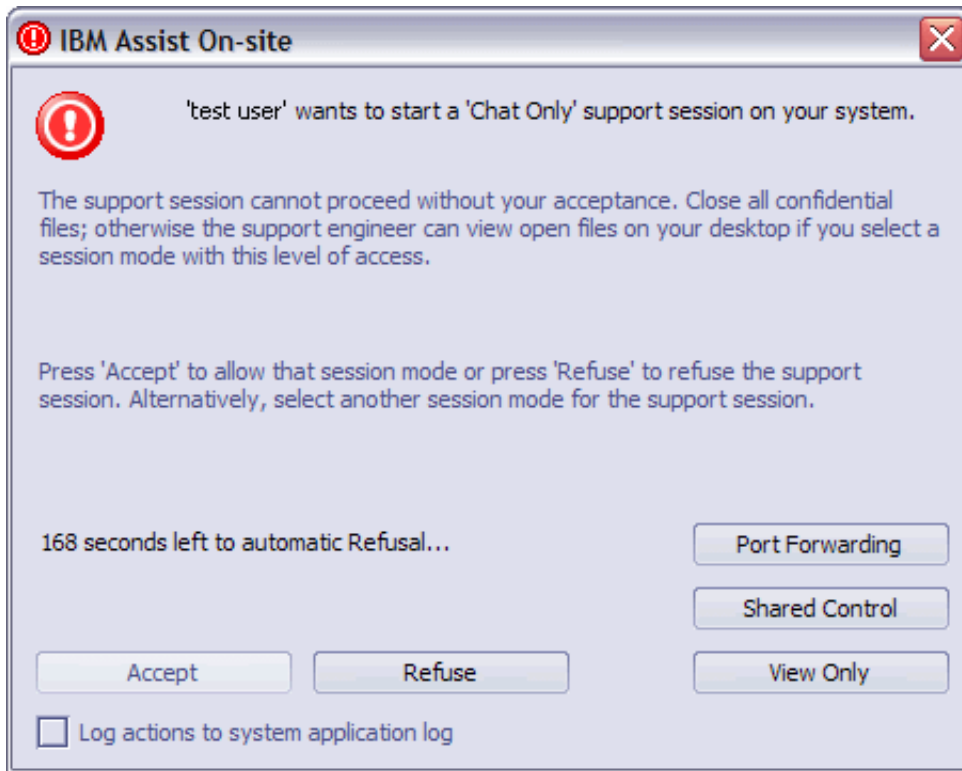


Figure 41. The Assist On-site window

2. Click **Log session actions into System Application log** check box if the support engineer requests it.
3. Click one of the following buttons:

Table 12. Session modes and options

Option	Description
Chat	Accept the connection and start the support session in Chat Only mode.
Guidance	Accept the connection and start the support session in Guidance mode.
Shared View	Accept the connection and start the support session in View Only mode.
Shared Control	Accept the connection and start the session in Shared Control mode.

Table 12. Session modes and options (continued)

Option	Description
Port Forwarding	Accept the connection and start the session as a port forwarding connection. <b>Note:</b> Ensure that you have configured port forwarding. For more information, see “Configuring port forwarding in the Utility” on page 78.
Refuse	Refuse the connection and deny access to your target machine. The Remote Support Console displays a refused access message to the support engineer.


**Important:** The choice of session modes is dependent on the default permissions of the team to which the support engineer belongs, the permissions of the support engineer, and the type of session.

## Stopping support sessions

You can stop a support session by different methods. There is no confirmation and the support session stops immediately. After the support session stops, a deletion utility within the Remote Support Utility deletes the main utility and flags itself for removal the next time you reboot your machine.

### Procedure

Choose one of the following options:

- Press **PAUSE/BREAK**.
- Click  .
- Click **End Session** in the Session in Progress window.

## Switching between session modes

You might want to change or the support engineer might request that you change session mode during a support session. You can select the new session mode from the Session Mode drop-down list. The current session mode is selected by default.

### Procedure

From the **Session Mode** list, select the new session mode. A message is displayed on the Remote Support Console informing the support engineer that you changed the session mode.

## Remote Support Utility actions

The Remote Support Utility provides a set of functions for a support session. These functions include displaying information about your system and who is connected to it, starting a chat or host session, opening your file transfer directory, and exiting the session.

You can access these functions from  .

## Obtaining Remote Support Utility version information

You can obtain information about the current version of the Remote Support Utility using the **About** function.


### Procedure

Click  and select **About**. An information window opens that contains the version information.

## Finding out who is connected to your machine

You can find out details about the support engineer and the support engineer's machine using the **Who is connected** function. The function displays the user name, IP, and MAC addresses for the support engineer.

### Procedure

Click  and select **Who is connected**. An information window opens with the support engineer's details.

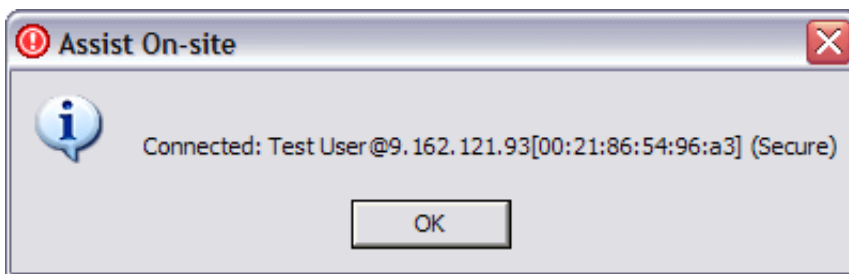


Figure 42. Information window with the support engineer's details

## Getting your system's information

During a support session, you can retrieve information about your system using the **View System Information** that uses the IBM System Information Gatherer. This tool gathers information such as the your system's details, network devices and status, and a list of running processes and saves it to a text file in the file transfer directory of the Remote Support Utility.

### Procedure

Click  and select **View System Information**.


## What to do next

The system engineer might request to copy this file to the system engineer's machine.

## Opening the file transfer directory

You can open the file transfer directory that using the **Transfer folder** function. The Remote Support Utility uses the most appropriate file manager for the operating system on which it is running.

## Procedure

Click  and select **Transfer folder**. A file manager window opens showing the file transfer directory. The default directory is named *IBM\_FT*.

## Chatting with the support engineer

During a support session, you can open and use a chat window to chat with a support engineer using the **Chat** function. You can also change the session mode in the Utility Chat window.

## About this task

**Note:** You do not need to be chatting to the support engineer to change the session mode. For more information about changing the session mode, see “Switching between session modes” on page 75.

## Procedure

1. Click  and select **Chat**. The Utility Chat window opens.

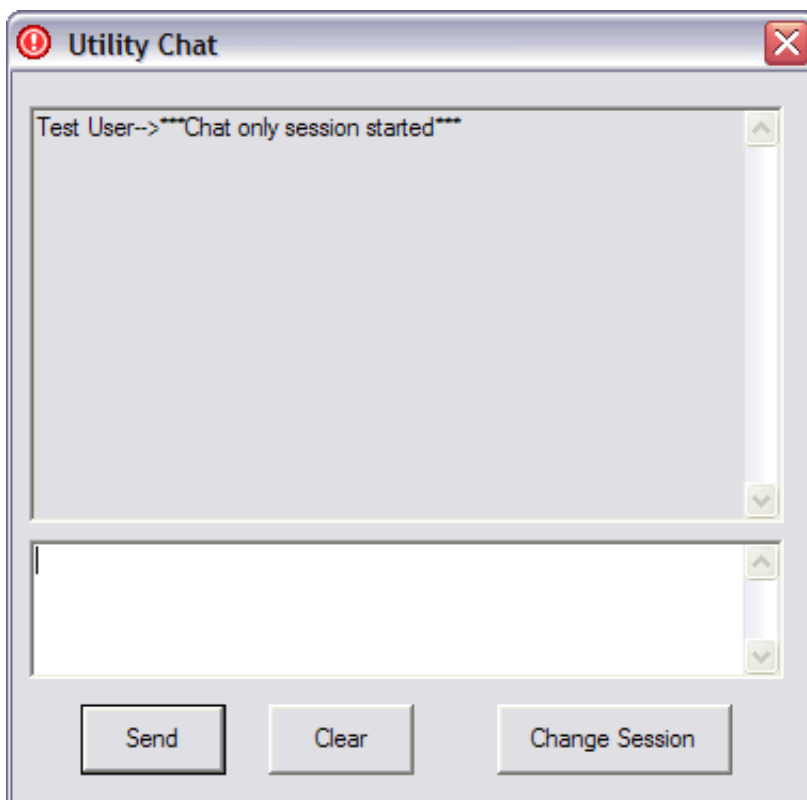
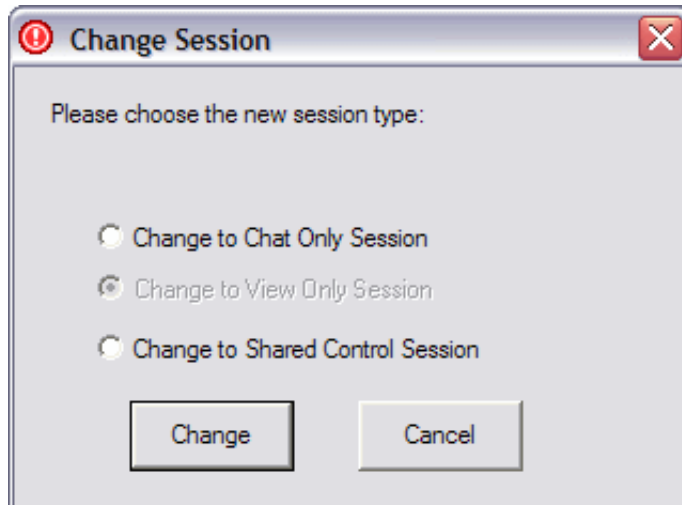


Figure 43. Utility Chat window

2. In the text area, type your message, and click **Send**. The support engineer's responses are displayed in the Utility Chat window.
3. If the support engineer requests that you change the session mode, do the following steps:
  - a. Click **Change Session**. The Change Session window opens.



**Important:** The choice of session modes is dependent on the default permissions of the team to which the support engineer belongs, the permissions of the support engineer, and the type of session.

- b. Select the radio button associated with the session mode to which you want to change.
- c. Click **Change**. A message is displayed in the Remote Support Console informing the support engineer of the session mode change.

### **Configuring port forwarding in the Utility**

You can configure port forwarding and reverse port forwarding by using the **Configure Port Forwarding** action in the Remote Support Utility. You can also set the time out value in hours for the port forwarding session. If you set the value to 0, no timeout applies and the port forwarding session continues until you or the support engineer stops it.

#### **Procedure**

1. Click **Configure Port Forwarding**. The Configure Port Forwarding window opens.

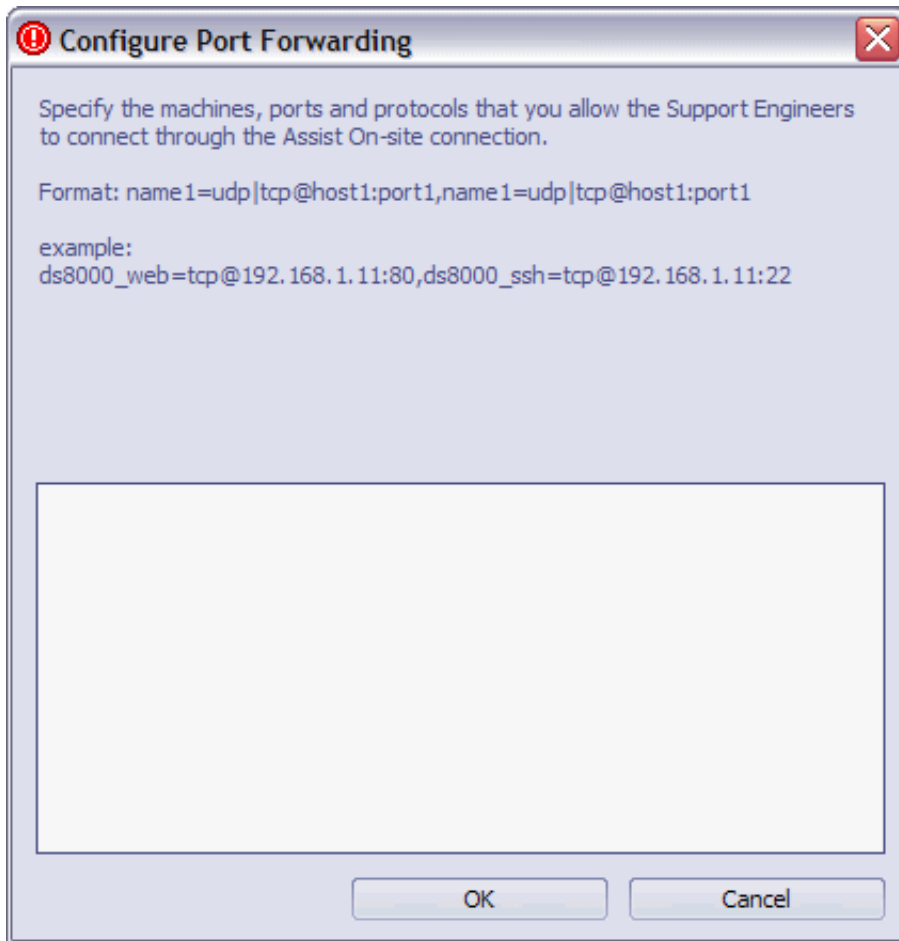


Figure 44. Configure Port Forwarding window

- In the text box, type a comma-separated list of host machine aliases, host machines, ports, and protocols that the support engineers can connect to during an Assist On-site session. The syntax for each allowed connection in the list is as follows:

`<host_alias>=udp|tcp@<host_name>|<IP_addr>:<port_num>`

Table 13. Variables for the port forwarding syntax

Variable	Description
<code>&lt;host_alias&gt;=</code>	The alias name for the host machine, for example, ds8000_web or ds8000_ssh.
<code>udp tcp</code>	The protocol for the connection, whether UDP or TCP, for example, tcp.
<code>&lt;host_name&gt; &lt;IP_addr&gt;</code>	The fully qualified name of the host machine or its IP address, for example:198.162.1.2 <b>Note:</b> If you want to configure a reverse port forwarding option, use 0.0.0.0 as the IP address.
<code>&lt;port_num&gt;</code>	The listening port for the connection, for example, 3456 or 22.

For example:

`ds8000_web=tcp@198.162.1.2:80,ds_rev=tcp@0.0.0.0:3567`

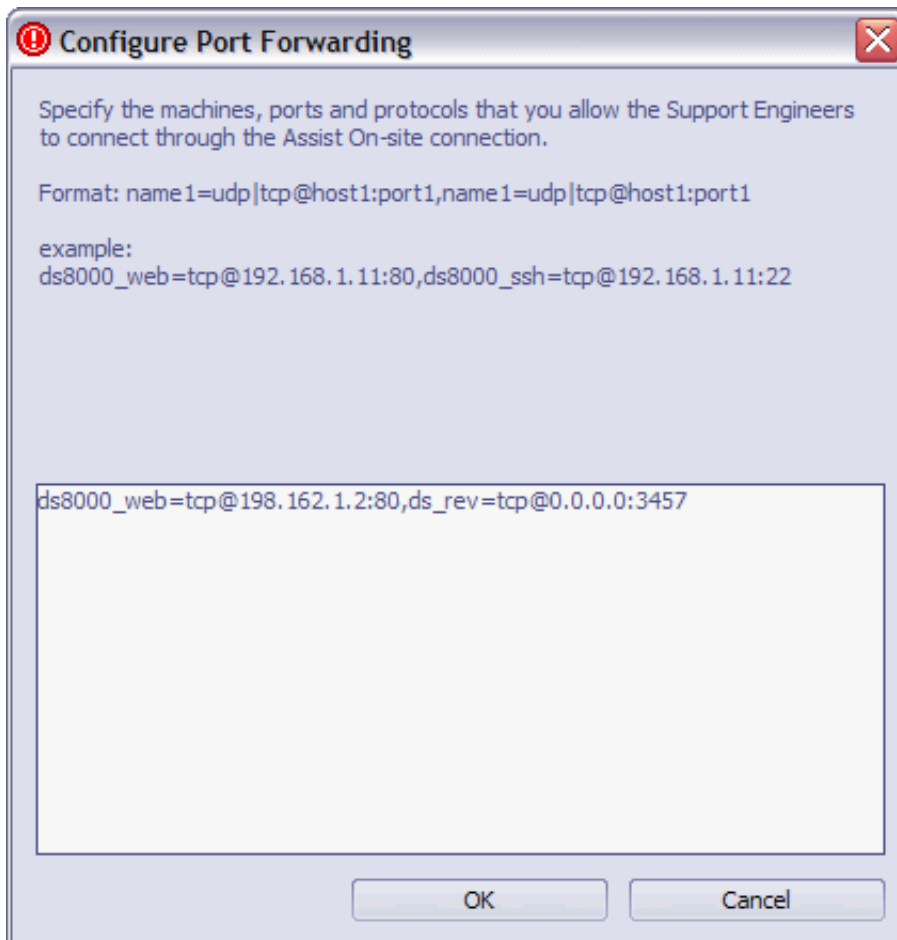


Figure 45. Configure Port Forwarding window with examples

3. Click **OK**.

### What to do next

After you explicitly configure permission for port forwarding in the Remote Support Utility, the support engineer can begin the attended, port forwarding session to the authorized ports. You must consent to the attended, port forwarding session.

### Starting host sessions


You can start a host session on the host machine over an existing Assist On-site connection using the **Start host session** function. After you have started it and logged onto the host machine, either you or the support engineer can run commands on the host machine using the emulator session in the Web browser window.

### Before you begin

Ensure that you have connected to a support session. For more information, see “Consenting to support sessions” on page 73.



## Procedure

1. Click  and select **Start host session**. The Start Host Session window opens.

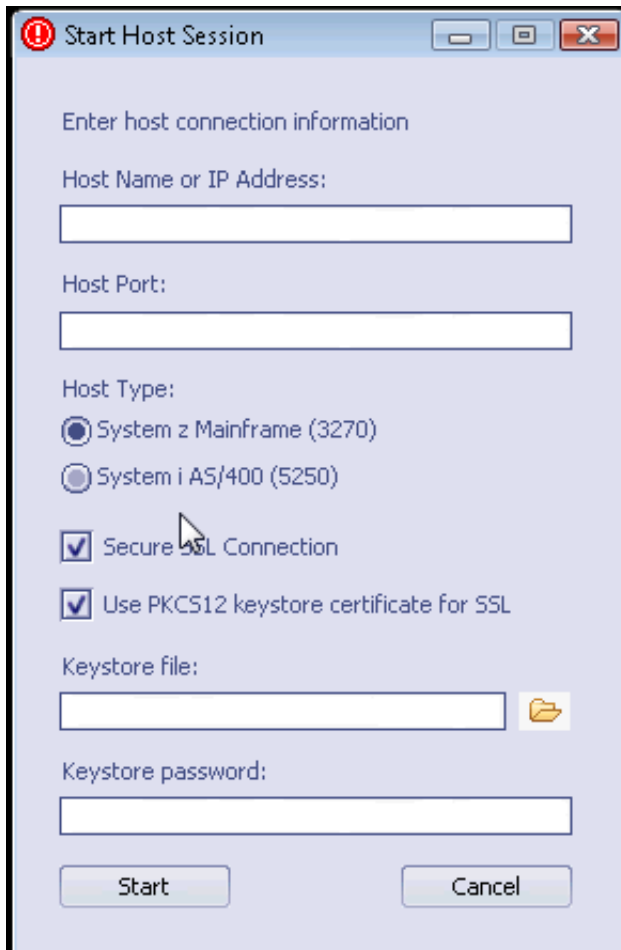


Figure 46. Start Host Session window

2. In the **Host Name or IP Address** field, type the fully qualified host name or IP address of the host machine.
3. In the **Host Port** field, type the port on the host machine for outgoing connections.
4. From the **Host Type** list, select the type of host machine.
5. Select the type of security for the connection and any associated details for the keystore certificate.
6. Click **Start**. A Web browser window opens on your machine and the support engineer's machine, running the same Rational Host Access Transformation Services emulator session.

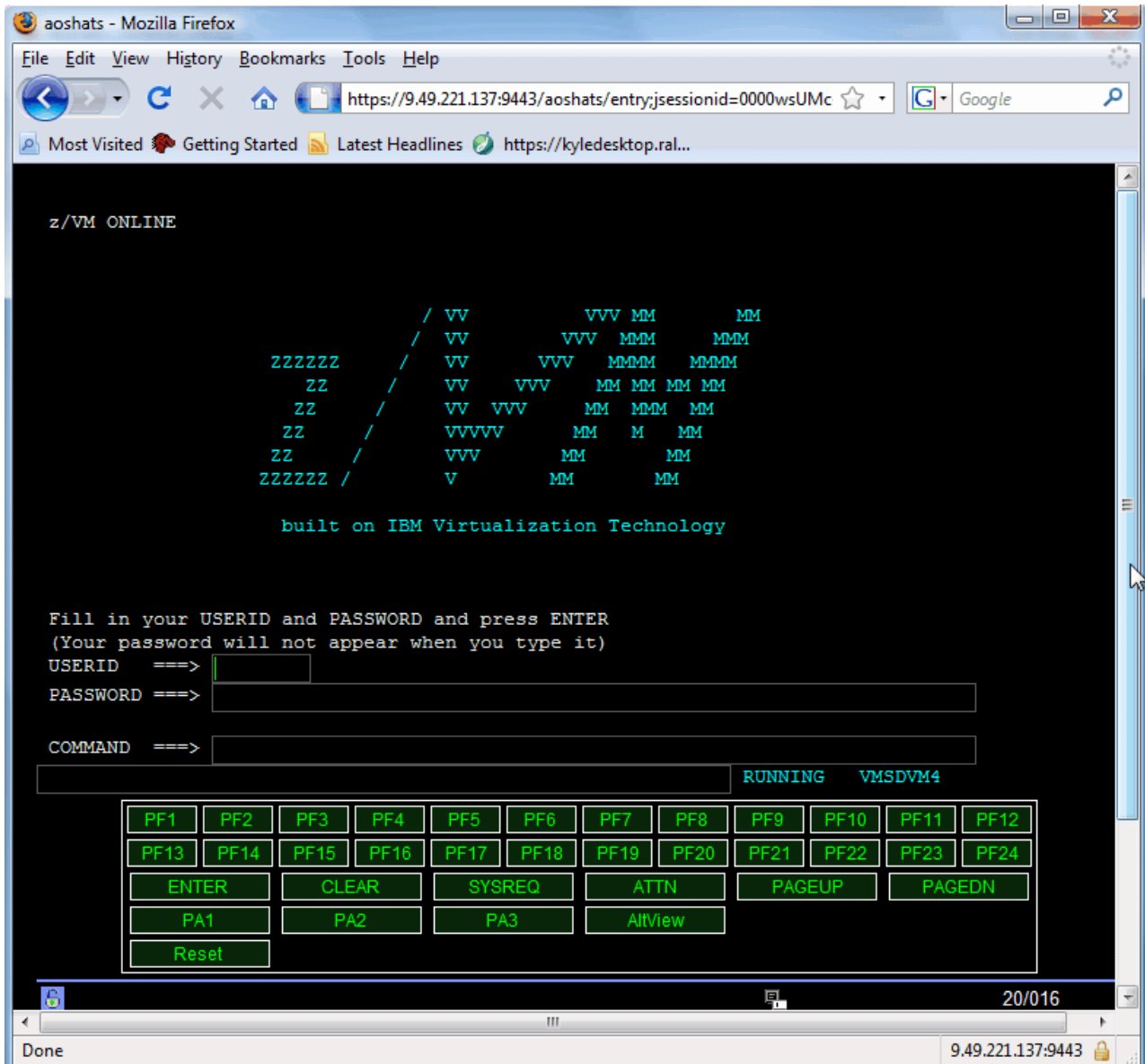


Figure 47. The emulator session running in the Web browser window

7. When prompted, enter your user name.
8. When prompted, accept the request from the support engineer to join the host session.
9. Log on to the host machine using your User ID and password.



### What to do next

Either you or the support engineer can run commands on the host machine using the emulator session in the Web browser window. You can also stop the host session at any time.

### Stopping host sessions

You can stop a host session at any time.

## Procedure

1. In the Web browser emulator session window, log off the host system.
2. Choose one of the following options:
  - To stop the host session only, close the Web browser emulator session window or click  and select **Exit**.
  - To stop the host and support sessions simultaneously, click  .



---

## Chapter 4. Administration Portal

The Administration Portal is a main component of IBM Tivoli Assist On-site. It is a single, secure point of access to information, applications, teams, and users that can be administered and managed to support Assist On-site.

---

### Logging on to the Administration Portal

You can log on using your Assist On-site user ID or using your IBM intranet ID if your team uses an Assist On-site BlueGroup.

#### Procedure

1. Open the following URL:

`https://aos.us.ihost.com/AssistOnSiteAdmin`

The Administration Portal logon page opens.

2. Choose one of the following options:

Option	Description
Use your Assist On-site ID and password	Enter your details, and click <b>Logon</b> .
Use your IBM intranet ID and password <b>Note:</b> Use this option only if your team uses an Assist On-site BlueGroup. Ensure that you have already connected to the IBM network.	<ol style="list-style-type: none"><li>1. Click <b>Use IBM Intranet Authentication</b>.</li><li>2. Enter your details, and click <b>Submit</b>.</li></ol>

---

### Assist On-site users, teams, and BlueGroups

Assist On-site has adopted IBM Intranet Password eXternal to use IBM BlueGroups to control membership of Assist On-site teams that contain IBM team members. These members can then log on to Assist On-site using their IBM intranet IDs and passwords, without Assist On-site compromising the IDs or passwords.

The Assist On-site administrator must first create an Assist On-site BlueGroup before creating the associated Assist On-site team in the Administration Portal. Its name must have the `aos:` prefix and be the same as the Assist On-site team, replacing / (forward-slash) with : (colon).

*Table 14. Team names*

Assist On-site team	Assist On-site BlueGroup
IBM/L3/EMEA	aos:IBM:L3:EMEA

**Important:** The team member must be connected to the IBM network, either onsite or offsite using an authorized VPN client. If not, Assist On-site authentication using the IBM intranet ID fails.

The Assist On-site administrator manages Assist On-site team permissions in the Administration Portal.

Any Assist On-site team in the Administration Portal database before Assist On-site 3.3 automatically has the associated Assist On-site BlueGroup created.

For new IBM users, the Assist On-site administrator must first add the users to the following Assist On-site BlueGroups:

- **AOS\_Users**  
This membership manages primary access to Assist On-site. This group can use the Remote Support Console and join collaborative sessions.
- **Assist On-site BlueGroup for associated Assist On-site team**  
This group can use the Remote Support Console and create support sessions.

**Note:** Use the IBM BlueGroups intranet site to manage BlueGroups.

The Assist On-site administrator does not need to manually create an Assist On-site user for an IBM member or add that user to the team. When the new user first connects to the Relay Server in the Remote Support Console using the IBM intranet ID, Assist On-site automatically adds the user to the Assist On-site team, based on the user's membership of the associated Assist On-site BlueGroup. Assist On-site also automatically applies the default team permissions to the associated user.

---

## User functions

The Administration Portal has a set of functions to let users edit their user profiles, download Assist On-site applications, and view the history of their support sessions. Users can access these functions on the Administration Portal home page or the **User** menu.

### Editing your profile

You can change details in your Assist On-site profile, such as your screen name, authentication password, and security question and answer in case you forget your password, on the Edit User page.

#### Before you begin

Ensure that you have correctly logged on to the Administration Portal.

#### Procedure

1. Click **User options > Edit User Profile**. The Edit User page opens.

# Assist On-site user management

---

## Edit user

Name:	<input type="text" value="Jane Smith"/>
Screen name:	<input type="text" value="JaneSmith"/>
Email (userid):	<input type="text" value="jsmith@thecomp.com"/>
Password:	<input type="password"/>
Re-type the password:	<input type="password"/>
Security question:	<input type="text" value="your security question"/>
Security answer:	<input type="text" value="your security answer"/>
Team:	<input type="text" value="BLUE"/>
Session modes:	<input checked="" type="checkbox"/> Chat Only <input checked="" type="checkbox"/> View Only <input checked="" type="checkbox"/> Share Control <input checked="" type="checkbox"/> Record
Tunneling	<input type="checkbox"/> Allow port forwarding <input type="checkbox"/> Allow reverse port forwarding

## Edit favorite URLs

---

Figure 48. Edit User page

2. In the **Name** field, type your name.
3. In the **Screen name** field, type the name to appear in Assist On-site applications.
4. In the **Password** field, type your password that is associated with your Assist On-site user ID, which you use to connect to the Relay Server.
5. In the **Security question** field, type the security question that you are asked should you forget your password.
6. In the **Security answer** field, type the answer to the security question.

7. Click **Update**.

## Adding favorite URLs

You can add URLs on the Add User URLs page.

### Procedure

1. Click **User options > User Profile**. The Edit User page opens.
2. Click **Edit Favorite URLs**.
3. Click **New URL**.
4. In the **URL** field, type the URL.
5. In the **Description** field, type a description for the URL.
6. Click **Create**.

## Viewing session history

You can select the dates between which to view the history of the support sessions on the Session History options page. The session history report shows a summary of the support sessions resolved or unresolved, start and end times of each support session, whether any recordings were made, and any feedback provided by the customer.

### Procedure


1. Click **User options > View Session History**. The View Session History page opens.

---


### Session history options

Please select the boundary dates or leave them blank to see all sessions

Start Date (yyyy-mm-dd):

2009-08-17 

End Date (yyyy-mm-dd):

2009-08-17 

[View session history](#)

[Back](#)

---

Figure 49. View Session History page

2. Choose one of the following options:

Option	Description
<b>View history for all support sessions</b>	Clear the <b>Start Date</b> and <b>End Date</b> fields.



Option	Description
View history for support sessions within a set of dates	<p>In the <b>Start Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget to select the start date.</p> <p>In the <b>End Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget to select the end date.</p>

3. Click **View Session History**.

## Viewing available installers to download

You can download the latest version of the Remote Support Console, the Assist On-site Player, or a permanent installation of the Remote Support Utility on the Downloads page.

### Before you begin

Ensure that you have version 1.6 or later of a Java Runtime Environment installed on your machine.

### Procedure

1. Click **User options > Downloads**. The Downloads page opens.
2. To download an application, click the hyperlink for the application, and save the download to your local machine.

### What to do next

You can install the Assist On-site application. For more information, see the relevant installation topics for that application.

---

## Administrator functions

The Administration Portal has a set of functions for Assist On-site administrators to view reports on Assist On-site usage and auditing metrics, to view support session recordings, and to manage Assist On-site users. Administrators can access these functions on the Administration Portal home page or the **Admin** menu.

## Creating users

You can create a user account for a support engineer or another team member on the Add User page. When you add a user, you must provide an e-mail address as the user ID, a temporary password, and a temporary security question and answer should the user forget the password. You can also set the team to which the user belongs and the functions available to the user in the Remote Support Console and the Administration Portal.

### Before you begin

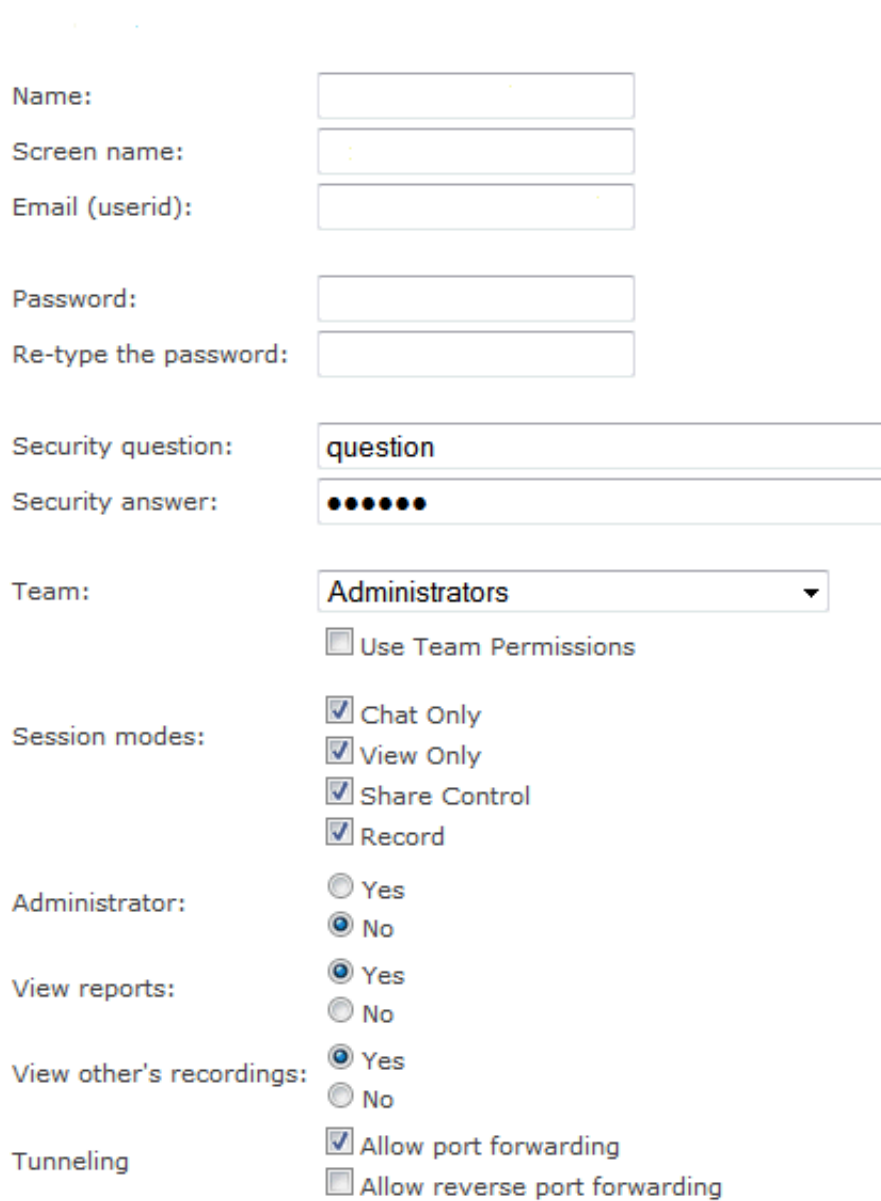
If you want to create an account for an IBM employee, you can use the IBM intranet ID. The Assist On-site administrator does not need to manually create an Assist On-site user for an IBM member or add that user to the team. For more information, see “Assist On-site users, teams, and BlueGroups” on page 85.

## Procedure

1. Click **Admin options > User Management**. The User and Team Administration page opens.
2. Click **Create User**. The Add User page opens.

## Assist On-site user management

---



Name:

Screen name:

Email (userid):

Password:

Re-type the password:

Security question:

Security answer:

Team:  ▼

Use Team Permissions

Session modes:

- Chat Only
- View Only
- Share Control
- Record

Administrator:  Yes  No

View reports:  Yes  No

View other's recordings:  Yes  No

Tunneling

- Allow port forwarding
- Allow reverse port forwarding

Figure 50. Add User page

3. In the **Name** field, type the name of the employee.
4. In the **Screen name** field, type the name to appear in Assist On-site applications.
5. In the **E-mail (User ID)** field, type the e-mail address for the user that becomes the user ID to use for Assist On-site authentication.

6. In the **Password** field, type the temporary password that is associated with the Assist On-site user ID, which the user logs on to the Relay Server.
7. In the **Security question** field, type a temporary security question that the user is asked should the user forget the password.
8. In the **Security answer** field, type the answer to the security question.
9. From the **Team** field, select the team to which the user belongs.
10. By default, the user's permissions are the same as the team's permissions. If you want to set different permissions, do the following steps:
  - a. Clear **Use Team Permissions**.
  - b. Select the associated check boxes for the session modes in which the user can run support sessions. For example, select **Chat Only** and **View Only** if you want the user to run sessions in Chat Only and View Only session modes.
  - c. Select **Record** to allow the user to record support sessions.
  - d. Select **Yes** or **No** for the following permissions:
    - Administrator
    - View reports
    - View other's recordings
  - e. Select any or all check boxes for **Allow port forwarding** and **Allow reverse port forwarding** to turn on tunneling.
11. Click **Add User**.

## What to do next

Provide the new user details to the employee. Ensure that the employee logs on to the Administration Portal and edits the user profile to change the password and security question and answer.

## Searching for users

You can quickly search for Assist On-site users on the User and Team Administration page. You can search using the user's name or user ID.

### Procedure

1. Click **Admin options > User Management**. The User and Team Administration page opens.

## User management

- [Create a new user](#)
- Search for users

- Manage users in selected teams

Automatically include subteams

## Team management

- [Create a new team](#)
- [Manage teams](#)

## Bulk import

- [Import users and teams](#)

Figure 51. User and Team Administration page

2. In the **Search for Users** field, type the screen name, name, or user ID for the user.
3. Click **Search**.

### Results

The Manage Users page opens and displays the results of the search.

## Managing users

You can manage users on the Manage Users page, for example, you can delete a user, edit a user's details, or save the details to a CSV file. You can search for the user using the Search function, or you can search for the user in a team or subteam.

### Procedure

1. Click **Admin options > User Management**. The User and Team Administration page opens.
2. Choose one of the following options:

Option	Description
Search for a user	See "Searching for users" on page 91
Search for a user within a team	<ol style="list-style-type: none"> <li>1. In the <b>Manage users in selected teams</b> list, select the team to which the user belongs. If you want to search within the subteam, select <b>Automatically include subteams</b>.</li> <li>2. Click <b>Continue</b>.</li> </ol>

The Manage Users page opens.

#### Manage users

Save as CSV-file

	Name	Email	Team	Admin status	View reports	View recordings	Actions carried out	
<input type="checkbox"/>	Jane Smith	jsmith@yourcomp.com	Administrators/AlphaTest/BetaTeam	Yes	Yes	Yes	By user	On user
<input type="checkbox"/>	Joe Nolan	jnolan@yourcomp.com	Administrators/AlphaTest/BetaTeam	No	No	No	By user	On user

Delete selected

Back

Figure 52. Manage Users page

3. Choose one of the following options:

Option	Description
Delete selected users	<ol style="list-style-type: none"> <li>1. In the <b>Manage Users</b> table, select the check box associated with each user that you want to delete.</li> <li>2. Click <b>Delete Selected</b>.</li> </ol>
Edit a user	In the <b>Manage Users</b> table, select the name associated with the user that you want to edit.
Save details to a CSV file	Click <b>Save as CSV File</b> .

## Creating teams

You can create teams for a set of support engineers, group of users, or department on the Add Team page. When you add a team, you must provide a name and description for the team, its parent team if a subteam, and its default permissions

for team members to perform functions in the Remote Support Console and the Administration Portal. You must also assign a maximum number of licenses to the team and its subteams.

## Before you begin

Assist On-site has adopted IBM Intranet Password eXternal to use IBM BlueGroups to control membership of Assist On-site teams that contain IBM team members. The Assist On-site administrator must first create an Assist On-site BlueGroup before creating the associated Assist On-site team in the Administration Portal. For more information, see “Assist On-site users, teams, and BlueGroups” on page 85.

## Procedure

1. Click **Admin options > User Management**. The User and Team Administration page opens.
2. Click **Create Team**. The Add Team page opens.

# Assist On-site user management

---

Name:

Description:

Parent team:

Default permissions:

- Chat Only
- View Only
- Share Control
- Record sessions
- View reports
- Admin users
- View other's recordings
- Allow port forwarding
- Allow reverse port forwarding

Resources bundle: System Default

Figure 53. Add Team page

3. In the **Name** field, type the name of the team.
4. In the **Description** field, type a description for the team.
5. From the **Parent Team** field, select the parent team if this team is a subteam.
6. Select any of the check boxes to set the default permissions for the team.
7. From the **Resources bundle** list, select the default branding resource bundle.

- Click **Add Team**. The Add User Licences page opens.

### Assign user licences

The team has been added successfully.

The parent group (Top level) has no usage restrictions.

If you would like to reserve a maximum number of licences for this team and any subteams please input the amount in the field below, otherwise please leave it empty to set no usage restrictions

Licences

**Reserve licences**

Figure 54. Add User Licences page

- In the **Licences** field, type the maximum number of licenses for the team and subteam. Alternatively, leave the field empty to have unlimited licenses.
- Click **Reserve Licenses**.

## Managing teams

You can manage teams, for example delete or edit teams, on the Manage Teams page.

### Procedure

- Click **Admin options > User Management**. The User and Team Administration page opens.
- Click **Manage Teams**. The Manage Teams page opens.

#### Manage teams

	Name	Number of users	(inc. subgroups)	Allocated licences	Available licences	(inc. subgroups)	Description
<input type="checkbox"/>	Administrators/AlphaTest	13	15	Unlimited	Unlimited	Unlimited	Alpha Test Users
<input type="checkbox"/>	Administrators/AlphaTest/BetaTeam	2	2	4	2	2	Beta Test Team

**Delete selected**

**Back**

Figure 55. Manage Teams page

- Choose one of the following options:

Option	Description
Delete selected teams	<ol style="list-style-type: none"> <li>In the <b>Manage Teams</b> table, select the check box associated with each team that you want to delete.</li> <li>Click <b>Delete Selected</b>.</li> </ol>

Option	Description
Edit a team	In the <b>Manage Teams</b> table, select the name associated with the team that you want to edit.

## Adding team URLs

You can add URLs on the Add Team URLs page. Support engineers that belong to this team can open these URLs in the Remote Support Console during support sessions. When you select **Propagate to subteams**, the URL is propagated from the parent team to its children. Support engineers, who are members of these subteams, can also open this URL.

### Procedure

1. Click **Admin options > User Management**. The User and Team Administration page opens.
2. Click **Manage Teams**. The Manage Teams page opens.
3. In the **Manage Teams** table, click the name of the team. The Edit Teams page opens.
4. Click **Edit Team URLs**. The View Team URLs page opens.

View team URLs

URL has been successfully created

URL	Description	Set by	On	Actions
http://www.greengrid.org	Green Grid		2009-09-24 12:24:47	Edit Delete Up Down

New URL

Back

Figure 56. View Team URLs page

5. Click **New URL**. The Create Team URL page opens.



# Assist On-site team management

---

## Create team URL

URL:

Description:

Propagate to subteams

Create

Back

---

Figure 57. Create Team URL page

6. In the **URL** field, type the URL.
7. In the **Description** field, type a description for the URL.
8. Select **Propagate to subteams** if you want to propagate the URL to teams that are children of this team.
9. Click **Create**.

### IBM Client Diagnostic Data Repository

Often IBM support engineers need to analyze customer data to diagnose customers' issues or they need to provide customers with utilities to debug the issues. Assist On-site provides support for the IBM Client Diagnostic Data Repository (CDDR) strategy in the exchange of data through the propagation of

team URLs and file transfer functions. Administrators can add team URLs to the relevant URLs associated with CDDR and propagate those URLs to subteams. During Assist On-site sessions, support engineers can open these URLs on the customers' machines and transfer diagnostic data.

The CDDR strategy uses the Enhanced Customer Data Repository (ECuRep) as the consolidated back end data repository for exchanging information with IBM Software Technical Support. The strategy also means that customers can exchange data by using the fastest method based on geographic location, for example, by connecting to the Testcase FTP server or by connecting to ECuRep directly. For more information, see the following address:

<http://www-01.ibm.com/software/support/exchangeinfo.html>

### **Propagation of parent team URLs to subteams**

When Assist On-site administrators add team URLs, they can choose to propagate the URLs to the teams of the parent team. Support engineers, who are members of these subteams, can also open these URLs. Administrators can turn on this function by selecting the **Propagate to subteams** check box on the Create team URL or Edit team URL pages in the Assist On-site Administration Portal. This function is useful when support teams want to use a standard URL to upload files from customers' machines to a support web site for further diagnostic checking.

Assist On-site provides support for the IBM Client Diagnostic Data Repository (CDDR) strategy in the exchange of data through the propagation of team URLs and file transfer functions. For example, during an Assist On-site session, an IBM Support engineer can open the URLs for ECuRep or Testcase FTP server that have been propagated from the parent team and upload the files by using the URL that is fastest for the geography of the customer.

## **Running bulk imports**

You can import users and teams in bulk on the Import Users and Teams page.

### **Before you begin**

Ensure that the CSV file is correctly structured. For more information, see "Bulk import CSV file" on page 99.

### **Procedure**

1. Click **Admin options > User Management**. The User and Team Administration page opens.

## User management

- [Create a new user](#)
- [Search for users](#)

- [Manage users in selected teams](#)

[Automatically include subteams](#)

## Team management

- [Create a new team](#)
- [Manage teams](#)

## Bulk import

- [Import users and teams](#)

Figure 58. User and Team Administration page

2. Click **Import Users and Teams**. The Import Users and Teams page opens.
3. In the **Choose CSV file to import** field, type the full path and file name. Alternatively, click **Browse** to select it.
4. Click **Import**.

### Bulk import CSV file

Before you can bulk import a set of users or a team into the Administration Portal database, you must ensure that the structure of the CSV file is correct.

## Structure for importing user details

Table 15 outlines each mandatory column and relevant valid values that you must have in the CSV file when importing users.

Table 15. User details structure

Column	Valid values	Description
U	U	Check box
Name		The name of the user.
Email		The e-mail address for the user that is used as the user ID.
Team		The name of the team to which the user belongs.
Screen Name		The screen name for the user.
Admin Status	y or n	Flag whether the user is an administrator.
Can Chat	y or n	Flag whether the user can run sessions in Chat Only mode.
Can View Only	y or n	Flag whether the user can run sessions in View Only mode.
Can Takeover	y or n	Flag whether the user can run sessions in Shared Control mode.
Can Record	y or n	Flag whether the user can record sessions.
Can View Recordings	y or n	Flag whether the user can view other user's recordings.
Can View Reports	y or n	Flag whether the user can run and view reports.
Enable port forwarding	y or n	Flag whether the user can use port forwarding during a session.
Enable reverse port forwarding	y or n	Flag whether the user can use reverse port forwarding during a session.

## Sample of the CSV file for users

The following example is the structure for importing two users, with each set of details separated by a semicolon (;). John Doe is not an administrator and cannot view the recordings of other users or reports. Jane Star is an administrator user with full permissions.

```
U,John Doe,jdoe@aos.ibm.com,Test Users,John Doe,n,y,y,y,y,n,n,y,n;  
U,Jane Star,jstar@aos.ibm.com,Test Users,Jane Star,y,y,y,y,y,y,y,y,y;
```

## Viewing lists of recordings

You can select the dates between which to view a set of recordings on the Report Options page. The list shows all permanent and temporary recordings for associated users within the specified period.


### Procedure


1. Click **Admin options > View Recordings**. The Report Options page opens.

---

## Report options

Please select the boundary dates for the report or leave them blank for a full report

Start Date (yyyy-mm-dd):  

End Date (yyyy-mm-dd):  

Limit to selected teams

AlphaTest  
AlphaTest/BetaTeam

Automatically include subteams

Screen out multiple failure attempts


Generate report

Back

---

Figure 59. Report Options page

2. Choose one of the following options:

Option	Description
View recordings for all support sessions	Clear the <b>Start Date</b> and <b>End Date</b> fields.
View recordings within a specified period	In the <b>Start Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget (  ) to select the start date.  In the <b>End Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget to select the end date.

3. In the Limit to Selected teams list, select the teams on which to view the associated recordings.
4. Select **Automatically include subteams** if you want to include the subteams for the teams selected in step 3.
5. Click **View Recordings**. The Recordings page opens.

### What to do next

You can run, save, or export recordings to another video format.

## Assist On-site Player

The Assist On-site Player is a Java application to open and view recordings of Assist On-site support sessions that are saved in the proprietary video format, .aos. You can download the application and run it locally, or you can run it as an applet through the Administration Portal.

## Saving recordings

You can save recordings that are displayed on the Recordings page to a location of your choosing. Recordings are in a proprietary video format, .aos. You need the Assist On-site Player to open and view recordings in this format.

## Before you begin

You can download the Assist On-site Player from the Administration Portal Downloads page. For more information, see “Viewing available installers to download” on page 89.

## Procedure

1. In the **Recordings** table, click **Save** for the recording that you want to save. The Save As window opens.
2. Browse to the location in which you want to save the recording.
3. Click **Save**.

## Exporting recordings

You can export recordings to another video format such as AVI or MOV on the Report Options page.

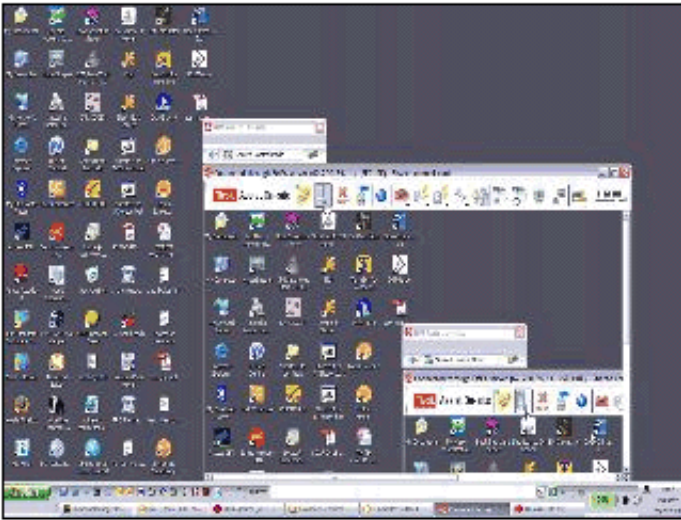
## Before you begin

You can use the View Recordings function to show a list of recordings that you can export to another format. For more information, see “Viewing lists of recordings” on page 100.

## Procedure

1. In the **Recordings** table, click **Export** for the recording that you want to export. The Video Export page opens.

## Export recording



User Sysop

Start time 2009-09-24 03:00:36

End time 2009-09-24 03:00:47

Duration 0:00:11

## Exports

Type	Width	Height	Size	By	Created
<input type="radio"/> avi	640	480			

[Download](#)

[Back](#)

Figure 60. Video Export page

2. From the Type list, select the video format to which you want to export.
3. In the **Width** field, type the width of the screen in pixels.
4. In the **Height** field, type the height of the screen in pixels.

### CAUTION:

If you change the width and height, you might impact the quality and size of the exported file.

5. Click **Download** to begin the export. The export status page opens displaying the progress of the export.
6. After the two stages are 100% complete, click **Download** to save the exported file locally.

### Opening and viewing recordings online

You can open and view a recording on the Recordings page. Recordings are saved to a proprietary video format, .aos. If you have not installed the applet for the Assist On-site Player, you are prompted to install it. You need the player to view recordings in this format.

## Before you begin

You can save the recording to your local machine. You can download the Assist On-site Player and use the player to open and view the recording rather than viewing it online. For more information, see "Opening and viewing recordings offline" on page 106

## Procedure

1. In the **Recordings** table, click **Open** for the recording that you want to open and view.
2. If you have not previously installed the Assist On-site Player applet, you are prompted to install it. The Run Assist On-site applet window opens.

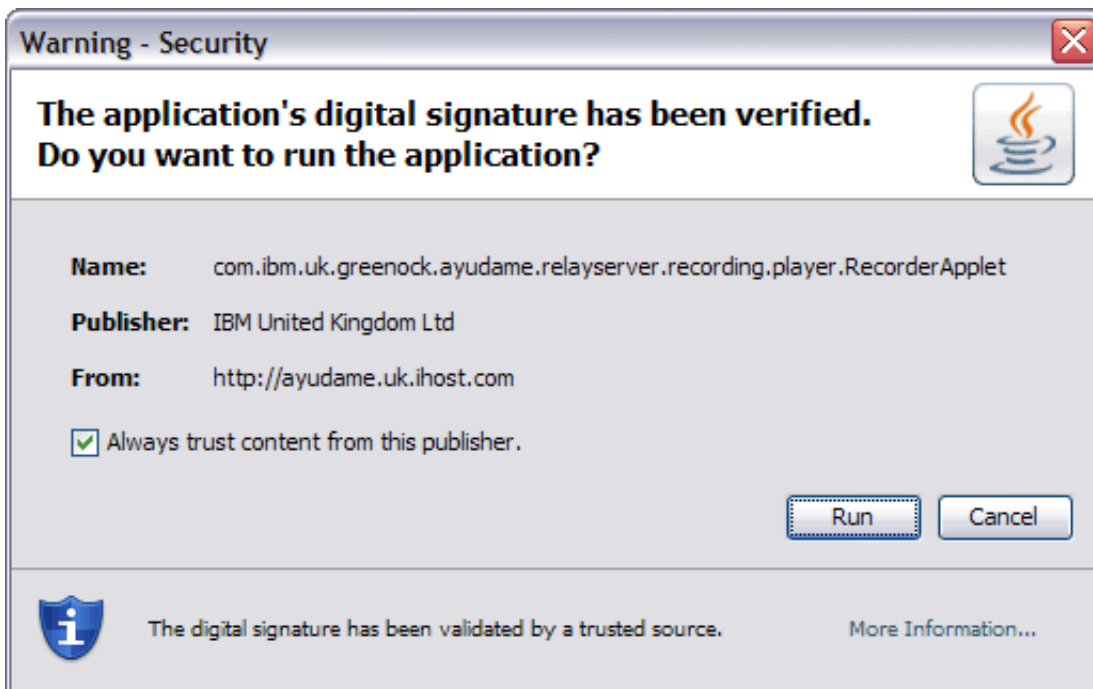


Figure 61. Run Assist On-site Player applet window

3. Click **Run** to install the applet. The Assist On-site Player window opens.



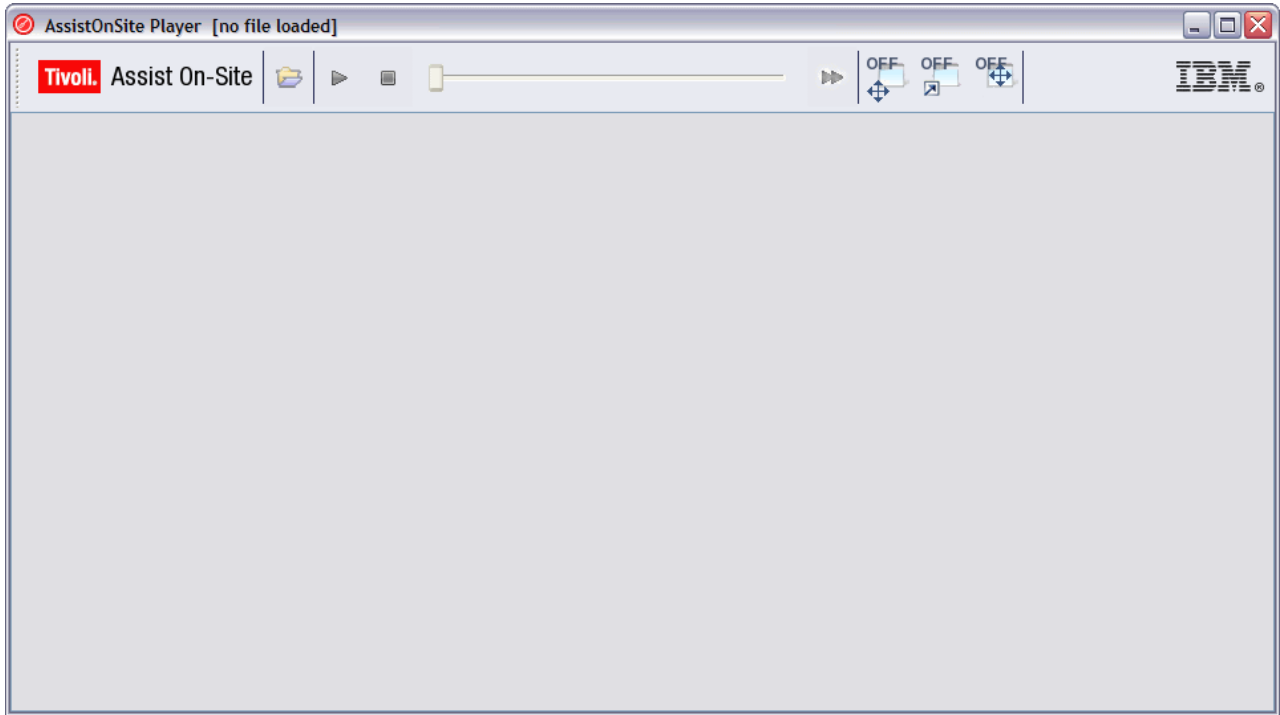













Figure 62. Assist On-site Player window

4. Click  to play the recording.
5. Choose any of the following options while playing the recording:
  - Click  to stop the recording.
  - Click  to fast forward the recording. Alternatively, click the slider to fast forward or rewind the recording.
  - Click  or  to toggle between turning on and off scaled view.
  - Click  or  to toggle between turning on and off full screen mode.
  - Click  or  to toggle between turning on and off automatic scrolling.
  - Click  to browse to the location of the recording and to open it.

- Click  to pause the recording.

### Opening and viewing recordings offline

You can save recordings locally, open, and view them in the Assist On-site Player. Recordings are in a proprietary video format, .aos and you need the player to view recordings in this format.

### Before you begin

Ensure that you have downloaded the Assist On-site Player from the Administration Portal Downloads page. For more information, see “Viewing available installers to download” on page 89.

### Procedure

1. Open a command-line interface, and run the Assist On-site Player. For example:  

```
javaw -jar aos_player_root\AOSPlayer.zip
```

The Assist On-site Player window opens.

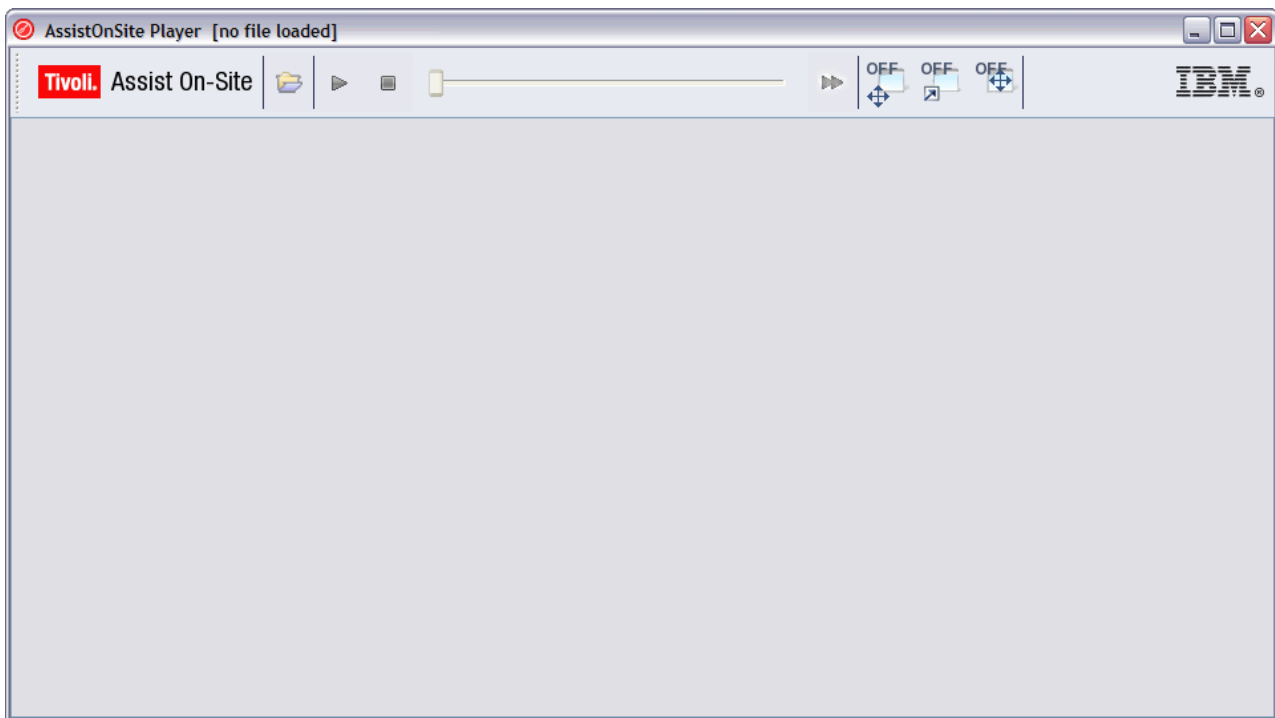














Figure 63. Assist On-site Player window

2. Click  to browse to the location of the recording and to open it.
3. Click  to play the recording.
4. Choose any of the following options while playing the recording:

- Click  to stop the recording.
- Click  to fast forward the recording. Alternatively, click the slider to fast forward or rewind the recording.
- Click  or  to toggle between turning on and off scaled view.
- Click  or  to toggle between turning on and off full screen mode.
- Click  or  to toggle between turning on and off automatic scrolling.
- Click  to browse to the location of the recording and to open it.
- Click  to pause the recording.

## Viewing administrative reports

You can select the dates between which to view the administrative report on the Report options page. The report shows summaries of sessions' status for the selected teams and subteams, customer survey participation, support engineers' performances, sessions details, customer survey results, and the number of sessions recorded or temporarily recorded.


### Procedure


1. Click **Admin options > View Reports**. The Report Options page opens.

---

## Report options

Please select the boundary dates for the report or leave them blank for a full report

Start Date (yyyy-mm-dd):  

End Date (yyyy-mm-dd):  

Limit to selected teams

AlphaTest  
AlphaTest/BetaTeam

Automatically include subteams

Screen out multiple failure attempts


[Generate report](#)

[Back](#)

---

Figure 64. Report Options page

2. Choose one of the following options:

Option	Description
View details for all support sessions for the selected teams	Clear the <b>Start Date</b> and <b>End Date</b> fields.
View details for support sessions for the selected teams between a set of dates	In the <b>Start Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget (  ) to select the start date.  In the <b>End Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget to select the end date.

3. In the Limit to Selected teams list, select the teams on which to report.
4. Select **Automatically include subteams** if you want to include the subteams for the teams selected in step 3.
5. Clear **Screen out multiple failure attempts** if you do not want to report on failed connections.
6. Click **Generate Report**.

## Results

The report opens in the page. Click **Save as CSV File** if you want to save the data from the report to a CSV file for further analysis.

## Viewing the audit history for administrators

You can first select the team to which the administrator belongs on the Report Options page. Then you can select the administrator for which to view the audit history on the Select Administrator page. The report displays the actions associated with the selected administrator, the target user or team, descriptions for each action, and the time the action occurred.

### Procedure

1. Click **Admin options > Audit History**. The Audit History page opens.
2. Click **View action carried out by administrator**. The Report Options page opens.
3. In the **Limit to Selected teams** list, select the team to which the administrator belongs.
4. Click **View**. The Select Administrator page opens if there are more than one administrators in the team.
5. From the **Administrator** list, select the administrator.
6. Click **View audit history**.

## Viewing the audit history for selected users or teams

You can select the users or teams for which to view the audit history on the Select User/Team page. The report displays the actions associated with the selected users or teams, the associated administrator, descriptions for each action, and the time the action occurred.

### Procedure

1. Click **Admin options > Audit History**. The Audit History page opens.
2. Click **View action carried out by others**. The Select Users/Teams page opens.
3. From the **Target** list, select the users or teams.
4. Click **View Target Audit History**.

---

## Server management functions

The Administration Portal has a set of functions for the Relay Server. These functions let the administrator view the current status of the Relay Server, the number of past connections, the bandwidth usage, and reports on connectivity issues. Administrators can access these functions on the Administration Portal home page or the **Server Management** menu.

## Viewing the status of the Relay Server

You can view the current status of the Relay Server including its active satellite servers on the Current Relay Server Status page. The report displays the current supported version for the Remote Support Console, the total amount of data forwarded to target machines or controller machines, and the total number of currently active and waiting sessions. You can also view details about the most recent sessions, such as the support engineer and customer, IP addresses, relevant session dates and times, and the status for the session.

## Procedure

1. Click **Server Management > Current Relay Server Status**. The Current Relay Server Status page opens.
2. To display additional information about recent sessions, click Show. The Current Relay Server Status with Recent Session Details page opens.

[Refresh](#)

## Current Relay Server Status

Version: 3.1.0.0009  
Accepting connections

Total time running: 423:15:40  
Data forwarded to console: 300474kB  
Data forwarded to client: 895kB

Active satellite servers:

## Session Details

Waiting Sessions: 0

Active Sessions: 0

Recent Sessions: 22 [\[hide\]](#)

Customer Name	Customer Number	Rep IP	Rep Email	Customer IP	Creation date	Start date	End date	Session time (s)	Status	Data forwarded to client	Data forwarded to console	Details
		193.34.56.24	admin@aos.ibm.com	212.150.181.66	Aug 17, 2009 10:56:46 AM	Aug 17, 2009 10:57:47 AM	Aug 17, 2009 11:02:10 AM	0:04:22	4: Finished	59kB	5800kB	<a href="#">View details</a>

Figure 65. Current Relay Server Status with Recent Session Details page


## Viewing the bandwidth history of the Relay Server

You can select the dates between which to view the bandwidth history for the Relay Server on the Relay Server Bandwidth History page. The page contains a graph that plots the bandwidth for each session forwarded by the Relay Server. You can click a data point to view the associated session details.

### Before you begin

You must have an SVG viewer to view the graph on the page. Mozilla Firefox, Opera and other Web browsers natively support SVG graphics. If you have Microsoft Internet Explorer, you can download an SVG plug-in from Adobe at the following address: <http://www.adobe.com/svg/viewer/install/>

## Procedure

1. Click **Admin options > View Reports**. The Relay Server Bandwidth History page opens.
2. In the **Select dates** from field, enter a date in the format YYYY-mm-dd or use the calendar widget (  ) to select the start date.
3. In the to field, enter a date in the format YYYY-mm-dd or use the calendar widget to select the end date.
4. Select **Update** to update the graph with data for the selected dates.


## Viewing the connections history

You can select the dates between which to view the history of Assist On-site concurrent sessions on the Connection History page. The page contains graphs that plot the number of simultaneous active connections and the maximum number of connections during a specified time period. You can click a data point in the first graph to view the associated session details.

### Before you begin

You must have an SVG viewer to view the graph on the page. Mozilla Firefox, Opera and other Web browsers natively support SVG graphics. If you have Microsoft Internet Explorer, you can download an SVG plug-in from Adobe at the following address: <http://www.adobe.com/svg/viewer/install/>

### Procedure


1. Click **Admin options > View Reports**. The Relay Server Bandwidth History page opens.
2. In the **Select dates from** field, enter a date in the format YYYY-mm-dd or use the calendar widget (  ) to select the start date.
3. In the **to** field, enter a date in the format YYYY-mm-dd or use the calendar widget to select the end date.
4. Select **Update** to update the graph with data for the selected dates.

## Viewing the connectivity problems report

You can select the dates between which to view the connectivity problems on the Connectivity Problem Report Options page. The report contains information about the session ID, the date that the issue was submitted, the customer name and number, the associated PMR, the support engineer, whether they were successful in later sessions, any comments and contact details.

### Procedure

1. Click **Admin options > View Reports**. The Connectivity Problem Report Options page opens.
2. Choose one of the following options:

Option	Description
View reported connectivity problems for all dates	Clear the <b>Start Date</b> and <b>End Date</b> fields.
View reported connectivity problems for a specified time period	In the <b>Start Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget (  ) to select the start date.  In the <b>End Date</b> field, enter a date in the format YYYY-mm-dd or use the calendar widget to select the end date.

3. Select **Generate Report**.

---

## Uploading branding resource bundles

You can upload it on the Assist On-site custom branding page.

## Before you begin

Create the branding resource bundle. For more information, see “Branding resource bundle.”

## Procedure

1. On the Home page, click **Custom Branding**.

# Assist On-site custom branding

---

## Upload Bundle

Bundle name

File

## Delete Bundle

Bundle name

---

Figure 66. Assist On-site custom branding page

2. In the **Bundle name** field, type its name.
3. In the **File** field, type its path and file name. Alternatively, click **Browse** to select it.
4. Click **Upload**.

## What to do next

Edit the team. From the **Resources bundle** list, select the default branding resource bundle. For more information, see “Managing teams” on page 95.

## Branding resource bundle

The Assist On-site Configuration Wizard configures the Remote Support Console to use your team's default resource branding bundle.

## Purpose

The bundle is a ZIP file that has:

- **config**: Contains the `resources.properties` file
- **resources**: Contains the graphics files of any format, such as JPEG or PNG



## resources.properties

Table 16 outlines the properties.

**Note:** If you do not enter a file name for a property, Assist On-site uses the default value.

Table 16. *resources.properties*

Properties	Description
LeftLogoHorizontal	Logo for the left horizontal bar of the Console. The pixel properties are: <ul style="list-style-type: none"><li>• Height: 178</li><li>• Width: 44</li></ul>
LeftLogoVertical	Logo for the left vertical bar of the Console. The pixel properties are: <ul style="list-style-type: none"><li>• Height: 110</li><li>• Width: 50</li></ul>
RightLogoHorizontal	Logo for the right horizontal bar of the Console. The pixel properties are: <ul style="list-style-type: none"><li>• Height: 88</li><li>• Width: 44</li></ul>
RightLogoVertical	Logo for the right vertical bar of the Console. The pixel properties are: <ul style="list-style-type: none"><li>• Height: 88</li><li>• Width: 44</li></ul>
SplashScreen	Splash screen for the Console. The pixel properties are: <ul style="list-style-type: none"><li>• Height: 650</li><li>• Width: 540</li></ul>
ApplicationIcon	Application logo for the title bar of the Console. The pixel properties are: <ul style="list-style-type: none"><li>• Height: 32</li><li>• Width: 32</li></ul>
ApplicationName	The custom name for Console for the title bar of the Console.

### Custom resources.properties file

LeftLogoHorizontal=left\_horizontal.jpg  
LeftLogoVertical=left\_vertical.jpg

RightLogoHorizontal=right\_horizontal.jpg  
RightLogoVertical=right\_vertical.jpg

SplashScreen=splash.jpg

ApplicationIcon=icon.png

ApplicationName=<My organization's name for RSC>



---

## Chapter 5. Relay Server

The Relay Server is one of the main components of Assist On-site. It is an application server that handles the data transmissions for support sessions between the Remote Support Console and the Remote Support Utility. There is a network of servers across several geographic regions, with support engineers and customers connecting to those servers within their geographic regions.

Table 17 outlines the connection details for the Relay Server in each geographic region. The Americas Relay Server is also the server that provides the connection codes for support sessions and distributes the Remote Support Utility installer for customers. Support engineers and customers must be able to connect to the Americas Relay Server and should also be able to connect to a Relay Server in their geographic region if not located in the Americas.

Table 17. Relay Server connection details

Region	IP Address	Port	SSL	Comments
Americas	72.15.208.234	8200	No	The fully qualified name is: aos.us.ihost.com
	72.15.208.234	80	No	
	72.15.223.61	8200	No	The fully qualified name is: aosback.us.ihost.com
	72.15.223.61	80	No	
EMEA	81.144.208.229	8200	No	The fully qualified name is: aos.uk.ihost.com
	81.144.208.229	443	Yes	
	81.144.208.229	443	No	
	81.144.208.229	80	No	
Asia Pacific	203.141.90.53	8200	No	
	203.141.90.53	443	Yes	
	203.141.90.53	443	No	
	203.141.90.53	80	No	



---

## Chapter 6. Assist On-site Support Service

The Assist On-site Support Service is a component of Assist On-site. It is an applicative service that has features similar to the Remote Support Utility and runs on target machines. It registers itself with the Relay Server and sends HTTPS heartbeats as status updates. Assist On-site Support Service configuration uses customer policies that determine when and how the support engineer can run unattended support sessions.

---

### Downloading and installing the Support Service

You can log on to the Administration Portal and download the installer for Windows operating systems only or binaries for multiple platforms from the Downloads page.

#### Procedure

1. Log on to the Administration Portal.
2. Click **User Options > Downloads**. The Downloads page opens.
3. (On **Windows systems**) Click `aos_support_service_setup.exe`. When prompted, click **Open** or **Run** to download.

**Note:** You might need to temporarily allow popup windows in your Web browser depending upon your Web browser security settings.

4. (On **Linux systems**) Click `ibm-aos-support-service-_ver.rpm`. Do the following steps:
  - a. When prompted, click **Save File**.

**Note:** You might need to temporarily allow popup windows in your Web browser depending upon your Web browser security settings.

- b. Run it using a graphical tool or command-line interface.

---

### Configuring the Assist On-site Support Service

Assist On-site Support Service configuration uses customer policies that determine when and how the support engineer can run unattended support sessions.

#### Procedure

1. Choose one of the following options:
  - (On **Windows systems**) Click **Start > All Programs > IBM > Assist On-site Support Service Configuration**.
  - (On **Linux systems**) Run the executable file, `aos_cfg`, in the Assist On-site Support Service's installation directory.

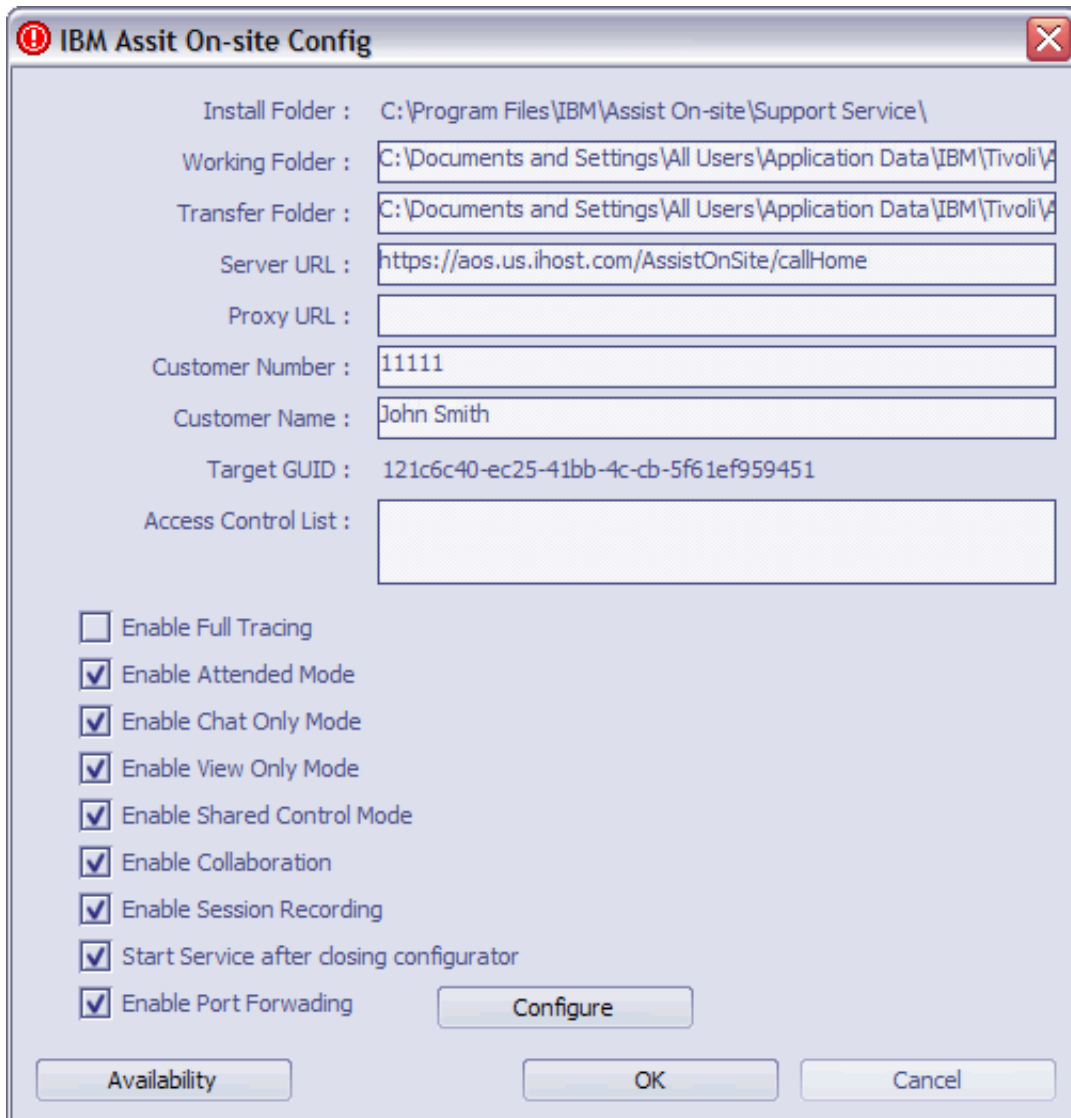


Figure 67. Support Service Config window

2. Enter your customer number and name.
3. In the **Server URL** field, type the URL for the listening Relay Server, for example:  
https://aos.us.ihost.com/AssistOnSite/callHome
4. In the **Access Control List (ACL)** box, type a comma-separated list of Assist On-site user IDs (e-mail addresses) and Assist On-site team names.
5. Clear the check boxes to disable session modes, collaboration, or session recording.

**Important:** If you do not clear **Enable Attended Mode**, ACL members cannot run unattended support sessions.

6. If you want to turn on tunneling, select **Enable Port Forwarding**. You can configure port forwarding. For more information, see “Configuring port forwarding” on page 119.
7. Click **OK**.
8. Use your operating system's tools to start the service.

## Configuring port forwarding

You can configure port forwarding and reverse port forwarding on the Configure Port Forwarding window. After you explicitly configure permission for port forwarding, the support engineer can begin the unattended port forwarding session to the authorized ports.

### Procedure

1. Optional: In the Support Service Config window, select **Enable Port Forwarding** if required.
2. Click **Configure**. The Configure Port Forwarding window opens.

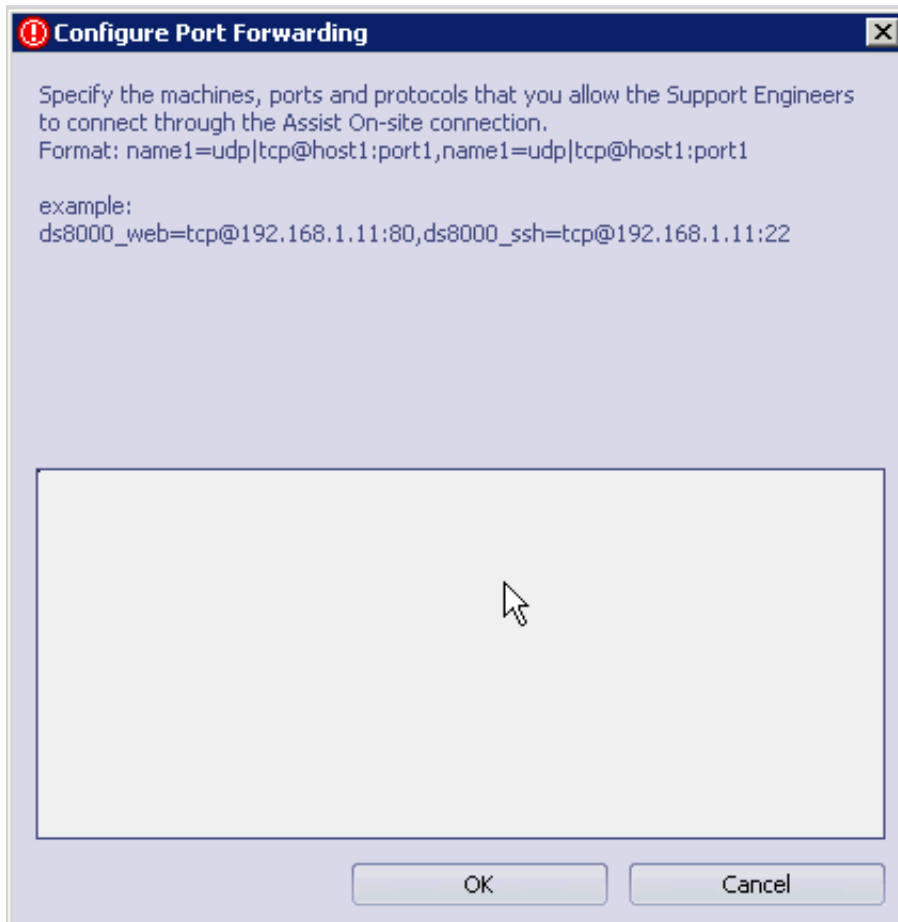


Figure 68. Configure Port Forwarding window

3. In the text box, type a comma-separated list of host machine aliases, host machines, ports, and protocols that the support engineers can connect to during an Assist On-site session. The syntax for each allowed connection in the list is as follows:

`<host_alias>=udp|tcp@<host_name>|<IP_addr>:<port_num>`

Table 18. Variables for the port forwarding syntax

Variable	Description
<code>&lt;host_alias&gt;=</code>	The optional alias name for the host machine, for example, ds8000_web or ds8000_ssh.

Table 18. Variables for the port forwarding syntax (continued)

Variable	Description
udp tcp	The protocol for the connection, whether UDP or TCP, for example, tcp.
<host_name> <IP_addr>	The fully qualified name of the host machine or its IP address, for example:198.162.1.2 <b>Note:</b> If you want to configure a reverse port forwarding option, use 0.0.0.0 as the IP address.
<port_num>	The listening port for the connection, for example, 3456 or 22.

For example:

ds8000\_web=tcp@198.162.1.2:80,ds\_rev=tcp@0.0.0.0:3457

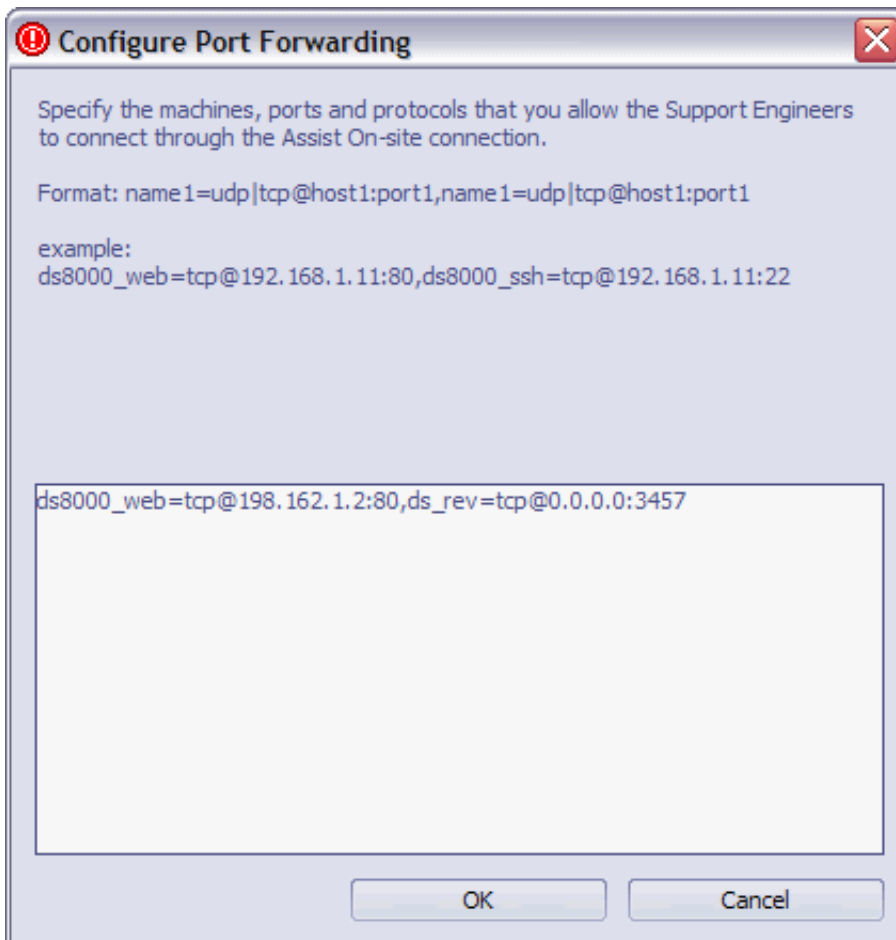


Figure 69. Configure Port Forwarding window with examples

4. Click **OK**.



---

## Notices

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

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

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

For license inquiries regarding double-byte (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.  
3-2-12, Roppongi, Minato-ku, Tokyo 106-8711 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 might not apply to you.

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

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

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

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

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

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

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

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

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

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

#### 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. 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 IBM's application programming interfaces.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

## Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com)<sup>®</sup> are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at <http://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.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

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.

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

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



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

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.

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

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







Product Number:

Printed in USA