Microsoft
WINDOWS
VISTA
Mitch Tulloch, Tony Northrup, and Jerry Honeycutt, with the Microsoft Windows Vista Team
Resource Kit

Windows Vista™ Resource Kit

Mitch Tulloch, Tony Northrup, Jerry Honeycutt with the MSWinVista Team

9780735622838
Publication Date: April 2007

Microsoft Press

Table of Contents

Part II Deployment

Part III Desktop Management

Part IV Desktop Maintenance

Part V Networking

Part VI Troubleshooting

Chapter 23

Supporting Users Using Remote Assistance

In this chapter:

Remote Assistance (RA) in Windows Vista includes a number of improvements in connectivity, performance, usability, and security along with feature enhancements that make it even more useful than RA in Windows XP. With increased Group Policy support, command-line scripting capabilities, session logging, bandwidth optimization, and more, Remote Assistance is now an essential tool for enabling enterprises to support users in Help Desk scenarios. This chapter examines how Remote Assistance works in Vista, how to use it to support end users, and how to manage it using Group Policy and scripts.

Understanding Remote Assistance

Supporting end users is an essential function of IT departments and the corporate Help Desk. Unfortunately, conventional technical support provided over the telephone or using chat tools is generally cumbersome and inefficient. As a result, supporting users is often both time-consuming and costly for large enterprises to implement. For example, end users often have difficulty describing the exact nature of the problem they are having. Because of their general inexperience and lack of technical knowledge, end users may try to describe their problem using non-technical, inexact language. As a result, Help Desk personnel are generally reduced to asking a series of simple questions to try and isolate the problem the user is having. The methodical nature of these questions sometimes causes users to feel as if Help Desk personnel are being condescending, and such misunderstanding can reduce the effectiveness of the support experience and can make users tend to avoid contacting support personnel when future problems arise.

End users also often have difficulty following instructions given to them by Help Desk personnel who are trying to assist them. Well-trained support personnel will try to avoid using technical jargon when communicating with end users, but although using plain language can improve the support experience, it may also mean that resolution steps become long and tiresome. For example, telling a user how to use Disk Cleanup from System Tools in Accessories can require several sentences or more, and this kind of communication can add time to support incidents, making them more costly to the company.

Remote Assistance (RA) solves these problems by enabling support personnel to view the user's desktop in real time. The user seeking assistance can demonstrate the nature of the problem to the support person. This is a quicker and more efficient way to communicate a problem than using words or e-mail. If necessary, the user can also give the support person permission to assume shared interactive control of the user's computer to show the user how to resolve the problem. The result of using Remote Assistance is faster problem resolution, an improved support experience, and a lower Total Cost of Ownership (TCO) for supporting end users in large, corporate environments.

Remote Assistance vs. Remote Desktop

Remote Assistance and Remote Desktop are different features of Vista that have entirely different uses. Remote Desktop is based on Microsoft's Terminal Services and is a tool for remotely logging on to remote computers. When you use Remote Desktop to connect to a remote computer, a new user session is established. Remote Desktop can also establish sessions with computers that have no interactive sessions running (no users logged on locally) such as headless servers. For more information on Remote Desktop, see Chapter 28, "Connecting Remote Users and Networks."

Remote Assistance, on the other hand, is a tool for interactively helping users troubleshoot problems with their computers. To use Remote Assistance, both the User (also called the Novice) and the Helper must be present on their computers. Unlike Remote Desktop, Remote Assistance does not create a new session. Instead, Remote Assistance allows the Helper to work in the existing session of the User. The User's desktop gets *remoted* to the Helper, who can then view the User's desktop and, with the User's consent, share control of the desktop.

Here is another way to summarize the difference between these two features: In Remote Assistance, both users involved are looking at the same desktop using the same logon credentials (those of the interactively logged-on User) and can share control of that desktop; in Remote Desktop, when the remote person logs on, the interactively logged-on user (if there is one) is logged out.

Improvements to Remote Assistance in Windows Vista

Windows Vista includes a number of new features and enhancements for Remote Assistance compared to the Remote Assistance available in Windows XP, including:

- Connectivity improvements with transparent NAT traversal using Teredo and IPv6.

- An improved user interface that is easier to launch and use.
- A standalone executable (msra.exe) that accepts command-line arguments and can easily be scripted.
- Improved overall performance with a smaller footprint, quicker startup and connect times, and optimized bandwidth usage for screen updates.
- Enhanced security with mandatory password and integration with UAC.
- New Offer RA via IM scenario and an open API for integration with peer-to-peer applications.
- Additional Group Policy settings for improved manageability.

Remote Assistance in Vista deprecates the following features that were available on XP:

- No more support for the MAILTO method of solicited Remote Assistance
- No more support for voice sessions

For information on interoperability between the XP and Vista versions of Remote Assistance, see the section titled "Interoperability with Remote Assistance in Windows XP" later in this chapter.

How Remote Assistance Works

In Remote Assistance, the person needing help is referred to as the *User* (or *Novice*) and the support person providing assistance is called the *Helper* (or *Expert*). RA is launched from the Start Menu by navigating to All Programs, clicking Maintenance, and then selecting Windows Remote Assistance. It can also be launched from a command prompt by typing **msra.exe**.

Remote Assistance has two basic modes of operation:

- **Solicited RA** In *Solicited RA* (also known as *Escalated RA*) the User requests assistance from the Helper by initiating the RA session using e-mail, instant messaging, or by providing the Helper with a saved copy of an invitation file (*.MsRcIncident). Each of these methods uses a different underlying mechanism:
  - ❑ **Solicited RA using e-mail** This method requires that the e-mail clients being used by the User support Simple Mail Application Programming Interface (SMAPI). An example of an e-mail client that supports SMAPI is Windows Mail, which is included with Windows Vista. Other examples of SMAPI-compliant e-mail clients include Microsoft Outlook and other third-party clients. In this approach, the User launches the RA user interface to create an email message that has an RA invitation file (*.MsRcIncident) attached to the message. The User must enter a password for the RA session, which must be communicated to the Helper using an out-of-band (OOB) method such as calling the Helper on the telephone. When the Helper receives the User's RA invitation, she opens the attached ticket, enters the

password that was conveyed by the User, and the RA session starts. The Helper must respond to the invitation from the User within a specified time limit (default is 6 hours) or the invitation will expire and a new one will need to be sent. In a domain environment this ticket lifetime can also be configured using Group Policy. See the section titled "Managing Remote Assistance Using Group Policy" later in this chapter.

  - **Solicited RA using file transfer** This method requires that both the User and Helper have access to a common folder (such as a network share on a file server) or that they use some other method for transferring the file (for example, by using a USB key to manually transfer the file or by uploading the file to an FTP site). The user creates an RA invitation file and saves it in the shared folder. The User must provide a password that must be communicated to the Helper using an out-of-band (OOB) method such as a telephone call. The Helper retrieves the ticket from the shared folder, opens it, enters the password, and the RA session starts. Again, the Helper must respond to the invitation within a specified time or the invitation will expire and a new one will be needed (the expiration time is configurable using Group Policy).
  - **Solicited RA using Instant Messaging** This method for soliciting assistance requires that the instant messaging (IM) applications being used by both the User and the Helper support Microsoft's new Rendezvous API. Windows Live Messenger is an example of an IM application that supports Rendezvous. Windows Live Messenger is available as a download. In this approach, the User requests assistance from someone on his buddy list. To ensure that the remote person is really the User's buddy (and not someone masquerading as the buddy), Remote Assistance requires that a password be relayed from the User to the Helper by other means (such as a phone call) before the Helper can connect. For more information on the Rendezvous API, see the Windows SDK on MSDN at *http://windowssdk.msdn.microsoft.com/en-us/library/default.aspx*.

- **Unsolicited RA** In Unsolicited RA (also known as Offer RA) the Helper offers help to the User by initiating the RA session.
  - **Offer RA using DCOM** This is a typical corporate Help Desk scenario in which all the users are in a domain. The Helper enters either the fully qualified name (FQDN) or IP address of the User's computer to connect to the User's computer. This method requires that the Helper has been previously authorized a domain administrator to be able to offer Remote Assistance to the Users. (For information on how to authorize Helpers for offering RA, see the section titled "Managing Remote Assistance Using Group Policy" later in this chapter.) This method also requires that the Helper either knows the name (the host name on a local subnet; the fully qualified name otherwise) or address (IPv4 or IPv6) of the User's computer.
  - **Offer RA using Instant Messaging** This method for soliciting assistance requires that the instant messaging (IM) applications being used by both the User and the

Helper support the Rendezvous API. In this approach, the Helper offers assistance to someone on her buddy list. If the buddy agrees, then he must enter a password to be used by the Helper. The password must be relayed by an OOB mechanism to ensure that the remote person is really the User's buddy (and not someone masquerading as the buddy). For more information on the Rendezvous API, see the Windows SDK on MSDN at *http://windowssdk.msdn.microsoft.com/en-us/library/default.aspx*.

How It Works: RA Invitation Files

Remote Assistance invitation files (.MsRcIncident) are XML-formatted file documents that include information used by the Helper's computer that will attempt to connect. This ticket information is encrypted to prevent unauthorized users from accessing the information should e-mail or file transfer be used to send the invitation over an unsecured network.

If the e-mail method is used to send the invitation file to the Helper, the invitation file is sent as an e-mail attachment with a file name of RATicket.MsRcIncident. If the file transfer method is used instead, the invitation file is created by default on the desktop of the User's computer and the file name of the invitation is Invitation.MsRcIncident.

Remote Assistance Operational States

Remote Assistance has three operational states:

- **Waiting For Connect** This state occurs when either:
  - ❑ The Helper has offered RA to the User but the User has not yet agreed to allow the Helper to connect to his computer.
  - ❑ The User has sent the Helper an invitation but the Helper has not yet responded by opening the invitation, or the Helper has opened the invitation and the User has not yet agreed to allow the Helper to connect to his computer.

  In the Waiting For Connect state, the Helper cannot view or control the screen of the User's computer until an RA connection has been established and both computers have entered the Screen Sharing state. Once the RA application has been started and is running in the Waiting For Connect state, the application should not be closed until the other party responds and establishes the connection. For example, if the User uses the Solicit RA Using E-mail method and sends an invitation file to a Helper, the RA application opens on the User's computer and waits for the Helper to accept the invitation. If the User closes RA on her computer before the Helper accepts the invitation, the Helper will not be able to connect to the User's computer and the User will need to send a new invitation.

- **Screen Sharing** This state occurs when the User has consented to allow the Helper to connect to his computer—either after the User has sent the Helper an invitation or the Helper has offered RA to the User. In the Screen Sharing state, an RA session has been established and the Helper can view—but not control—the screen of the User's computer.

  When the User is prompted for consent to allow the Helper to connect to his computer, a warning message appears on the User's computer saying that the Helper wants to connect to his computer. This warning message is customizable using Group Policy. See the section titled "Managing Remote Assistance Using Group Policy" later in this chapter for more information.

- **Control Sharing** This state occurs after the Screen Sharing state, when the Helper has requested control of the User's computer and the User has consented to allow the Helper to have shared control of his computer. In the Control Sharing state, the Helper has the same level of access to the User's computer that the User has and the Helper can use his own mouse and keyboard to remotely perform actions on the User's computer. Specifically:

  - If the User is a standard user on his computer, the Helper will only be able to perform actions on the User's computer that can be performed by a standard user on that computer.
  - If the User is a local administrator on his computer, the Helper will be able to perform any actions on the User's computer that can be performed by a local administrator on that computer.

  For more information on the level of control that a Helper has on a User's computer, see the section titled "Remote Assistance and the Secure Desktop" later in this chapter.

User vs. Helper Functionality

Once an RA connection has been established and both computers have entered the Screen Sharing state, the User and Helper are able to perform the tasks listed in Table 23-1.

Table 23-1 Tasks That Can Be Performed by User and Helper During an RA Session

Description of task	User?	Helper?
Chat	Yes	Yes
Send files	Yes	Yes
Save a log of session activity	Yes (default)	Yes (default)
Configure bandwidth usage	Yes	No
Pause (temporarily hide screen)	Yes	No
Request shared control	No	Yes
Give up shared control	Yes	Yes
Disconnect	Yes	Yes
Disconnect using Esc key	Yes	No

Remote Assistance and NAT Traversal

Remote Assistance works by establishing a peer-to-peer connection between the User's computer and the Helper's computer. One challenge this poses is that it can be difficult to establish peer-to-peer connections if one or both of the computers involved are behind a gateway or router that uses Network Address Translation (NAT). NAT is an IP routing technology described by RFC 1631 that is used to translate IP addresses and TCP/UDP port numbers of packets being forwarded. NAT is typically used to map a set of private IP addresses to a single public IP address (or to multiple public addresses). Home networks using a wireless or wired router also use NAT technology.

To overcome this difficulty, Vista includes built-in support for Teredo, an IPv6 transition technology described in RFC 4380 that provides address assignment and automatic tunneling for unicast IPv6 connectivity across the IPv4 Internet. The NAT traversal capability provided by Teredo in Vista allows RA connectivity when one or both of the users involved in an RA session are hidden behind a NAT. The RA experience is transparent from the perspective of the users involved, regardless of whether NAT is being used on either user's network. For most small business and home user environments, Vista's RA will seamlessly traverse a NAT-enabled router with no additional router configuration required. For information on enterprises that need to remotely support users who work from home, see the section titled "Other Possible Remote Assistance Usage Scenarios" later in this chapter.

> **Note** Offering RA using DCOM is not usually a Teredo scenario because enterprise users are behind a corporate firewall and not separated from each other by NATs.

Remote Assistance will not connect in certain configurations. Specifically:

- Teredo cannot traverse a symmetric NAT. Remote Assistance can only connect across restricted NATs and cone NATs. In most cases, this is not a significant limitation because the large majority of deployed NATs are either the restricted or cone variety. For more information on NAT traversal support in Vista, see Chapter 29, "Deploying IPv6."
- RA will not work if the NAT-enabled router is configured to block the specific ports used by RA. See the section titled "Remote Assistance and Windows Firewall" later in this chapter for more information.
- Remote Assistance will not work if the user's NAT-enabled router is configured to block all UDP traffic.

> **Note** To determine the type of NAT a network is using, open an elevated command prompt and type **netsh interface teredo show state**.

For more information on IPv6 support in Windows Vista, including built-in client support for Teredo and other IPv6 transition technologies, see Chapter 29.

Remote Assistance and IP Ports Used

The ports used by a Remote Assistance session depend on whether the session is between two Vista computers or between a Vista computer and a downlevel Windows XP computer. Specifically:

- **Vista to Vista RA Session** Dynamic ports allocated by the system in the range TCP/UDP 49152–65535
- **Vista to XP RA Session** Port 3389 TCP (local/remote)

In addition, the Offer RA via DCOM scenario uses Port 135 (TCP).

Remote Assistance and Windows Firewall

The Windows Firewall is configured with a group exception for Remote Assistance. This group exception has multiple properties that are grouped together as part of the RA exception. The RA exception properties will change depending on the network location of the computer (private, public, or domain). For example, the default RA exception when the computer is in a public location is stricter than when the computer is in a private location. In a public location (such as an airport), the RA exception is disabled by default and does not open ports for Universal Plug-and-Play (UPnP) and Simple Service Discovery Protocol (SSDP) traffic. In a private network (a home or work network, for example) the RA exception is enabled by default and uPnP and SSDP traffic is permitted.

Table 23-2 summarizes the state of the Remote Assistance firewall inbound exception for each type of network location. The RA exception has outbound properties as well; however, the Windows Firewall is not by default configured to enable outbound properties.

Table 23-2 Default State Of Remote Assistance Firewall Inbound Exception for Each Type of Network Location

Network location	State of RA exception	Default properties of the RA exception
Private (Home or Work)	Enabled by default	■ Msra.exe application exception ■ uPnP enabled for communications with uPnP NATs ■ Edge traversal enabled to support Teredo
Public	Disabled by default—must be enabled by user with Admin credentials	■ Msra.exe application exception ■ Edge traversal enabled to support Teredo

Table 23-2 **Default State Of Remote Assistance Firewall Inbound Exception for Each Type of Network Location**

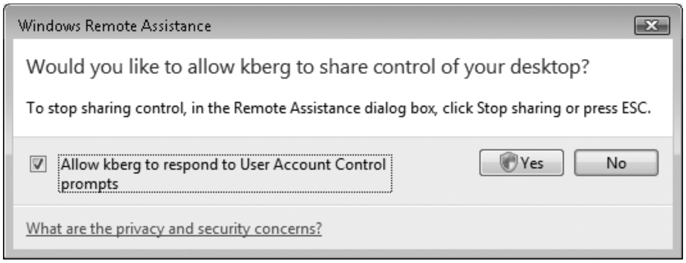
Network location	State of RA exception	Default properties of the RA exception
Domain	Disabled by default—typically enabled by Group Policy	■ Msra.exe application exception ■ RAServer.exe (the RA COM server) application exception ■ DCOM Port 135 ■ uPnP enabled for communications with uPnP NATs

In other Windows Firewall profiles, the default configuration of the Remote Assistance exception is as follows:

- **Private profile** The RA exception in the Windows Firewall is enabled by default when the computer location is set to "private." It is configured for NAT traversal using Teredo by default so that users in a private networking environment (for example, the home environment) can solicit help from other users who may also be behind NATs. The private profile includes the appropriate exceptions needed to allow communication with uPnP NAT devices. If there is a uPnP NAT in this environment, Remote Assistance will attempt to use the uPnP for NAT traversal. Offer RA via DCOM is not configured in this profile.
- **Public profile** The RA exception is disabled by default and no inbound RA traffic is permitted. Windows Firewall is configured this way by default to better protect users in a public networking environment (such as a coffee shop or airport terminal). When the RA exception is enabled, NAT traversal using Teredo is enabled. However, traffic to uPnP devices is not enabled and Offer RA via DCOM is not enabled.
- **Domain Profile** The RA exception when the computer is in a domain environment is geared towards the Offer RA scenario. This exception is disabled by default and is typically enabled via Group Policy. Teredo is not enabled in this profile because corporate networks typically have a corporate firewall that blocks Teredo UDP traffic. However, uPnP is enabled so that uPnP NATs can be communicated with.

Remote Assistance and the Secure Desktop

When a User consents to having a Helper share control of her computer during a Remote Assistance session, the User has the option of allowing the Helper to respond to UAC prompts (Figure 23-1). Typically, User Account Control (UAC) prompts appear on the Secure Desktop (which is not remoted) and consequently the Helper cannot see or respond to Secure Desktop prompts. The Secure Desktop mode is the same mode that a user sees when she logs on to her computer or presses the Secure Attention Sequence (SAS) keystroke (Ctrl+Alt+Delete). UAC elevation prompts are displayed on the Secure Desktop instead of the user's normal desktop to protect the user from unknowingly allowing malware to run with elevated privileges on her computer. The user must provide consent to a UAC prompt to return to her normal desktop and continue working. This consent requires either clicking Continue (if the user is a local admin on her computer) or by entering local admin credentials (if she is a standard user on her computer).



Windows Remote Assistance

Would you like to allow kberg to share control of your desktop?

To stop sharing control, in the Remote Assistance dialog box, click Stop sharing or press ESC.

☑ Allow kberg to respond to User Account Control prompts

Figure 23-1 The User has the option of allowing the Helper to respond to UAC prompts when the RA session is in Control Sharing State.

It is important to understand that the Secure Desktop on the User's computer is not remoted to the Helper's computer. In other words, the Helper can only respond to UAC prompts on the User's computer using the User's own credentials. This means that if the User is a standard user on her computer while the Helper is a local administrator on the User's computer, the Helper can only have administrative privileges on the User's computer if the User can first supply those credentials.

Enforcing this limitation is essential to ensure the security of Vista desktops. The reason behind this design decision is that if RA was architected to allow the Helper to remotely elevate the User's privileges, the User would be able to terminate the RA session and thus steal local admin credentials from the Helper.

Remote Assistance Logging

Remote Assistance can generate a session log of RA-associated activity. Session logging is enabled by default and consists of time-stamped records that identify RA-related activities on each computer. Session logs only contain information about activities that specifically relate to RA functionality, such as who initiated the session, whether consent was given to a request for shared control, and so on.

Session logs do not contain information on actual tasks that the User or Helper performed during a session. For example, if the Helper is given Shared Control privileges, starts an Admin command prompt, and performs steps to reconfigure the TCP/IP configuration on the User's computer during an RA session, the session logs will not contain a record of this action.

Session logs do include any chat activity performed during an RA session. The log generated during a session is also displayed within the chat window so that both the User and the Helper can see what is being logged during the session. Session logs also include any file transfer activity that occurs during the session, and also record when the session has been paused.

Purpose of RA Session Logging Session logs for RA are mainly intended for enterprises that are required to maintain records of system and user activity for record-keeping purposes. They are not intended as a way to record every action performed by Help Desk personnel when troubleshooting problems with users' computers. A typical environment in which session logging might be required would be in a banking environment, where a financial institution is required by law to maintain records of who accessed a computer and at what time.

Because the ACLs on these session logs grant the User full control over logs stored on her own computer, by default session logs are generated on both the User's computer and Helper's computer so that the Helper can protect and archive them from tampering. The logs created on each side of an RA session are similar but not identical. This is because session logs are generated from the perspective of the computer involved—whether the User's computer or the Helper's computer—and therefore complement each other instead of being identical.

In an enterprise environment, Group Policy can be used to enable or disable session logging. If session logging is not configured using Group Policy, both the User and Helper are free to disable session logging on their own computers. For more information, see the section titled "Managing Remote Assistance Using Group Policy" in this chapter.

Session Log Path and Naming Convention Session logs are XML-formatted documents so that they can be easily integrated into other data sets—for example, by importing them into a database managed by Microsoft SQL Server 2005. All session logs are stored under each user's Documents folder within the following path:

Users\user_name\\Documents\\Remote Assistance Logs

A unique session log file is created for each RA session on the computer. Log files stored within this folder are formatted using XML and are named using the convention *YYYYMMDDHHMMSS*.xml, where the time format is 24-hour. For example, a session log created at 3:45:20 p.m. on August 13, 2006, would be named 20060813154520.xml.

The XML content of a typical session log looks like this:

```
<?xml version="1.0" ?>
<SESSION>
  <INVITATION_OPENED TIME="3:24 PM" DATE="Wednesday, August 09, 2006" EVENT="A Remote Assist
ance invitation has been opened." />
  <INCOMING_IP_ADDRESS TIME="3:26 PM" DATE="Wednesday, August 09, 2006">fe80::2856:e5b0:fc18
:143b%10</INCOMING_IP_ADDRESS>
  <CONNECTION_ESTABLISHED TIME="3:26 PM" DATE="Wednesday, August 09, 2006" EVENT="A Remote A
ssistance connection has been established.">jdow</CONNECTION_ESTABLISHED>
  <EXPERT_REQUEST_CONTROL TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow has r
equested to share control of the computer." />
  <EXPERT_GRANTED_CONTROL TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow has b
een granted permission to share control of the computer." />
```

```
  <EXPERT_CONTROL_STARTED TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow is sh
aring control of the computer." />
  <EXPERT_CONTROL_ENDED TIME="3:27 PM" DATE="Wednesday, August 09, 2006" EVENT="jdow is not
sharing control of the computer." />
  <CHAT_MESSAGE TIME="3:30 PM" DATE="Wednesday, August 09, 2006">jdow: test</CHAT_MESSAGE>
  <CHAT_MESSAGE TIME="3:30 PM" DATE="Wednesday, August 09, 2006">jchen: ok</CHAT_MESSAGE>
  <CONNECTION_ENDED TIME="3:30 PM" DATE="Wednesday, August 09, 2006" EVENT="The Remote Assis
tance connection has ended." />
  <INVITATION_CLOSED TIME="3:30 PM" DATE="Wednesday, August 09, 2006" EVENT="A Remote Assist
ance invitation has been closed." />
</SESSION>
```

Using Remote Assistance in the Enterprise

The main Remote Assistance scenario within a corporate networking environment is supporting desktop computers that are on the corporate network and joined to a domain. Users' machines must be configured appropriately before they can be offered RA. This is done via Group Policy, as explained in the section of this chapter titled "Managing Remote Assistance Using Group Policy." Additionally, the Remote Assistance exception in the Windows Firewall must be enabled. For more information, see the section titled "Remote Assistance and Windows Firewall" earlier in this chapter .

Because most corporate networks have a perimeter firewall blocking access from outside the internal network, supporting remote users who are connecting from outside the corporate network can be more difficult. However, most enterprises now use virtual private network (VPN) technologies to allow remote users to connect to their corporate networks over the Internet, and this kind of scenario generally poses no problem to RA functionality.

Using Remote Assistance in the Corporate Help Desk Environment

The standard approach to using Remote Assistance in an enterprise environment is for Help Desk personnel to offer Remote Assistance to users who telephone in to request assistance. A typical scenario might be as follows:

1. User Jane Dow (the User) is having problems configuring an application on her computer. She phones Help Desk, explains her problem briefly, and asks for help.
2. A Help Desk person named Jacky Chen (the Helper) asks Jane for the fully qualified name or IP address of her computer. She responds with the information, which she can get from computer properties or by running ipconfig.
3. Jacky starts Remote Assistance on his computer and uses the Offer RA feature to offer help to Jane. This causes a dialog to appear on Jane's computer, asking her if she would like to allow Jacky to connect to her computer.
4. Jane accepts the offer, and at this point Jane's desktop may temporarily change to conserve network bandwidth used by the Remote Assistance session. The Remote Assistance window that opens on Jane's screen tells her that she is being helped by Jacky.

5. At this point, Jacky can see Jane's screen but he can't control it. Jane then explains the problem she is having, either by using the Chat feature of Remote Assistance, or more likely over the telephone. Jacky asks Jane to perform a series of steps to correct the problem and watches her screen in his own Remote Assistance window as she does this.

6. If the instructions Jacky provides are too complex or if time is limited, Jacky can ask Jane if he can share control of her computer. If Jane agrees, Jacky clicks the Request Control button at the top of his Remote Assistance window. A dialog appears on Jane's desktop asking her if she wants to allow Jacky to share control of her desktop. Jane accepts the prompt, and also selects the option to allow Jacky to respond to User Account Control (UAC) prompts on Jane's computer.

7. Jacky is now connected to Jane's computer using Jane's credentials, and he can both view her screen and interact with it using his own mouse and keyboard. Jacky then proceeds to perform the steps needed to resolve the problem, either correcting the issue or demonstrating to Jane how to fix the problem if it occurs again in the future. If at any time Jane wants to force Jacky to relinquish control of her computer, she can click the Stop Sharing button, the Disconnect button, or press the Panic key (Esc).

> **Note** Offer RA needs preconfiguration of the User's machine via Group Policy. See the section titled "Managing Remote Assistance Using Group Policy" later in this chapter for more information.

Other Possible Remote Assistance Usage Scenarios

Other types of Remote Assistance scenarios are also possible for businesses ranging from large enterprises to Small Office/Home Office (SOHO) environments. Examples of possible usage scenarios include:

- A user who is having a problem with configuring an application on her computer can phone Help Desk for assistance. A support person can then use Offer RA to connect to the user's computer, ask for control of her screen, and show the user how to configure her application. This scenario is the standard one for enterprise Help Desk environments and is described in more detail in the section titled "Using Remote Assistance in the Corporate Help Desk Environment" later in this chapter.
- A user who is having trouble installing a printer sends an RA invitation to Help Desk using Windows Mail. A support person who is monitoring the Help Desk e-mail alias reads the message, opens the attached invitation file, and connects to the user's computer. The support person asks for control of the user's computer and walks him through the steps of installing the printer.
- A user is on the road and is connected to the internal corporate network using a VPN connection over the Internet. The user is having problems configuring Windows Mail on her computer, so she opens Windows Messenger and notices that someone she

knows in Corporate Support is currently online. She sends an RA invitation to the support person using Windows Messenger, who responds to the invitation, asks for control, and shows the user how to configure Windows Mail.

The preceding list is not intended to be complete–other corporate support scenarios using RA are possible. Generally speaking, however, corporate environments will use Offer RA to provide assistance to users who phone Help Desk when they have problems. Some enterprises may also allow users to submit RA invitations either via e-mail or by saving invitation files to network shares that are monitored by support personnel. Others may use instant messaging applications that support Remote Assistance within the corpnet.

Note Helpers can have multiple RA sessions open simultaneously—one session for each User they are supporting. However, Users can have only one RA session in the Waiting For Connect state. The invitation that was created could be sent to multiple recipients—any of whom may connect. All subsequent connect attempts will be blocked until the first helper disconnects, after which another helper may connect. If the user disconnects the session, the RA application terminates and no further connections will be allowed.

Interoperability with Remote Assistance in Windows XP

Remote Assistance in Vista is backward-compatible with Remote Assistance in Windows XP, with the following limitations:

- Offer RA from Vista to XP is supported, but Offer RA from XP to Vista is not supported. This means that enterprises who want to implement Offer RA as a support solution for their Help Desk departments should ensure that computers used by support personnel who will help users running Vista are themselves running Vista. (and not XP).
- NAT traversal using Teredo and IPv6 is supported on Vista to Vista RA only, and not on Vista to XP.
- Voice support for RA in XP is not supported by RA in Vista, and any attempt by a User on an XP computer to use this feature during an RA session with a Helper on a Vista computer will cause a notification message regarding this limitation to appear.
- The MAILTO method of soliciting assistance that is supported by RA in XP is not supported by RA in Vista.
- Windows Messenger (which shipped with XP) does not ship with Vista. Users of RA with Windows Messenger in XP will need to migrate to an IM vendor that supports Vista and Remote Assistance. Windows Live Messenger currently supports XP, Vista, and Remote Assistance.
- Offer RA via Messenger is a new feature in Vista and is not available in Windows XP.

Implementing and Managing Remote Assistance

Remote Assistance is a powerful and flexible feature that can be used in many different ways to support users within large enterprises, medium-sized businesses, and SOHO environments. This section outlines how to initiate Remote Assistance sessions from both the UI and the command line. The section also demonstrates how to use Remote Assistance in an enterprise Help Desk environment involving two common scenarios:

- Helper offers RA to User who has telephoned Help Desk with a problem.
- User creates an RA invitation and saves it on a network share that is monitored by Help Desk personnel.

For information on other scenarios for implementing Remote Assistance, including sending invitations with Windows Mail and Windows Messenger, search for the topic "Remote Assistance" within Windows Help and Support.

Initiating Remote Assistance Sessions

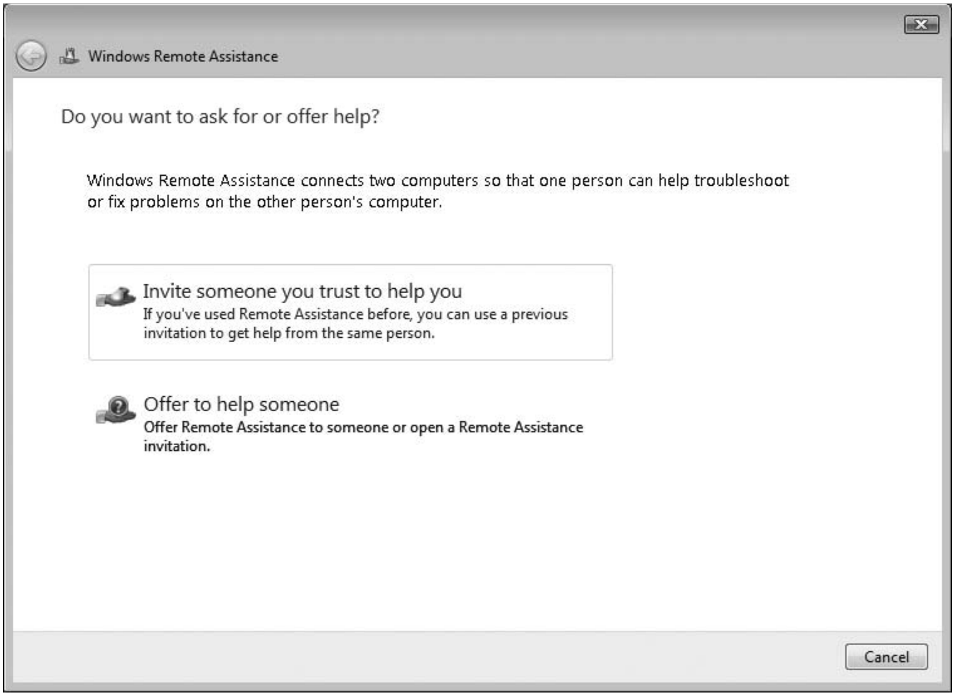
Remote Assistance sessions can be initiated either from the user interface or the command line. A significant usability enhancement, from the perspective of support personnel, is that Offer RA is no longer buried within Help And Support as it was in Windows XP, but is instead easily accessible now from the GUI.

Initiating Remote Assistance From the GUI

Initiating Remote Assistance sessions from the GUI can be done using any of several available methods:

- From the Start menu, click Start, then All Programs, then Maintenance, and then Windows Remote Assistance. This launches the RA app.
- Click Start, then Help And Support, and then under the Ask Someone heading click Windows Remote Assistance.
- Click Start, type **assistance**, and when Windows Remote Assistance appears in the Programs list, click it.

Any of these methods will open the initial Remote Assistance screen, shown in Figure 23-2.



Do you want to ask for or offer help?

Windows Remote Assistance connects two computers so that one person can help troubleshoot or fix problems on the other person's computer.

Invite someone you trust to help you
If you've used Remote Assistance before, you can use a previous invitation to get help from the same person.

Offer to help someone
Offer Remote Assistance to someone or open a Remote Assistance invitation.

Figure 23-2 The initial screen of Windows Remote Assistance.

Initiating Remote Assistance From the Command Line

Remote Assistance in Vista is implemented as a standalone executable called msra.exe. You can initiate RA sessions directly from the command line or by using scripts. The syntax and usage for this command is explained in Table 23-3.

Table 23-3 Syntax and Usage for Command-Line Remote Assistance (msra.exe)

Option	Description
/novice	Launches Remote Assistance as Novice in Solicited RA mode and presents the user with the choice of either sending an RA ticket using a SMAPI-enabled e-mail application such as Windows Mail or by saving the invitation as a file. Once this choice has been made, Windows Remote Assistance opens on the Novice's computer in the Waiting For Connect state.
/expert	Launches Remote Assistance in the Helper mode and presents the user with the choice of either specifying the location of an RA ticket to open or specifying the Novice's computer name or address (Offer RA). The computer name can be either a host name (if the Novice is on the local subnet) or a fully qualified name (DNS name), and the address can be either an IPv4 address or an IPv6 address. Unsolicited RA without an invitation requires preconfiguration of the remote machine being helped.

Table 23-3 Syntax and Usage for Command-Line Remote Assistance (msra.exe)

Option	Description
/offerRA *computer*	Launches Remote Assistance as Helper in Unsolicited (Offer) RA mode and uses DCOM to remotely open Remote Assistance on the Novice's computer and then connect to the Novice's computer to initiate an RA session. The Novice's computer can be specified using either its computer name or address. The computer name can be either a host name (if the Novice is on the local subnet) or a fully qualified name (DNS name), and the address can be either an IPv4 address or an IPv6 address. This method is demonstrated in more detail in the section titled "Scenario 1: Offering Remote Assistance to Novices" later in this chapter.
/email *password*	Launches Remote Assistance as Novice in Solicited RA mode and creates a password-protected RA ticket that is attached to a new RA invitation message opened by the default SMAPI-enabled e-mail client (which by default is Windows Mail). The password must be six characters or more and must be relayed separately to the Helper. The e-mail client application launches a window with the invitation file attached. The User must enter the e-mail address of the Helper in the To field to send the message to the Helper.
/saveasfile *path password*	Launches Remote Assistance as Novice in Solicited RA mode and creates a password-protected RA ticket that is saved at the path specified. The path may be either a local folder or network share and the User must have appropriate permissions on the destination folder to create the file. The path must include a file name for the ticket. (The .MsRcIncident file extension will be automatically added to the file name.) The password must be six characters or more. Use of this method is demonstrated in more detail in the section titled "Scenario 2: Soliciting Remote Assistance by Creating RA Tickets and Saving Them on Monitored Network Shares" later in this chapter.
/openfile *path password*	Launches Remote Assistance as Helper in Solicited RA mode and opens a previously created RA ticket that was saved within the path specified. The path may be either a local folder or network share and the Helper must have appropriate permissions on the destination folder to open the file. The path must include the file name of a valid ticket that has the .MsRcIncident file extension. The password must be the same password that was used by the User to secure the ticket when it was created.

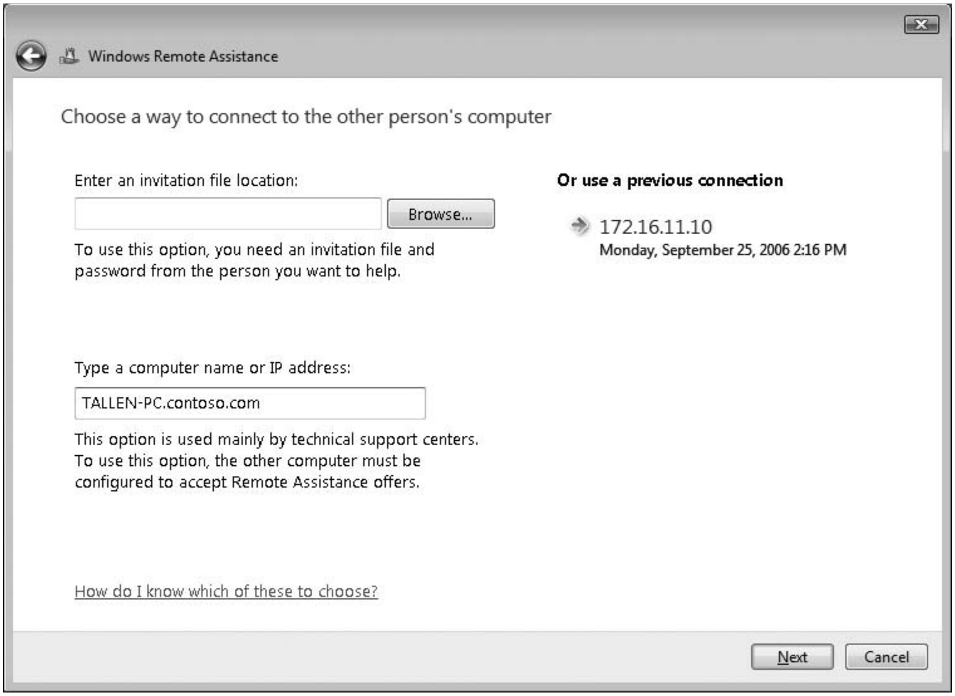
Note There is no support for Windows Managing Instrumentation (WMI) scripting of msra.exe.

Scenario 1: Offering Remote Assistance Using DCOM

Before you can offer Remote Assistance to other users, your user account must be authorized as a Helper on the user's computer. You can use Group Policy to do this in an enterprise environment. (See the section titled "Managing Remote Assistance Using Group Policy" in this chapter for information on how to do this.)

Once a support person (or group of individuals) has been configured as a Helper for all Vista computers in a domain or OU, the support person can offer RA to users of those computers when they need assistance. For this scenario, let's say that Tony Allen (tallen@contoso.com) is a Vista user who needs assistance with an issue on his computer. Tony telephones the Help Desk department and the call is taken by Karen Berg (kberg@contoso.com) who asks Tony for the name or IP address of his computer. Tony provides Karen with his fully qualified computer name (TALLEN-PC.contoso.com) or IP address, and Karen then offers assistance to Tony by following these steps:

1. Start Remote Assistance using any of the methods described previously.
2. Click Offer To Help Someone.
3. Enter **TALLEN-PC.contoso.com** in the field labeled Type A Computer Name Or IP Address.



Windows Remote Assistance

Choose a way to connect to the other person's computer

Enter an invitation file location:

To use this option, you need an invitation file and password from the person you want to help.

Or use a previous connection

172.16.11.10
Monday, September 25, 2006 2:16 PM

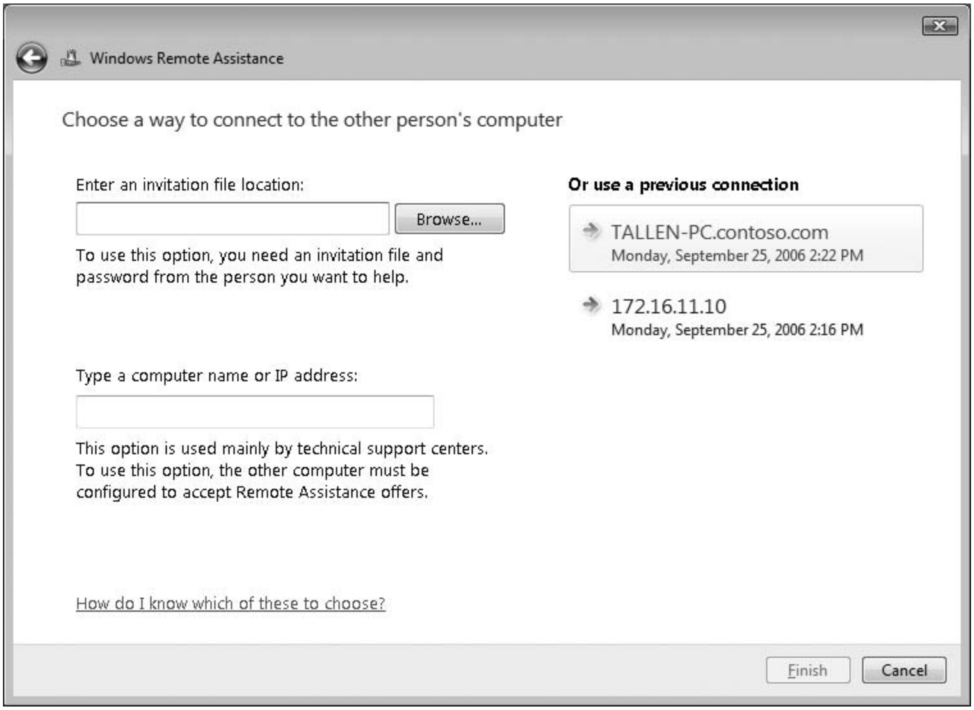
Type a computer name or IP address: TALLEN-PC.contoso.com

This option is used mainly by technical support centers. To use this option, the other computer must be configured to accept Remote Assistance offers.

How do I know which of these to choose?

4. Click Next.

At this point a dialog box will appear on Tony's computer asking if he would like to allow Karen to connect to his computer and view his desktop. Tony has two minutes to respond to this dialog before the offer times out and the dialog box disappears, which will cause a message saying "The person you are trying to help isn't responding" to appear on Karen's computer. If the offer to Tony times out, Karen can resubmit the offer by selecting it from the list of previous connections that are displayed in her RA application (Figure 23-3). If Tony accepts the offer (grants consent), the Remote Assistance session begins and Tony's desktop will be viewable by Karen in a Remote Assistance application window.



Windows Remote Assistance

Choose a way to connect to the other person's computer

Enter an invitation file location:

To use this option, you need an invitation file and password from the person you want to help.

Type a computer name or IP address:

This option is used mainly by technical support centers. To use this option, the other computer must be configured to accept Remote Assistance offers.

How do I know which of these to choose?

Or use a previous connection

TALLEN-PC.contoso.com
Monday, September 25, 2006 2:22 PM

172.16.11.10
Monday, September 25, 2006 2:16 PM

Figure 23-3 Recent RA invitations and offers listed under Or Use A Previous Connection can be reused.

At this point the desktop properties of Tony's desktop may change (based on configurable settings) to optimize the network bandwidth used by RA for screen updates on Karen's computer. Karen can now request control from Tony, send files to Tony or receive files from him, chat with Tony, or disconnect the session. Tony can send and receive files, chat, or pause or disconnect the session.

Note If you are a User and a Helper has shared control of your computer, you can immediately terminate shared control and return the session to Screen Sharing state by pressing the Panic key (Esc).

Scenario 2: Soliciting Remote Assistance by Creating RA Tickets and Saving Them on Monitored Network Shares

Another way that you can use Remote Assistance in an enterprise environment is by having users create invitation files and save them on a network share that is monitored by Help Desk personnel. This way, when Help Desk determines that a new ticket has been uploaded to the share, a support person can call the user on the telephone to obtain the password for the ticket and then use the ticket to establish an RA session with the user who needs help.

To make procedure easier, administrators an first deploy a script on users' desktops that uses command-line Remote Assistance (msra.exe) to create the invitation file and save it on the network share. For example, let's say that users' invitation files should be uploaded to \\FILESRV3.contoso.com\Support\IncomingTickets, a folder in the Support share on the file server named FILESRV3. The following script, named SubmitTicket.vbs, could be deployed on each user's desktop to accomplish this task:

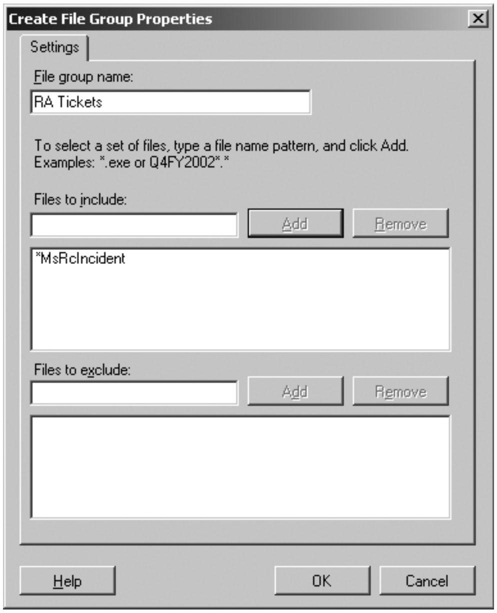
```
dim strPassword
dim strUser
dim strTicketName

strPassword = InputBox("Enter a password for your ticket")
Set WshShell = Wscript.CreateObject("Wscript.Shell")
strUser = WshShell.ExpandEnvironmentStrings("%username%")
strTicketName = strUser & "-" & Year(Now) & "-" & Month(Now) & "-" & Day(Now) & _
   "-" & Hour(Now) & "-" & Minute(Now) & "-" & Second(Now)
strRA = "msra.exe /saveasfile \\FILESRV3\Support\IncomingTickets\" & _
   strTicketName & " " & strPassword
WshShell.Run strRA
```

When the user double-clicks on this script to run it, an Input box appears asking the user to provide a password to be used to secure the invitation. After the user supplies a password, a new RA ticket is created and saved in the target folder on the file server. The name of the ticket is unique and consists of the user's name followed by the date and time, such as tallen-YYYY-MM-DD-HH-MM-SS.MsRcIncident. Once the support person monitoring the share has obtained the ticket's password using an OOB method such as a telephone call, the support person opens the ticket. After the User grants consent, the RA connection is established.

To monitor the IncomingTickets folder in the network share, Help Desk personnel can use the file-screening capabilities of Windows Server 2003 R2 file servers. To do this, you can create a passive file screen that monitors the folder and sends an e-mail alert to a Help Desk alias whenever a new ticket is uploaded to the folder. The steps for doing this are:

1. Install or upgrade the File Server role on the Windows Server 2003 R2 computer where the Support folder is located.
2. Start the File Server Resource Manager console from Administrative Tools, right-click the root node, and select Configure Options.
3. Specify the DNS name of the IP address of an SMTP host that can be used to forward alert e-mails generated by the file screen you will create.
4. Click OK to close File Server Resource Manager Options, and expand the console tree to select File Screens under File Screening Management.
5. Select the option Create File Screen in the Action pane.

6. Click Browse to select the Incoming folder for the File Screen Path.
7. Select the option labeled Define Custom File Screen Properties and click Custom Properties.
8. Choose the option for Passive Screening so that uploaded tickets will only be monitored and not blocked by the screen.
9. Click Create to create a new file group called RA Tickets and use the Add button to add files of type *MsRcIncident to the group.



Create File Group Properties

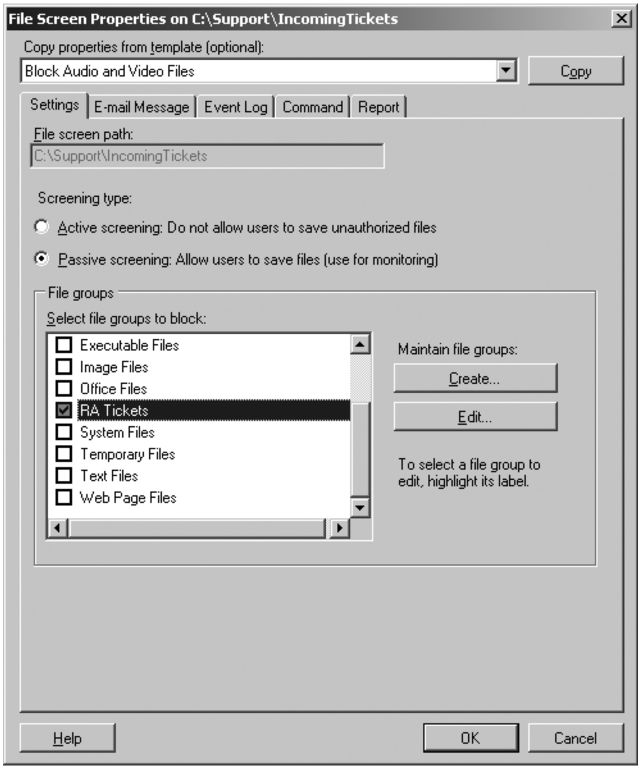
File group name: RA Tickets

To select a set of files, type a file name pattern, and click Add.
Examples: *.exe or Q4FY2002*.*

Files to include: *MsRcIncident

Files to exclude:

10. Click OK to return to the properties sheet for the new file screen, and select the check box for the RA Tickets file group you just created.



File Screen Properties on C:\Support\IncomingTickets

Copy properties from template (optional): Block Audio and Video Files

File screen path: C:\Support\IncomingTickets

Screening type:

○ Active screening: Do not allow users to save unauthorized files

● Passive screening: Allow users to save files (use for monitoring)

File groups

Select file groups to block:

- □ Executable Files
- □ Image Files
- □ Office Files
- ☑ RA Tickets
- □ System Files
- □ Temporary Files
- □ Text Files
- □ Web Page Files

Maintain file groups:

To select a file group to edit, highlight its label.

11. Click the Email tab and specify a support alias (such as support@contoso.com) that will be notified whenever a new ticket is uploaded to the folder. Configure a suitable subject and body for the message.

12. Click Create to create the new file screen and then choose the option to save the screen without creating a template.

13. Test the new file screen by opening a command prompt on a user's computer and typing **msra.exe /saveasfile *path password*** where *path* is the UNC path to the Incoming folder within the Support share on the file server, and *password* is any password of six or more characters that you specify.

For more information on how to implement file screening in Windows Server 2003 R2, see the topic "Screening Files" on the Microsoft Windows Server TechCenter at *http://technet2.microsoft.com/WindowsServer/en/library/de035087-2e9c-4b98-af4c-07d2d690ad6c1033.mspx*.

Managing Remote Assistance Using Group Policy

In an enterprise environment, Remote Assistance can be managed using Group Policy. The policy settings for Remote Assistance are all machine settings and are found in the following policy location:

Computer Configuration\Administrative Templates\System\Remote Assistance

When these policy settings are written to the registry on targeted computers, they are stored under the following registry key:

HKLM\SOFTWARE\Policies\Microsoft\WindowsNT\Terminal Services

Remote Assistance policy settings are summarized in Table 23-4.

Table 23-4 Group Policy Settings for Remote Assistance

Policy	Description
Solicited Remote Assistance	Enabling this policy allows users of targeted computers to use Solicited RA to request assistance using e-mail, file transfer, or instant messaging. Disabling this policy prevents users from using Solicited RA. The default setting is Not Configured, which allows users to change their Remote Assistance settings using the Remote tab of the System CPL in Control Panel. If the policy is Enabled, you can further configure whether Helpers can be prevented from sharing control of the User's computer, the maximum ticket lifetime, and the method used for sending invitations my e-mail. (Windows Vista does not support the MAILTO method—select SMAPI instead if the targeted computers are running Windows Vista.) Ticket lifetime applies only to RA invitations sent by e-mail or file transfer. The default ticket lifetime when Group Policy is not being used is 6 hours. If this policy is Enabled, you must also enable the Remote Assistance exception in Windows Firewall to allow Solicited RA to work. In an unmanaged environment, this setting can also be configured using the Remote tab of the System CPL in Control Panel. This policy is also supported on Windows XP Professional and Windows Server 2003.
Offer Remote Assistance	Enabling this policy allows designated Helpers to use Offer RA to offer assistance to users of targeted computers. Disabling this policy or leaving it Not Configured prevents Offer RA from being used to offer assistance to users of targeted computers. If the policy is Enabled, you can further configure whether Helpers can view or control the Users' computers, and you must specify a list of Helpers who are allowed to Offer RA to the users of the targeted computers. Helpers can be either users or groups and must be specified in the form *domain_name\username* or *domain_name\groupname*. If this policy is Enabled, you must also enable the Remote Assistance exception in Windows Firewall to allow Offer RA to work. This policy is also supported on Windows XP Professional and Windows Server 2003. See the Explain tab of this policy setting for more details.

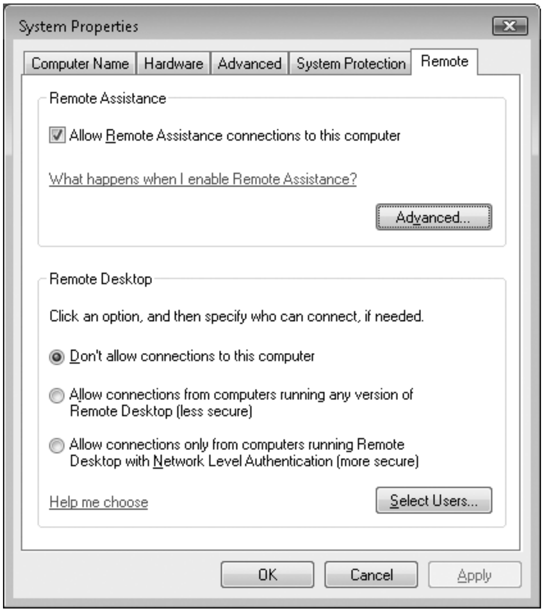
Table 23-4 **Group Policy Settings for Remote Assistance**

Policy	Description
Allow Only Vista Or Later Connections	The default Vista invitation file includes a XP-specific node for backward compatibility. This node is not encrypted and allows XP machines to connect to the Vista machine that created the ticket. Enabling this policy causes all RA invitations generated by users of targeted computers to *not* include the XP node, thereby providing an additional level of security and privacy. Disabling this policy or leaving it Not Configured leaves information such as IP address and port number unencrypted in RA invitations This policy setting only applies to RA invitations sent using e-mail or file transfer, and has no effect on using instant messaging to solicit assistance or on using Offer RA to offer assistance. In an unmanaged environment, this setting can also be configured by clicking Advanced from the Remote tab of the System Properties dialog. This policy is supported only on Windows Vista and later platforms.
Customize Warning Messages	Enabling this policy causes a specified warning to be displayed on targeted computers when a Helper wants to enter Screen Sharing State or Control Sharing State during an RA session. Disabling this policy or leaving it Not Configured causes the default warning to be displayed in each instance. If the policy is Enabled, you can further specify the warning message to be displayed in each instance. This policy is supported only on Windows Vista and later platforms.
Turn On Session Logging	Enabling this policy causes RA session activity to be logged on the targeted computers. For more information, see the section titled “Remote Assistance Logging” earlier in this chapter. Disabling this policy causes RA auditing to be disabled on the targeted computers. The default setting is Not Configured, in which case RA auditing is automatically turned on. This policy is supported only on Windows Vista and later platforms.
Turn On Bandwidth Optimization	Enabling this policy causes the specified level of bandwidth optimization to be used to enhance the RA experience over low-bandwidth network connections. Disabling this policy or leaving it Not Configured allows the system defaults to be used. If the policy is Enabled, you must specify the level of bandwidth optimization you want to use from the following options: ■ No Optimization ■ No Full Window Drag ■ Turn Off Background ■ Full Optimization (Use 8-Bit Color) If No Optimization is selected, the User’s computer will use the Windows Basic theme with full background, and during a shared control session the Helper will be able to drag full windows across the User’s screen. Additional optimization turns off effects to allow a more responsive experience for the Helper. This policy is supported only on Windows Vista and later platforms.

> **Note** In Windows XP, members of the Domain Admins group were implicitly granted Helper privileges even if they were not added to the Helpers list of the Offer Remote Assistance policy setting. This is no longer the case in Vista, where the Domain Admins group must now be explicitly added to the Helpers list to grant them Helper privileges for Offer RA.

Configuring Remote Assistance in Unmanaged Environments

Users of unmanaged computers can enable and configure Remote Assistance using the Remote tab of the System CPL in Control Panel (Figure 23-4). Enabling or disabling Remote Assistance and configuring its settings this way requires local administrator credentials on the computer, so a UAC prompt will appear when the user tries to do this.



Remote Assistance

☑ Allow Remote Assistance connections to this computer

What happens when I enable Remote Assistance?

Remote Desktop

Click an option, and then specify who can connect, if needed.

● Don't allow connections to this computer

○ Allow connections from computers running any version of Remote Desktop (less secure)

○ Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)

Help me choose

Figure 23-4 Configuring RA from the Remote tab of the System CPL in Control Panel.

Note that settings changes made this way will affect all users on the system. The per-machine registry settings for Remote Assistance are found under the following key:

HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance

In managed environments, when the following Group Policy setting is Enabled, the Control Panel settings for configuring Remote Assistance become unavailable (are grayed out).

Computer Configuration\Administrative Templates\System\Remote Assistance\Solicited Remote Assistance

> **Note** Group Policy settings always prevail over locally configured settings when they overlap.

Additional Registry Settings for Configuring Remote Assistance

Additional behavior for Remote Assistance can be configured by modifying certain registry settings. Specifically, per-user registry settings for Remote Assistance are found under the following key:

HKCU\Sofware\Microsoft\Remote Assistance

These settings are changeable when in the Waiting To Connect mode or when in the connected mode from the Settings button.

> **Caution** If Group Policy is used to manage Remote Assistance settings and any configured policy settings overlap these registry settings, the policy settings prevail.

Direct from the Source: Troubleshooting Remote Assistance

The following are some tips for troubleshooting Remote Assistance in Windows Vista:

1. *When I attempt to create an invitation with e-mail or save-to-file, I see a warning message that says that the Windows Firewall is currently blocking Remote Assistance.*

   The Remote Assistance firewall exception will change depending upon your network location (private, public, or domain). If you are at home, your network location type should be set to "private" since this enables the Remote Assistance firewall exception automatically. If your network location is set to "public," the Remote Assistance firewall exception is not enabled automatically for security purposes. It will need to be enabled by an Administrator.

   If you are connected to a managed network (for example when you are within a corporate domain) the network location is categorized as "domain" and the Remote Assistance exception is not enabled automatically. It is expected to be configured by Group Policy by your System Administrator.

2. *I cannot use RA to connect from my home computer to a work computer.*

   RA uses Teredo (IPv6) to traverse NATs. However, Teredo cannot be used to traverse corporate edge firewalls that provide NAT for intranet clients and blocks dynamic ports or outbound UDP traffic. Since you do not have a globally reachable IPv4 address within the corpnet, RA cannot make a connection to you from outside the corpnet.

3. *If I disable the Windows Firewall I cannot make an RA connection in certain cases. This is counter-intuitive since I expect connectivity to be less restrictive with the firewall disabled.*

   In Vista, the Windows Firewall is IPv6-aware. The RA exception in the Windows Firewall enables Teredo for edge traversal. If the Windows Firewall is disabled, the ability to use Teredo for NAT traversal is also disabled. The Windows Firewall must be running with the RA exception enabled for RA to be able to traverse NATs using Teredo.

4. *I cannot use RA to connect from my work to my home computer.*

   Your corporate firewall may be configured to block outbound peer-to-peer connections. In a managed environment (domain-joined computers), which is typically found in a corporate network, the RA exception does not enable Teredo (edge traversal) since corporate firewalls typically block outbound UDP traffic. NAT traversal using Teredo is disabled by default in this scenario. If the person you are trying to help is behind a UPnP NAT or directly connected to the Internet, you should be able to make a connection. Check with your network administrator to see if outbound peer-to-peer connections through the corporate firewall can be enabled.

5. *When I move my laptop (or change my home network location) from a "private" to "public" location, I am not able to connect to certain computers.*

   If you have a laptop that moves between work and home, the properties of the RA firewall exception in the Windows Firewall will change depending on whether your network location is classified as "private," "public," or "domain". In a private location, the RA exception is enabled by default, and if you are using a UPnP NAT, the RA exception will allow communications with the UPnP NAT to enable RA connections that make use of UPnP. In a public network the RA exception is not enabled by default and will need to be enabled using Administrator credentials. In addition, the default "public" profile does not permit UPnP communication for security purposes, thereby restricting RA connectivity in certain cases.

6. *I am on a low bandwidth connection and the person helping me is experiencing slow screen refreshes.*

   Set the Bandwidth Usage under Settings to "Low" to reduce the bandwidth used during a Remote Assistance connection. Keep in mind that display quality decreases as bandwidth usage is limited.

7. *Why can't I connect to XP machines that are behind a NAT as easily as I can connect to Vista machines?*

   RA in XP does not support Teredo for NAT traversal. Consequently, a Vista-to-XP RA connection attempt may fail in cases where both computers are behind non-UPnP NATs.

8. *How does RA make a connection?*

   When the RA invitation is created, the User's computer will set itself as a listener on all of its IP addresses (IPv4 and IPv6), including its Teredo address. All these listeners are waiting for a connection from the Helper's computer. The address and port information associated with these different listeners is relayed to the Helper's computer using the RA invitation (which gets transported by Messenger when Messenger is used to launch RA). The Helper's computer then tries to connect concurrently on all the address/port pairs in the invitation. The first successful connection that is made is used for the RA session and the rest of the connection attempts are terminated.

9. *How do I troubleshoot a connection failure between two home-based Vista machines that are behind NATs?*

   Refer to the RA Connectivity information in Tables 23-5 and 23-6 to verify that the network configuration you have is supported for RA connectivity. Then do the following:

   - ❑ Confirm that the Windows Firewall on the computer of the person that is being helped is running and configured for RA.
     - The Windows Firewall is IPv6 compatible and must be running to enable NAT traversal using Teredo.
     - The network location of the computer must set to "private" or "public" since Teredo is not enabled in "domain" or "managed" settings.
     - The Remote Assistance exception in the firewall must be enabled to allow RA connections.
   - ❑ Check that there is no edge firewall between User and Helper since it may block peer-to-peer applications like RA.
   - ❑ Confirm that the User and Helper are not behind a symmetric NAT and that Teredo is able to get to the "qualified" state on both machines. To determine this, do the following:
     1. First, initiate Teredo by forcing RA into the "waiting to connect" state. You can do this by typing msra.exe /saveasfile myinvitation mypassword at a command prompt.
     2. Then, check to see if Teredo can be activated on both machines and goes into the "qualified" state. Open an elevated command prompt window and type netsh interface teredo show state at the command prompt. The output should show Teredo in the "qualified" state. If Teredo does not go to the "qualified" state on both machines, an RA

connection may not be possible between these two computers. Teredo will not go into the qualified state if one of these 2 conditions exists:

- A global Teredo server could not be reached at teredo.ipv6.microsoft.com.
- The computer is behind a symmetric NAT. To verify this, look at the output of netsh interface teredo show state and check the output on the "NAT :" line which specifies NAT type.

10. *When I am helping someone who is a Standard user, I cannot run a program that needs Administrator privileges even though I have Administrator privileges to the user's computer.*

    RA allows a User to share control of their computer with a remote Helper. If the User is a Standard user, the remote Helper is given the same privileges as the Standard user. If the Helper attempts to launch a program that requires Administrator credentials, these credentials must be entered *locally* (on the Secure Desktop) by the User and cannot be entered remotely by Helper. This is required in order to prevent a security loophole where Admin programs launched by a remote Helper could be hijacked by the local User by simply terminating the RA session.

Table 23-5 RA Connectivity for Expert on Windows XP

		Expert on XP			
		Directly Connected	**Behind UPnP NAT**	**Behind non UPnP NAT**	**Behind corporate Edge Firewall****
Novice on XP	**Directly Connected**	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Msgr Only	Yes using Msgr Only	No	No
	Behind corporate Edge Firewall**	Yes using Msgr Only	Yes using Msgr Only	No	Yes - if both are behind same firewall No - if both are behind different firewalls

Table 23-5 RA Connectivity for Expert on Windows XP

		Expert on XP			
		Directly Connected	**Behind UPnP NAT**	**Behind non UPnP NAT**	**Behind corporate Edge Firewall****
Novice on Vista	**Directly Connected**	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Msgr Only	Yes using Msgr Only	No	No
	Behind corporate Edge Firewall**	Yes using Msgr Only	Yes using Msgr Only	No	Yes - if both are behind same firewall No - if both are behind different firewalls

Table 23-6 RA Connectivity for Expert on Windows Vista

		Expert on Vista			
		Directly Connected	**Behind UPnP NAT**	**Behind non UPnP NAT**	**Behind corporate Edge Firewall****
Novice on XP	**Directly Connected**	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Msgr Only	Yes using Msgr Only	No	No
	Behind corporate Edge Firewall**	Yes using Msgr Only	Yes using Msgr Only	No	Yes - if both are behind same firewall No - if both are behind different firewalls

Table 23-6 RA Connectivity for Expert on Windows Vista

		Expert on Vista			
		Directly Connected	**Behind UPnP NAT**	**Behind non UPnP NAT**	**Behind corporate Edge Firewall****
Novice on Vista	**Directly Connected**	Yes	Yes	Yes	Yes
	Behind UPnP NAT	Yes	Yes	Yes	Yes
	Behind non UPnP NAT	Yes using Teredo*	Yes using Teredo*	Yes using Teredo*	None
	Behind corporate Edge Firewall**	No	No	No	Yes - if both are behind same firewall No - if both are behind different firewalls

* Teredo connectivity is not available if either computer is behind a "symmetric NAT"

** Edge Firewall must permit outbound connection (e.g. using the Microsoft ISA Firewall Client)

John Thekkethala
Program Manager for Remote Assistance and the Remote Assistance team at Microsoft

Summary

Remote Assistance has been enhanced in Windows Vista to provide better performance, improved usability, NAT-traversal flexibility, and increased security. Best practices for implementing Remote Assistance in an enterprise environment include:

- Use Group Policy to enable users of targeted computers in a domain or OU to receive offers of RA from Help Desk personnel.
- Use Group Policy to enable the RA exception in the Windows Firewall.
- Use Group Policy to deploy scripts to enable users to run the msra.exe executable if you want to customize how they launch RA sessions—for example, to upload an invitation to a network share monitored by support personnel.
- If all of your support computers are running Vista, use Group Policy to encrypt RA tickets to hide sensitive information such as users' IP addresses and computer names.
- If corporate policy requires RA records for auditing purposes, use Group Policy to enable RA logging on your company's desktop computers and run scripts to periodically move both Helper and User RA logs to a safe storage.

- To meet corporate privacy and security requirements, use Group Policy to customize the text message that users see before they allow the Helper view their screens or share control.

Additional Resources

The following resources contain additional information and tools related to this chapter.

Related Information

- Remote Assistance FAQ from Windows Vista Help and Support can be found at *http://windowshelp.microsoft.com/Windows/en-US/help/398b5eda-aa7f-4078-94c5-1519b697bfa01033.mspx.*
- Remote Assistance Rendezvous API reference from the Windows SDK can be found at *http://windowssdk.msdn.microsoft.com/en-us/library/aa359213.aspx.*