



[Windows Server 2008 Technical Library](#) > [Terminal Services](#) > [Getting Started: Terminal Services](#)

Windows Server 2008 Terminal Services RemoteApp Step-by-Step Guide

Updated: January 24, 2008

With Terminal Services, organizations can provide access to Windows®-based programs from almost any location to almost any computing device. Terminal Services in Windows Server® 2008 includes Terminal Services RemoteApp™ (TS RemoteApp). You can use several different methods to deploy RemoteApp programs, such as Terminal Services Web Access (TS Web Access). With TS Web Access, you can provide access to RemoteApp programs through a Web page over the Internet or over an intranet. TS Web Access is also included in Windows Server 2008.

What are RemoteApp programs?

RemoteApp programs are programs that are accessed remotely through Terminal Services and appear as if they are running on the end user's local computer. Instead of being presented to the user in the desktop of the remote terminal server, the RemoteApp program is integrated with the client's desktop, running in its own resizable window with its own entry in the taskbar. Users can run RemoteApp programs side-by-side with their local programs. If a user is running more than one RemoteApp program on the same terminal server, the RemoteApp programs will share the same Terminal Services session.

In Windows Server 2008, users can access RemoteApp programs in several ways, depending on the deployment method that you choose. They can:

- Access a link to the program on a Web site by using TS Web Access.
- Double-click a Remote Desktop Protocol (.rdp) file that has been created and distributed by their administrator.
- Double-click a program icon on their desktop or **Start** menu that has been created and distributed by their administrator with a Windows Installer (.msi) package.
- Double-click a file where the file name extension is associated with a RemoteApp program. This can be configured by their administrator with a Windows Installer package.

The .rdp files and Windows Installer packages contain the settings that are needed to run RemoteApp programs. After opening a RemoteApp program on their local computer, the user can interact with the program that is running on the terminal server as if it were running locally.

Client requirements

To access RemoteApp programs that are deployed as .rdp files or as Windows Installer packages, the client computer must be running Remote Desktop Connection (RDC) 6.0 or RDC 6.1. A supported version of the RDC client is included with Windows Server 2008 and Windows Vista®. To download RDC 6.0 for Windows Server 2003 with Service Pack 1 (SP1) or Windows XP with Service Pack 2 (SP2), see article 925876 in the Microsoft® Knowledge Base (<http://go.microsoft.com/fwlink/?LinkId=79373> [<http://go.microsoft.com/fwlink/?LinkId=79373>]).

 **Note:**

RDC 6.1 (6.0.6001) supports Remote Desktop Protocol 6.1.

To access RemoteApp programs through TS Web Access, the client computer must be running RDC 6.1. RDC 6.1 is included with the following operating systems:

- Windows Server 2008
- Windows Vista with Service Pack 1 (SP1)
- Windows XP with Service Pack 3 (SP3) Beta and Windows XP with SP3 Release Candidate (RC)

Who should use TS RemoteApp?

This guide is intended for the following audiences:

- IT planners and analysts who are evaluating the product
- Enterprise architects
- IT professionals who deploy or administer terminal servers, line-of-business (LOB) applications, or applications that can be more efficiently deployed with TS RemoteApp

Key scenarios for TS RemoteApp

TS RemoteApp is especially useful in scenarios such as the following:

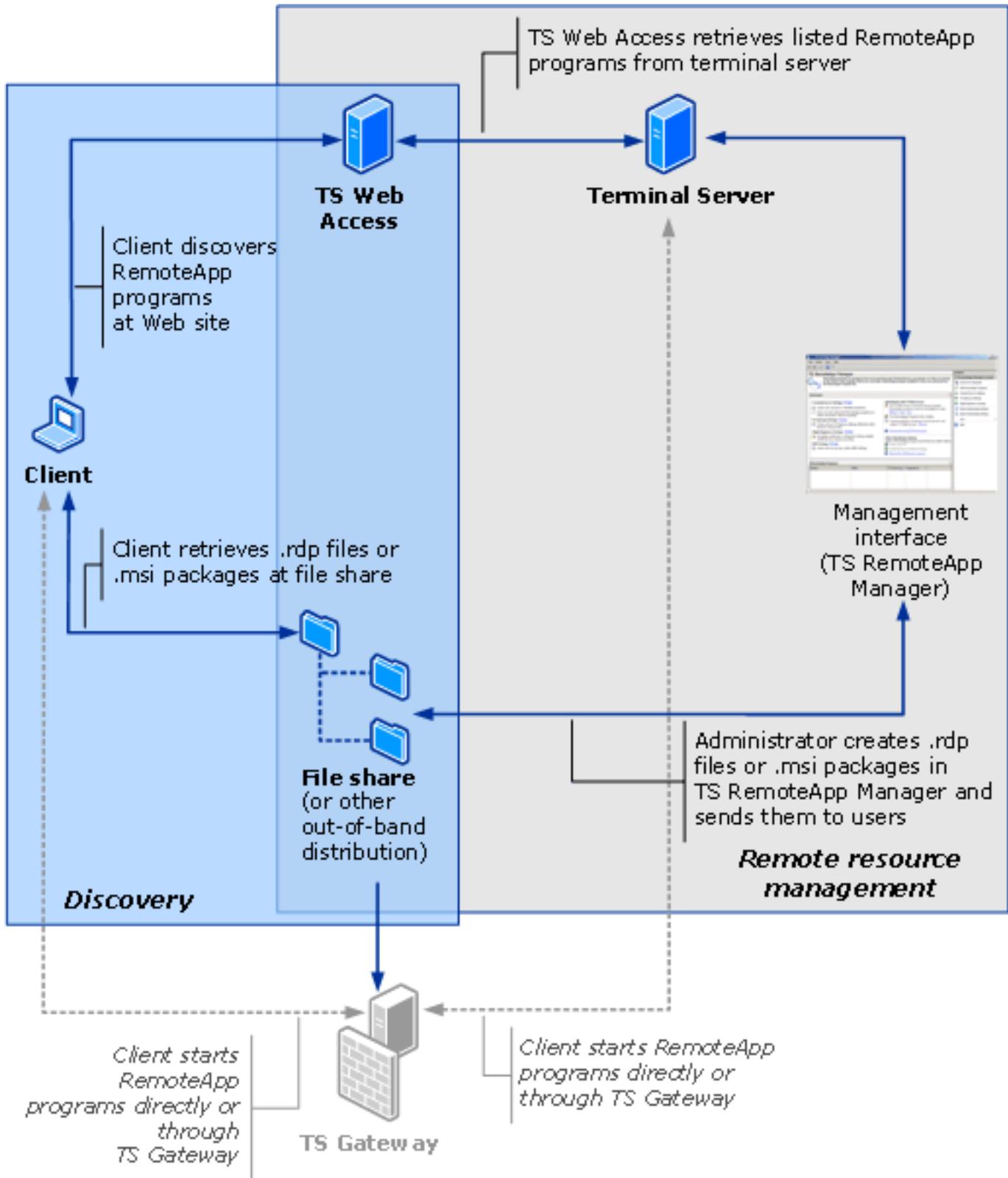
- Remote users. Users often need to access programs from remote locations, such as while working from home or while traveling. If you want users to access RemoteApp programs over an Internet connection, you can allow access through a Virtual Private Network (VPN), or you can deploy TS RemoteApp together with Terminal Services Gateway (TS Gateway) to help secure remote access to the programs.
- Branch offices. In a branch office environment, there may be limited local IT support and limited network bandwidth. By using TS RemoteApp, you can centralize the management of your applications and improve remote program performance in limited bandwidth scenarios.

- Line-of-business (LOB) applications deployment. Companies often need to run consistent LOB applications on computers that are running different Windows versions and configurations. Instead of deploying the LOB applications to all the computers in the company, which can be expensive in terms of time and cost, you can install the LOB applications on a terminal server and make them available through TS RemoteApp.
- Application deployment. With TS RemoteApp you do not have to deploy and maintain different versions of the same program for individual computers. If employees need to use multiple versions of a program, you can install those versions on one or more terminal servers, and users can access them through TS RemoteApp.
- Roaming users. In a company with a flexible desk policy, users can work from different computers. In some cases, the computer where a user is working may not have the necessary programs installed locally. By using TS RemoteApp, you can install the programs on a terminal server and make them available to users as if those programs were installed locally.

How should I deploy RemoteApp programs?

Before you configure TS RemoteApp, you should decide how you want to distribute RemoteApp programs to users. You can use either of the following deployment methods:

- You can make RemoteApp programs available on a Web site by distributing the RemoteApp programs through TS Web Access.
- You can distribute RemoteApp programs as .rdp files or Windows Installer packages through a file share, or through other distribution mechanisms such as Microsoft Systems Management Server or Active Directory software distribution.



RemoteApp deployment components

About deploying RemoteApp programs through TS Web Access

If you use TS Web Access, you can deploy RemoteApp programs from a single terminal server or farm, or a link to the full terminal server desktop, directly through TS Web Access. All RemoteApp programs on the terminal server or farm that are configured for TS Web Access will appear on the TS Web Access Web site.

 **Note:**

Additionally, TS Web Access includes the Remote Desktop Web Connection feature, which allows users to connect from a Web browser to the remote desktop of any server or client computer where they have Remote Desktop access. You can determine whether you want this feature to be available to users. For more information, see [Configure Remote Desktop Web Connection Behavior](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_RemoteDesktopWeb) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_RemoteDesktopWeb] .

To deploy RemoteApp programs by using TS Web Access, you must complete the following tasks.

Task	Reference
1. Configure the server that will host RemoteApp programs. This includes installing Terminal Server, installing programs, and verifying remote connection settings.	Configure the server that will host RemoteApp programs [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ConfigureHostServer]
2. Use TS RemoteApp Manager to add RemoteApp programs that are enabled for TS Web Access, and to configure global deployment settings.	Add RemoteApp programs and configure global deployment settings [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_AddPrograms]
3. Install TS Web Access on the server that you want users to connect to over the Web to access RemoteApp programs.	Install the TS Web Access role service [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_InstallTSWebAccess]
4. Add the computer account of the TS Web Access server to the TS Web Access Computers group on the terminal server.	Populate the TS Web Access Computers security group [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_PopulateGroup]
5. Configure the TS Web Access server to populate its list of RemoteApp programs from a single terminal server or single farm.	Configure the data source for TS Web Access [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ConfigDataSource]

[↑Top of page](#)

About deploying RemoteApp programs through a file share or other distribution mechanism

You can also deploy RemoteApp programs through .rdp files or Windows Installer packages that are made available through file sharing, or through other distribution mechanisms such as Microsoft Systems Management Server or Active Directory software distribution. These methods enable you to distribute RemoteApp programs to

users without using TS Web Access.

 **Note:**

If you distribute RemoteApp programs through Windows Installer packages, you can also configure whether the terminal server will take over client file name extensions for the RemoteApp programs. If this is the case, a user can double-click a file where the file name extension is associated with a RemoteApp program.

You must complete the following tasks to prepare RemoteApp programs for distribution through a file share or some other distribution mechanism.

Task	Reference
1. Configure the server that will host RemoteApp programs. This includes installing Terminal Server, installing programs, and verifying remote connection settings.	Configure the server that will host RemoteApp programs [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_ConfigureHostServer]
2. Use TS RemoteApp Manager to add RemoteApp programs and to configure global deployment settings.	Add RemoteApp programs and configure global deployment settings [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_AddPrograms]
3. Use TS RemoteApp Manager to create .rdp files or Windows Installer packages from RemoteApp programs.	<ul style="list-style-type: none"> • Create an .rdp file from a RemoteApp program [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_CreateRDP] • Create a Windows Installer package from a RemoteApp program [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_CreateMSI]

After you create .rdp files or Windows Installer packages, you can distribute them to users.

Configure the server that will host RemoteApp programs

Before you can deploy RemoteApp programs to users, you must configure the server to host RemoteApp programs. The following procedures are covered:

- [Install the Terminal Server role service](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_InstallTerminalServerRole) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_InstallTerminalServerRole]
- [Install programs on the terminal server](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_InstallApps) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_InstallApps]
- [Verify remote connection settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_EnableRemoteConnections) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_EnableRemoteConnections]

 **Note:**

These procedures apply to an environment where you are using a single terminal server to host RemoteApp programs.

To perform these procedures, you must be a member of the Administrators group on the terminal server.

Install the Terminal Server role service

To install the Terminal Server role service

1. Open Server Manager. To open Server Manager, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. Under **Roles Summary**, click **Add Roles**.
3. On the **Before You Begin** page of the Add Roles Wizard, click **Next**.
4. On the **Select Server Roles** page, select the **Terminal Services** check box, and then click **Next**.
5. On the **Terminal Services** page, click **Next**.
6. On the **Select Role Services** page, select the **Terminal Server** check box, and then click **Next**.
7. On the **Uninstall and Reinstall Applications for Compatibility** page, review the information, and then click **Next**.
8. On the **Specify Authentication Method for Terminal Server** page, select the desired authentication method, and then click **Next**.
9. On the **Specify Licensing Mode** page, select the licensing mode that applies to your Terminal Services environment, and then click **Next**.
10. On the **Select User Groups Allowed Access To This Terminal Server** page, add any users or groups that you want to add to the Remote Desktop Users group, and then click **Next**.
11. On the **Confirm Installation Selections** page, verify that the Terminal Server role service will be installed, and then click **Install**.
12. On the **Installation Results** page, you are prompted to restart the server to finish the installation process. Click **Close**, and then click **Yes** to restart the server.

13. After the server restarts, the Resume Configuration Wizard completes the installation. When you see an **Installation succeeded** status message on the **Installation Results** page, click **Close**.

[⤴Top of page](#)

Install programs on the terminal server

We recommend that you install programs on the terminal server after you have installed the Terminal Server role service. If you install a program from a Windows Installer package, the program will automatically install in Terminal Server Install mode. If you are installing from another kind of Setup package, use either of the following methods to put the server into Install mode:

- Use the **Install Application on Terminal Server** option in Control Panel to install the program.
- Before you install a program, run the **change user /install** command from the command line. After the program is installed, run the **change user /execute** command to exit from Install mode.

If you have programs that are related to each other or have dependencies on each other, we recommend that you install the programs on the same terminal server. For example, we recommend that you install Microsoft Office as a suite instead of installing individual Office programs on separate terminal servers.

You should consider putting individual programs on separate terminal servers in the following circumstances:

- The program has compatibility issues that may affect other programs.
- A single program and the number of associated users may fill server capacity.

[⤴Top of page](#)

Verify remote connection settings

By default, remote connections are enabled after you install the Terminal Server role service. You can use the following procedure to add users and groups that need to connect to the terminal server, and to verify or to change remote connection settings.

To verify remote connection settings

1. Start the System tool. To do this, click **Start**, click **Run**, type **control system** in the **Open** box, and then click **OK**.
2. Under **Tasks**, click **Remote settings**.
3. In the **System Properties** dialog box, on the **Remote** tab, ensure that the Remote Desktop connection setting is configured correctly, depending on your environment. You can select either of the following options:
 - **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)**

For more information about the two options, on the **Remote** tab, click the **Help me choose** link.

4. To add the users and groups that need to connect to the terminal server by using Remote Desktop, click **Select Users**, and then click **Add**.

The users and groups that you add are added to the Remote Desktop Users group.



Note:

Members of the local Administrators group can connect even if they are not listed.

5. When you are finished, click **OK** to close the **System Properties** dialog box.

[⬆️Top of page](#)

[⬆️Top of page](#)

Add RemoteApp programs and configure global deployment settings

After you have prepared the terminal server to host RemoteApp programs, you can use TS RemoteApp Manager to do the following:

- [Add programs to the RemoteApp Programs list](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_AddAllowList) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_AddAllowList]

- [Configure global deployment settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ConfigureGlobalSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ConfigureGlobalSettings]

In TS RemoteApp Manager, you can also delete, modify, import RemoteApp programs and settings from another terminal server, or export RemoteApp programs and settings to another terminal server. For more information, see [Manage RemoteApp programs and settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ManageAllow) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ManageAllow] .

Add programs to the RemoteApp Programs list

To make a RemoteApp program available to users through any distribution mechanism, you must add the program to the **RemoteApp Programs** list. By default, programs that you add to the list are configured to be available through TS Web Access.

To add a program to the RemoteApp Programs list

1. Start TS RemoteApp Manager. To do this, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS RemoteApp Manager**.
2. In the **Actions** pane, click **Add RemoteApp Programs**.
3. On the **Welcome to the RemoteApp Wizard** page, click **Next**.
4. On the **Choose programs to add to the RemoteApp Programs list** page, select the check box next to each program that you want to add to the **RemoteApp Programs** list. You can select multiple programs.

Note:

The programs that are shown on the **Choose programs to add to the RemoteApp Programs list** page are the programs that are found on the All Users **Start** menu on the terminal server. If the program that you want to add to the **RemoteApp Programs** list is not in the list, click **Browse**, and then specify the location of the program's .exe file.

5. To configure the properties for a RemoteApp program, click the program name, and then click **Properties**. You can configure the following:
 - The program name that will appear to users. To change the name, type a new name in the **RemoteApp program name** box.

- The path of the program executable file. To change the path, type the new path in the **Location** box, or click **Browse** to locate the .exe file.

**Note:**

You can use system environment variables in the path name. For example, you can substitute %windir% for the explicit path of the Windows folder (such as C:\Windows). You cannot use per user environment variables.

- The alias for the RemoteApp program. The alias is a unique identifier for the program that defaults to the program's file name (without the extension). We recommend that you do not change this name.
 - Whether the RemoteApp program is available through TS Web Access. By default, the **RemoteApp program is available through TS Web Access** setting is enabled. To change the setting, select or clear the check box.
 - Whether command-line arguments are allowed, not allowed, or whether to always use the same command-line arguments.
 - The program icon that will be used. To change the icon, click **Change Icon**.
6. When you are finished configuring program properties, click **OK**, and then click **Next**.
 7. On the **Review Settings** page, review the settings, and then click **Finish**.

The programs that you selected should appear in the **RemoteApp Programs** list.

[↑Top of page](#)

Configure global deployment settings

You can configure global deployment settings that apply to all RemoteApp programs in the **RemoteApp Programs** list. These settings will apply to any RemoteApp program that you make available through TS Web Access. Additionally, these settings will be used as the default settings if you create .rdp files or Windows Installer packages from any of the listed RemoteApp programs.

**Note:**

Any changes to deployment settings that you make when you use TS RemoteApp Manager to create .rdp files or Windows Installer packages will override the global settings.

These global deployment settings include:

- [Terminal server settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TerminalServerSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TerminalServerSettings]

- [TS Gateway settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TSGatewaySettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TSGatewaySettings]
- [Common Remote Desktop Protocol \(RDP\) settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_CommonRDPSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_CommonRDPSettings]
- [Custom RDP settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_CustomRDPSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_CustomRDPSettings]
- [Digital signature settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_DigitalSigSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_DigitalSigSettings]

Configure terminal server settings

To define how users will connect to the terminal server (or terminal server farm) to access RemoteApp programs, you can configure terminal server deployment settings.

To configure terminal server settings

1. In the **Actions** pane of TS RemoteApp Manager, click **Terminal Server Settings**. (Or, in the **Overview** pane, next to **Terminal Server Settings**, click **Change**.)
2. On the **Terminal Server** tab, under **Connection settings**, accept or modify the server or farm name, the RDP port number, and server authentication settings.

Important:

If the **Require server authentication** check box is selected, consider the following:

- If any client computers are running Windows Server 2003 with SP1 or Windows XP with SP2, you must configure the terminal server to use a Secure Sockets Layer (SSL) certificate. (You cannot use a self-signed certificate.)
 - If the RemoteApp program is for intranet use, and all client computers are running either Windows Server 2008 or Windows Vista, you do not have to configure the terminal server to use an SSL certificate. In this case, Network Level Authentication is used.
3. To provide a link to the full terminal server desktop through TS Web Access, under **Remote desktop access**, select the **Show a remote desktop connection to this terminal server in TS Web Access** check box.

4. Under **Access to unlisted programs**, choose either of the following:

- **Do not allow users to start unlisted program on initial connection (Recommended)**

To help protect against malicious users, or a user unintentionally starting a program from an .rdp file on initial connection, we recommended that you select this setting.

 **Important:**

This setting does not prevent users from starting unlisted programs remotely after they connect to the terminal server by using the RemoteApp program. For example, if Microsoft Word is in the **RemoteApp Programs** list and Microsoft Internet Explorer is not, if a user starts a remote Word session, and then clicks a hyperlink in a Word document, they can start Internet Explorer.

- **Allow users to start both listed and unlisted programs on initial connection**

 **Caution:**

If you choose this option, users can start any program remotely from an .rdp file on initial connection, not just those programs in the **RemoteApp Programs** list. To help protect against malicious users, or a user unintentionally starting a program from an .rdp file, we recommend that you do not select this setting.

5. When you are finished, click **OK**.

[↑Top of page](#)

Configure TS Gateway settings

To define whether users will connect to the terminal server across a firewall through TS Gateway, you can configure TS Gateway deployment settings. For more information about TS Gateway, see the TS Gateway Step-by-Step Guide (<http://go.microsoft.com/fwlink/?LinkId=85872> [http://go.microsoft.com/fwlink/?LinkId=85872]).

To configure TS Gateway settings

1. In the **Actions** pane of TS RemoteApp Manager, click **TS Gateway Settings**. (Or, in the **Overview** pane, next to **TS Gateway Settings**, click **Change**.)
2. On the **TS Gateway** tab, configure the desired TS Gateway behavior. You can configure whether to automatically detect TS Gateway server settings, to use TS Gateway server settings that you specify, or to not use a TS Gateway server.

If you select **Automatically detect TS Gateway server settings**, the client tries to use Group Policy settings to determine the behavior of client connections to TS Gateway.

 **Note:**

For more information about client Group Policy settings, see the Help topic "Using Group Policy to Manage Client Connections Through TS Gateway." (To open TS Gateway Help on a Windows Server 2008-based server, click **Start**, click **Run**, type **hh ts_gateway.chm**, and then click **OK**.)

If you select **Use these TS Gateway server settings**, do the following:

1. Configure the TS Gateway server name and the logon method.

 **Important:**

The server name must match what is specified in the SSL certificate for the TS Gateway server.

2. If you want the connection to try to use the same user credentials to access both the TS Gateway server and the terminal server, select the **Use the same user credentials for TS Gateway and terminal server** check box. However, users may still receive two prompts for credentials if conflicting credentials exist from any source such as Group Policy settings, and those credentials do not work. They may also receive two prompts for credentials if default credentials are used for the connection and those credentials do not work.
3. If you want the client computer to automatically detect when TS Gateway is required, select the **Bypass TS Gateway server for local addresses** check box. (Selecting this option optimizes client performance.)

To always use a TS Gateway server for client connections, clear the **Bypass TS Gateway server for local addresses** check box.

3. When you are finished, click **OK**.

[↑Top of page](#)

Configure common RDP settings (optional)

You can specify common Remote Desktop Protocol (RDP) settings for RemoteApp connections, such as device and resource redirection, and some user display settings. These settings will apply when a user connects to a

RemoteApp program through TS Web Access, or when you create an .rdp file or a Windows Installer package from an existing RemoteApp program.

To configure common RDP settings

1. In the **Overview** pane of TS RemoteApp Manager, next to **RDP Settings**, click **Change**.
2. Under **Devices and resources**, configure which devices and resources on the client computer you want to make available in the remote session.
3. Under **User experience**, choose whether to enable font smoothing and the desired color depth.
4. When you are finished, click **Apply**.

 **Note:**

To configure additional RDP settings, such as audio redirection, click the **Custom RDP Settings** tab. For more information, see [Configure Custom RDP Settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_CustomRDPSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_CustomRDPSettings] .

5. To close the **RemoteApp Deployment Settings** dialog box, click **OK**.

 **Note:**

If you do not sign .rdp files with a digital signature, or if you sign .rdp files with a digital signature that clients do not recognize (such as a certificate from a private certification authority), some redirection settings that you specify in TS RemoteApp Manager may be overridden by the client. For example, if you enable all redirection settings on the **Common RDP Settings** tab, and a user connects to an .rdp file that is not signed, disk drives, and supported Plug and Play devices will not be redirected automatically. These devices and resources will only be redirected if the user enables these redirection settings in the **RemoteApp** warning dialog box that appears when they try to connect. This default behavior helps to reduce potential security vulnerabilities. (Note that the same behavior occurs if you enable serial port redirection on the **Custom RDP Settings** tab.)

[⤴Top of page](#)

Configure custom RDP settings (optional)

You can specify custom RDP settings for RemoteApp connections, such as audio redirection. These settings will apply when a user connects to a RemoteApp program through TS Web Access, or when you create a Windows Installer package or .rdp file from an existing RemoteApp program.

 **Note:**

You can use custom RDP settings to configure the working directory for RemoteApp programs. By default, the working directory for a RemoteApp program is the same location as the program executable file. If you configure the working directory as a custom RDP setting, the setting will apply to all RemoteApp programs that are available through TS Web Access, and to any .rdp files or Windows Installer packages that you create from a RemoteApp program. If you want to customize the working directory for RemoteApp programs that you plan to distribute as .rdp files or Windows Installer packages, you can add the working directory as a custom RDP setting, create the files from the RemoteApp programs, and then clear the working directory custom RDP setting.

To specify custom RDP settings

1. In the **Overview** pane of TS RemoteApp Manager, next to **RDP Settings**, click **Change**.
2. On the **Custom RDP Settings** tab, type or copy the custom RDP settings that you want to use into the **Custom RDP settings** box.

To copy settings from an existing .rdp file, open the file in a text editor such as Notepad, and then copy the desired settings.

Important:

You cannot override settings that are available in the global deployment settings in TS RemoteApp Manager. If you do so, you will be prompted to remove those settings when you click **Apply**.

To create an .rdp file to copy the settings from, follow these steps:

1. Open the RDC client, and then click **Options**.
2. Configure the settings that you want, such as audio redirection.
3. When you are finished, on the **General** tab, click **Save As**, and then save the .rdp file.
4. Open the .rdp file in Notepad, and then copy the desired settings into the **Custom RDP settings** box on the **Custom RDP Settings** tab.
3. When you have finished adding the settings that you want, click **Apply**.
4. If the **Error with Custom RDP Settings** dialog box appears, do the following:
 1. Click **Remove** to automatically remove the settings that are either not valid or cannot be overridden, or click **OK** to remove the settings manually.
 2. After the settings are removed, click **Apply** again.
5. To close the **RemoteApp Deployment Settings** dialog box, click **OK**.

[↑Top of page](#)

Configure digital signature settings (optional)

You can use a digital signature to sign .rdp files that are used for RemoteApp connections to the terminal server. This includes the .rdp files that are used for connections through TS Web Access to RemoteApp programs on the terminal server and to the terminal server desktop.

Important:

To connect to a RemoteApp program by using a digitally signed .rdp file, the client must be running RDC 6.1. (The RDC 6.1 [6.0.6001] client supports Remote Desktop Protocol 6.1.)

If you use a digital certificate, the cryptographic signature on the connection file provides verifiable information about your identity as its publisher. This enables clients to recognize your organization as the source of the RemoteApp program or the remote desktop connection, and allows them to make more informed trust decisions about whether to start the connection. This helps protect against the use of .rdp files that were altered by a malicious user.

You can sign .rdp files that are used for RemoteApp connections by using a Server Authentication certificate (SSL certificate) or a Code Signing certificate. You can obtain SSL and Code Signing certificates from public certification authorities (CAs), or from an enterprise CA in your public key infrastructure hierarchy.

If you are already using an SSL certificate for terminal server or TS Gateway connections, you can use the same certificate to sign .rdp files. However, if users will connect to RemoteApp programs from public or home computers, you must use either of the following:

- A certificate from a public certification authority (CA) that participates in the Microsoft Root Certificate Program Members program (<http://go.microsoft.com/fwlink/?LinkID=59547> [http://go.microsoft.com/fwlink/?LinkID=59547]).
- If you are using an enterprise CA, your enterprise CA-issued certificate must be co-signed by a public CA that participates in the Microsoft Root Certification Program Members program.

To configure the digital certificate to use

1. In the **Actions** pane of TS RemoteApp Manager, click **Digital Signature Settings**. (Or, in the **Overview** pane, next to **Digital Signature Settings**, click **Change**.)
2. Select the **Sign with a digital certificate** check box.
3. In the **Digital certificate details** box, click **Change**.
4. In the **Select Certificate** dialog box, select the certificate that you want to use, and then click **OK**.



Note:

The **Select Certificate** dialog box is populated by certificates that are located in the local computer's certificates store or in your personal certificate store. The certificate that you want to use must be located in one of these stores.

Group Policy settings to control client behavior when opening a digitally signed .rdp file

You can use Group Policy to configure clients to always recognize RemoteApp programs from a particular publisher as trusted. You can also configure whether clients will block RemoteApp programs and remote desktop connections from external or unknown sources. By using these policy settings, you can reduce the number and complexity of security decisions that users face. This reduces the chances of inadvertent user actions that may lead to security vulnerabilities.

The relevant Group Policy settings are located in the Local Group Policy Editor at the following location, in both the Computer Configuration and in the User Configuration node:

Administrative Templates\Windows Components\Terminal Services\Remote Desktop Connection Client

The available policy settings are:

- Specify SHA1 thumbprints of certificates representing trusted .rdp publishers

This policy setting allows you to specify a list of Secure Hash Algorithm 1 (SHA1) certificate thumbprints that represent trusted .rdp file publishers. If you enable this policy setting, any certificate with an SHA1 thumbprint that matches a thumbprint on the list will be considered trusted.

- Allow .rdp files from valid publishers and user's default .rdp settings

This policy setting allows you to specify whether users can run .rdp files from a publisher that signed the file with a valid certificate. This policy setting also controls whether the user can start an RDP session by using default .rdp settings, such as when a user directly opens the RDC client without specifying an .rdp file.

- Allow .rdp files from unknown publishers

This policy setting allows you to specify whether users can run unsigned .rdp files and .rdp files from unknown publishers on the client computer.

Important:

To use these Group Policy settings, the client computer must be running RDC 6.1.

For more information about these policy settings, view the Group Policy Explain text in the Local Group Policy Editor.

[Top of page](#)

[Top of page](#)

Manage RemoteApp programs and settings

In TS RemoteApp Manager, you can make changes to an existing RemoteApp program, or you can remove the program from the list. Additionally, you can export or import the **RemoteApp Programs** list and the global deployment settings to or from another terminal server.

- [Change or delete a RemoteApp program](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ChangeDeleteRP) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ChangeDeleteRP]
- [Export or import RemoteApp programs and settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ExportImportAllow) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_ExportImportAllow]

Change or delete a RemoteApp program

After you have added a program to the **RemoteApp Programs** list, you can change the deployment settings for all RemoteApp programs, change the properties of a single RemoteApp program, or delete the RemoteApp program from the list.

- To change deployment settings for all RemoteApp programs, in the **Actions** pane of TS RemoteApp Manager, click **Terminal Server Settings**, **TS Gateway Settings**, or **Digital Signature Settings**. (Or, click one of the **Change** options in the **Overview** pane. You can also change custom RDP settings in the **Overview** pane.)

Important:

If you make any changes, the changes will not affect .rdp files or Windows Installer packages that you already created by using TS RemoteApp Manager.

- To change the properties of a single RemoteApp program, click the program in the **RemoteApp Programs** list, and then in the **Actions** pane for the program, click **Properties**.

Note:

You cannot change the properties of an existing .rdp file or Windows Installer package by using TS RemoteApp Manager. Instead, you must click **Create .rdp File** or **Create Windows Installer Package** in the **Actions** pane to create a new .rdp file or Windows Installer package that has the desired properties.

- To change whether the RemoteApp program will be available from TS Web Access, click the program, and then click **Show in TS Web Access** or **Hide in TS Web Access** in the **Actions** pane.
- To delete a program in the **RemoteApp Programs** list, click the RemoteApp program, and then in the **Actions** pane for the program, click **Remove**. Click **Yes** to confirm the deletion.

 **Note:**

When you delete a program in the **RemoteApp Programs** list, any .rdp files or Windows Installer packages that you created from the RemoteApp program are not deleted.

[↑Top of page](#)

Export or import RemoteApp programs and settings

You can copy the **RemoteApp Programs** list and deployment settings from one terminal server to another terminal server. You might want to do this if you want to configure multiple terminal servers identically to host RemoteApp programs, such as in a terminal server farm.

To export the RemoteApp Programs list and deployment settings

1. Start TS RemoteApp Manager.
2. In the **Actions** pane, click **Export RemoteApp Settings**.
3. Select either of the following options:
 - **Export the RemoteApp Programs list and settings to another terminal server**

If you select this option, in the **Terminal server name** box, enter the name of the terminal server that you want to export the settings to, and then click **OK**. (For the export operation to succeed, the source terminal server must have Windows Management Instrumentation (WMI) access to the target terminal server.)

 **Important:**

When you click **OK**, the **RemoteApp Programs** list and deployment settings will be automatically overwritten on the target terminal server.

- **Export the RemoteApp Programs list and settings to a file**

If you select this option, click **OK**. In the **Save As** dialog box, specify a location to save the .tspub file, and then click **Save**.

To import the RemoteApp Programs list and deployment settings

1. Start TS RemoteApp Manager.
2. In the **Actions** pane, click **Import RemoteApp Settings**.
3. Select either of the following options:
 - **Import the RemoteApp Programs list and settings from another terminal server**

If you select this option, in the **Terminal server name** box, enter the name of the terminal server that you want to import the settings from, and then click **OK**. The settings are imported directly into TS RemoteApp Manager. (For the import operation to succeed, the source terminal server must have WMI access to the target terminal server.)

- **Import the RemoteApp Programs list and settings from a file**

If you select this option, click **OK**. In the **Open** dialog box, locate and then click the .tspub file that you want to import, and then click **Open**.

If you import a configuration, and the target terminal server does not have a program in the **RemoteApp Programs** list installed or the program is installed in a different folder, the program will appear in the **RemoteApp Programs** list. However, the name will be displayed with strikethrough text.

Note:

Only the **RemoteApp Programs** list and deployment settings are exported or imported. Any .rdp files or Windows Installer packages that were created from the programs will not be exported or imported. You must create new .rdp files or Windows Installer packages on each terminal server unless the server is a member of a terminal server farm. If you specified a farm name when you created the .rdp files or Windows Installer packages, and the server where you want to copy the files to is a member of the same terminal server farm, you can manually copy the files.

[⤴Top of page](#)

[⤴Top of page](#)

[⤴Top of page](#)

Deploy RemoteApp programs to users

The following section includes instructions about how to deploy RemoteApp programs to users through TS Web Access or through a file share or other distribution mechanism.

Deploy RemoteApp programs through TS Web Access

With TS Web Access, users can access RemoteApp programs from a Web site over the Internet or from an intranet. To start a RemoteApp program, they just click the program icon. TS Web Access provides a solution that works with minimal configuration. The default TS Web Access Web page includes a customizable Web Part, which can be incorporated into a customized Web page.

Note:

For information about client requirements, see [Client requirements and configuration](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.aspx#BKMK_TSWAClientRequirements) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.aspx#BKMK_TSWAClientRequirements] .

To use TS Web Access to deploy RemoteApp programs, you must do the following:

1. Install the TS Web Access role service.
2. Populate the TS Web Access Computers security group.
3. Specify the terminal server from which to populate the list of RemoteApp programs that will appear in the TS Web Access Web Part.

Install the TS Web Access role service

You must install the TS Web Access role service on the server that you want users to connect to over the Web to access RemoteApp programs. When you install the TS Web Access role service, Microsoft Internet Information Services (IIS) 7.0 is also installed.

The server where you install TS Web Access acts as the Web server. The server does not have to be a terminal server.

Note:

By default, when you install TS Web Access, the TS Web Access Web site installs to the Default Web Site in IIS. To change the default install location of the site, you can configure a different location in the registry. You must do this before you install the TS Web Access role service. For more information, see the [Change the install location of the default TS Web Access Web site](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.aspx#BKMK_DefaultInstallLocation) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.aspx#BKMK_DefaultInstallLocation] section later in this guide.

Membership in the local Administrators group is the minimum required to complete this procedure.

To install TS Web Access

1. Open Server Manager. To open Server Manager, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
2. If the Terminal Services role is already installed:
 1. Under **Roles Summary**, click **Terminal Services**.
 2. Under **Role Services**, click **Add Role Services**.
 3. On the **Select Role Services** page, select the **TS Web Access** check box.

If the Terminal Services role is not already installed:

1. Under **Roles Summary**, click **Add Roles**.
 2. On the **Before You Begin** page, click **Next**.
 3. On the **Select Server Roles** page, select the **Terminal Services** check box, and then click **Next**.
 4. Review the **Terminal Services** page, and then click **Next**.
 5. On the **Select Role Services** page, select the **TS Web Access** check box.
3. Review the information about the required role services, and then click **Add Required Role Services**.
 4. Click **Next**.
 5. Review the **Web Server (IIS)** page, and then click **Next**.
 6. On the **Select Role Services** page, where you are prompted to select the role services that you want to install for IIS, click **Next**.
 7. On the **Confirm Installation Selections** page, click **Install**.
 8. On the **Installation Results** page, confirm that the installation succeeded, and then click **Close**.

[⤴ Top of page](#)

Populate the TS Web Access Computers security group

If the TS Web Access server and the terminal server that hosts the RemoteApp programs are separate servers, you must add the computer account of the TS Web Access server to the TS Web Access Computers security group on the terminal server.

To add the computer account of the TS Web Access server to the security group

1. On the terminal server, click **Start**, point to **Administrative Tools**, and then click **Computer Management**.
2. In the left pane, expand **Local Users and Groups**, and then click **Groups**.
3. In the right pane, double-click **TS Web Access Computers**.
4. In the **TS Web Access Computers Properties** dialog box, click **Add**.
5. In the **Select Users, Computers, or Groups** dialog box, click **Object Types**.
6. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
7. In the **Enter the object names to select** box, specify the computer account of the TS Web Access server, and then click **OK**.
8. Click **OK** to close the **TS Web Access Computers Properties** dialog box.

[⤴Top of page](#)

Configure the data source for TS Web Access

You can configure TS Web Access to populate the list of RemoteApp programs that appear in the Web Part from a specific terminal server or terminal server farm.

Specify the data source for TS Web Access

By default, TS Web Access populates its list of RemoteApp programs from a single terminal server, and points to the local host. The Web Part is populated by all RemoteApp programs that are enabled for TS Web Access on that terminal server's **RemoteApp Programs** list.

To complete this procedure, you must log on to the TS Web Access server by using the local Administrator account or an account that is a member of the TS Web Access Administrators group on the TS Web Access server.

To specify which terminal server to use as the data source

1. Connect to the TS Web Access Web site. To do this, use either of the following methods:
 - On the TS Web Access server, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS Web Access Administration**.
 - Use Internet Explorer to connect to the TS Web Access Web site. By default, the Web site is located at the following address, where *server_name* is the name of the TS Web Access server:

`http://server_name/ts`

2. Log on to the site by using either the local Administrator account, or an account that is a member of the local TS Web Access Administrators group. (If you are already logged on to the computer as one of these accounts, you are not prompted for credentials.)
3. On the title bar, click the **Configuration** tab.

 **Note:**

If you access the TS Web Access Web site by using the TS Web Access Administration option, the page automatically opens to the **Configuration** tab.

4. In the **Editor Zone** area, in the **Terminal server name** box, enter the name of the terminal server that you want to use as the data source.
5. Click **Apply** to apply the changes.

To test TS Web Access, see [Connect to TS Web Access](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_ConnectTSWA) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_ConnectTSWA] .

[⬆️Top of page](#)

[⬆️Top of page](#)

Connect to TS Web Access

By default, you can access the TS Web Access Web site at the following location, where *server_name* is the NetBIOS name or the fully qualified domain name of the Web server where you installed TS Web Access:

`http://server_name/ts`

If you connect to TS Web Access from a public computer, such as a computer in an "Internet café," you should clear the **I am using a private computer that complies with my organization's security policy** check box that appears in the lower-right corner of the Web Part. In public mode, you are not provided with the option to

save your credentials, and the caching of bitmaps is not enabled.

Client requirements and configuration

To connect to TS Web Access, the client computer must be running RDC 6.1. RDC 6.1 is included with the following operating systems:

- Windows Server 2008
- Windows Vista with SP1
- Windows XP with SP3 Beta or Windows XP with SP3 RC

Additionally, the Terminal Services ActiveX Client control must be enabled. The ActiveX control is included with RDC 6.1.

If you are running Windows Server 2008 or Windows Vista with SP1, and you receive a warning message on the Internet Explorer Information bar about the site being restricted from showing certain content, click the message line, point to **Add-on Disabled**, and then click **Run ActiveX Control**. When you do this, you may see a security warning. Make sure that the publisher for the ActiveX control is "Microsoft Corporation" before you click **Run**.

Note:

If the Internet Explorer Information bar does not appear, and you cannot connect to TS Web Access, you can enable the Terminal Services ActiveX control by using the **Manage Add-ons** tool on the **Tools** menu of Internet Explorer. The add-on appears as **Microsoft Terminal Services Client Control**.

If you are running Windows XP with SP3 RC, you must modify the registry to enable the ActiveX control. To do this, follow these steps:

Caution:

Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

To enable the ActiveX control in Windows XP with SP3 RC by modifying the registry

1. Start Registry Editor. To do this, click **Start**, click **Run**, type **regedit** in the **Open** box, and then click **OK**.
2. Locate the following registry subkey:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Settings

3. In case you need to restore, we recommend that you back up the **Settings** subkey. To do this, right-click **Settings**, click **Export**, type a file name in the **File name** box, and then click **Save**.
4. Under the **Settings** subkey, delete the following subkeys. (To delete a subkey, right-click the subkey, click **Delete**, and then click **Yes** to confirm.)
 - **{4eb89ff4-7f78-4a0f-8b8d-2bf02e94e4b2}**
 - **{7390f3d8-0439-4c05-91e3-cf5cb290c3d0}**
5. Close Registry Editor.
6. Refresh the TS Web Access Web page.

The TS Web Access Web page should display correctly.



Note:

Depending on your Internet Explorer security settings, you may receive a warning message on the Internet Explorer Information bar that asks if you want to allow the add-on to run. If you receive the message, click the message line, and then click **Run ActiveX Control**. When you do this, you may see a security warning. Make sure that the publisher for the ActiveX control is "Microsoft Corporation" before you click **Run**.

[↑Top of page](#)

[↑Top of page](#)

[↑Top of page](#)

Deploy RemoteApp programs through file sharing or other distribution methods

You can deploy RemoteApp programs to users by making .rdp files or Windows Installer packages available from a file share or through other distribution mechanisms. You can use TS RemoteApp Manager to create the .rdp files or Windows Installer packages from RemoteApp programs that are in the **RemoteApp Programs** list.

Create an .rdp file from a RemoteApp program

You can use the RemoteApp Wizard to create an .rdp file from any program in the **RemoteApp Programs** list.

To create an .rdp file

1. Start TS RemoteApp Manager. To do this, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS RemoteApp Manager**.
2. In the **RemoteApp Programs** list, click the program that you want to create an .rdp file for. To select multiple programs, press and hold the CTRL key when you click each program name.
3. In the **Actions** pane for the program or selected programs, click **Create .rdp file**.

 **Note:**

If you selected multiple programs, the settings described in the rest of this procedure apply to all of the selected programs. A separate .rdp file is created for each program.

4. On the **Welcome to the Remote App Wizard** page, click **Next**.
5. On the **Specify Package Settings** page, do the following:
 1. In the **Enter the location to save the packages** box, accept the default location or click **Browse** to specify a new location to save the .rdp file.
 2. In the **Terminal server settings** area, click **Change** to modify the terminal server or farm name, the RDP port number, and the **Require server authentication** setting. (For more information about these settings, see [Configure terminal server settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_TerminalServerSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_TerminalServerSettings] .) When you are finished, click **OK**.
 3. In the **TS Gateway settings** area, click **Change** to modify or to configure whether clients will use a TS Gateway server to connect to the target terminal server across a firewall. (For more information about these settings, see [Configure TS Gateway settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_TSGatewaySettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_TSGatewaySettings] .) When you are finished, click **OK**.

 **Note:**

For more information about TS Gateway, see the TS Gateway Step-by-Step Guide (<http://go.microsoft.com/fwlink/?LinkId=85872> [http://go.microsoft.com/fwlink/?LinkId=85872]).

4. To digitally sign the .rdp file, in the **Certificate Settings** section, click **Change** to select or to change the certificate to use. Select the certificate that you want to use, and then click **OK**. (For more information about these settings, see [Configure digital signature settings \(optional\)](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_DigitalSigSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.mspx#BKMK_DigitalSigSettings] .)
6. When you are finished, click **Next**.
7. On the **Review Settings** page, click **Finish**.

When the wizard is finished, the folder where the .rdp file was saved opens in a new window. You can confirm that the .rdp file was created.

[Top of page](#)

Create a Windows Installer package from a RemoteApp program

You can use the RemoteApp Wizard to create a Windows Installer (.msi) package from any program in the **RemoteApp Programs** list.

To create a Windows Installer package

1. Start TS RemoteApp Manager. To do this, click **Start**, point to **Administrative Tools**, point to **Terminal Services**, and then click **TS RemoteApp Manager**.
2. In the **RemoteApp Programs** list, click the program that you want to create a Windows Installer package for. To select multiple programs, press and hold the CTRL key when you click each program name.
3. In the **Actions** pane for the program or selected programs, click **Create Windows Installer package**.

Note:

If you selected multiple programs, the settings described in the rest of this procedure apply to all of the selected programs. A separate Windows Installer package is created for each program.

4. On the **Welcome to the RemoteApp Wizard** page, click **Next**.

5. On the **Specify Package Settings** page, do the following:
 1. In the **Enter the location to save the packages** box, accept the default location or click **Browse** to specify a new location to save the Windows Installer package.
 2. In the **Terminal server settings** area, click **Change** to modify the terminal server or farm name, the RDP port number, and the **Require server authentication** setting. (For more information about these settings, see [Configure terminal server settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TerminalServerSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TerminalServerSettings] .) When you are finished, click **OK**.
 3. In the **TS Gateway settings** area, click **Change** to modify or to configure whether clients will use a TS Gateway server to connect to the target terminal server across a firewall. (For more information about these settings, see [Configure TS Gateway settings](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TSGatewaySettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_TSGatewaySettings] .) When you are finished, click **OK**.



Note:

For more information about TS Gateway, see the TS Gateway Step-by-Step Guide (<http://go.microsoft.com/fwlink/?LinkId=85872> [http://go.microsoft.com/fwlink/?LinkId=85872]).

4. To digitally sign the file, in the **Certificate Settings** section, click **Change** to select or to change the certificate to use. Select the certificate that you want to use, and then click **OK**. (For more information about these settings, see [Configure digital signature settings \(optional\)](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_DigitalSigSettings) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_DigitalSigSettings] .)
6. When you are finished, click **Next**.
7. On the **Configure Distribution Package** page, do the following:
 1. In the **Shortcut icons** area, specify where the shortcut icon for the program will appear on client computers.

2. In the **Take over client extensions** area, configure whether to take over client file name extensions for the program.

If you associate the file name extensions on the client computer with the RemoteApp program, all file name extensions that are handled by the program on the terminal server will also be associated on the client computer with the RemoteApp program. For example, if you add Microsoft Word as a RemoteApp program, and you configure the option to take over client file name extensions, any file name extensions on the client computer that Word takes over will be associated with Remote Word. This means that any existing program on the client computer will no longer handle file name extensions such as .doc and .dot. Note that users are not prompted whether the terminal server should take over file extensions for the program.

To view what file name extensions are associated with a program on the terminal server, click **Start**, click **Control Panel**, and then double-click **Default Programs**. Click **Associate a file type or protocol with a program** to view the file name extensions and their default associated program.

 **Caution:**

Do not install Windows Installer packages that were created with this setting enabled on the terminal server itself. If you do, clients that use the Windows Installer package may not be able to start the associated RemoteApp program.

8. After you have configured the properties of the distribution package, click **Next**.
9. On the **Review Settings** page, click **Finish**.

When the wizard is finished, the folder where the Windows Installer package was saved opens in a new window. You can confirm that the Windows Installer package was created.

[↑Top of page](#)

[↑Top of page](#)

Make RemoteApp programs available from the Internet

By using TS RemoteApp together with TS Gateway, you can enable users to connect from the Internet to individual programs on a terminal server without having to first establish a virtual private network (VPN) connection. (Alternatively, if you do not want to deploy TS Gateway, you can make RemoteApp programs available through a VPN solution.) Depending on the deployment method that you choose, remote users can connect to a program by opening an .rdp file, by clicking a shortcut to a Windows Installer package on their desktop or **Start** menu, or by accessing a RemoteApp program on a Web page through TS Web Access.

To make RemoteApp programs available from the Internet through TS Gateway, follow these steps:

1.Ensure that you meet the following prerequisites:

- You must have already deployed RemoteApp programs on the terminal server.
- If you want to make RemoteApp programs available from the Internet through TS Web Access, you must have successfully deployed TS Web Access in an intranet environment.

2.Review the TS Gateway Step-by-Step Guide (<http://go.microsoft.com/fwlink/?LinkId=85872> [<http://go.microsoft.com/fwlink/?LinkId=85872>]).

3.Following the procedures in the TS Gateway Step-by-Step Guide, deploy and configure TS Gateway. When you do so, make sure that you do the following:

- 1.Create a Terminal Services connection authorization policy (TS CAP) to define the list of user groups that can connect to the terminal servers that host the RemoteApp programs. For more information, see the "Create a TS CAP for the TS Gateway server" section of the TS Gateway Step-by-Step guide.
- 2.Create a Terminal Services resource authorization policy (TS RAP) that provides access to the terminal servers that host the RemoteApp programs.

When you create the TS RAP, add the user groups that you defined in the TS CAP. Also, create a new TS Gateway-managed computer group that contains both the NetBIOS names and the fully qualified domain names (FQDNs) of the terminal servers that host the RemoteApp programs.

 **Note:**

If you are using a terminal server farm, specify the name of the farm, and not the individual farm members.

For more information, see the "Create a TS RAP and specify computers that users can connect to through the TS Gateway server" section of the TS Gateway Step-by-Step Guide.

4.Configure TS Gateway settings in TS RemoteApp Manager (either in the global deployment settings or when you create an .rdp file or Windows Installer package). When you do so, make sure that you specify the FQDN of the TS Gateway server.

When you configure global deployment settings, the changes will be reflected immediately on the TS Web Access Web site.

 **Note:**

If you have previously created .rdp files and Windows Installer packages, the new settings will not be reflected in those packages. You must create new packages with the correct settings, and then distribute them to users.

5.To allow Internet access to RemoteApp programs through TS Web Access, configure firewall and authentication settings. For more information, see [Configure the TS Web Access server to allow access from the Internet](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_AllowInternetAccess) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_AllowInternetAccess] in the following section.

Configure the TS Web Access server to allow access from the Internet

To allow users to access the TS Web Access server from the Internet through TS Gateway, the recommended configuration is to place both the TS Gateway server and the TS Web Access server in the perimeter network, with the terminal servers that host RemoteApp programs behind the internal firewall.

Alternatively, you can deploy TS Web Access on the internal network, and then make the Web site available through Microsoft Internet Security and Acceleration (ISA) Server. For more information about Web publishing through ISA Server 2006, visit the "Publishing Concepts in ISA Server 2006" Web site (<http://go.microsoft.com/fwlink/?LinkId=86359> [<http://go.microsoft.com/fwlink/?LinkId=86359>]).

If you deploy TS Web Access in the perimeter network, you must configure your firewall to allow Windows Management Instrumentation (WMI) traffic from the TS Web Access server to the terminal server. You must ensure that TCP port 135 is open for WMI-related DCOM traffic. To control the other ports that are used for WMI traffic, you can configure a fixed port. For information about how to do this, see "Setting Up a Fixed Port for WMI" in MSDN (<http://go.microsoft.com/fwlink/?LinkId=109867> [<http://go.microsoft.com/fwlink/?LinkId=109867>]). To use this procedure on a Windows Server 2008-based server, note the following additional information:

- If you are not logged on by using the local Administrator account, you must run the commands from an elevated command prompt. To open an elevated command prompt, click **Start**, right-click **Command Prompt**, and then click **Run as administrator**.
- The procedure shows how to configure TCP port 24158 for WMI traffic. By default, the **winmgmt -standalonehost** command moves the Windows Management Instrumentation service (Winmgmt) to a standalone Svchost process that has a fixed DCOM endpoint of "ncacn_ip_tcp.0.24158".

To specify a different port number, do not use the **winmgmt -standalonehost** command. Instead, you must do the following.

To specify a port number that is different from the default

1. Use Component Services to configure the fixed DCOM endpoint for WMI to the port that you want. To do this, follow these steps:
 1. Open Component Services. To do this, click **Start**, point to **Administrative Tools**, and then click **Component Services**.
 2. In the console tree, expand **Component Services**, expand **Computers**, expand **My Computer**, and then click **DCOM Config**.
 3. In the middle pane, right-click **Windows Management and Instrumentation**, and then click **Properties**.
 4. Click the **Endpoints** tab, and then click either **Properties** or **Add**, depending on whether an existing custom entry already exists.

5. Click **Use static endpoint**, enter the port number to use, and then click **OK** two times.

- Restart the Winmgmt service for the change to take effect. To restart the service, run the commands **net stop winmgmt** and **net start winmgmt** from the command line.
 - Run the **netsh** command with the **port** parameter set to the same port that you specified in Component Services. (See the following bullet point for more information about the **netsh** command syntax.)
- When you run the **netsh** command to create a firewall rule, you must include the **protocol** parameter and specify TCP as the protocol type. The following is an example of the command syntax:

```
netsh firewall add portopening protocol=TCP port=24158 profile=domain name=WMIFixedPort
```

 **Note:**

The **profile** parameter indicates whether the firewall rule applies to the Domain, Private, or Public profile. For more information see "Understanding Windows Firewall with Advanced Security profiles" in Windows Firewall with Advanced Security Help.

Additionally, the TS Web Access Web site must be configured to use Windows authentication. By default, Windows authentication is enabled for the TS Web Access Web site.

To verify that Windows authentication is enabled

- On the TS Web Access server, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
- In the left pane of Internet Information Services (IIS) Manager, expand the server name, expand **Sites**, expand **Default Web Site**, and then click **TS**.
- In the middle pane, under **IIS**, double-click **Authentication**.
- Ensure that Windows Authentication is set to **Enabled**. If it is not, right-click **Windows Authentication**, and then click **Enable**.

 **Note:**

If you placed TS Web Access in a custom Web site, you must ensure that the authentication method that is used for the Web site can map to the user's Windows account. You can do this by using integrated Windows authentication on the custom Web site.

[⬆️Top of page](#)

Additional information

Configure Server Manager and Initial Tasks not to run in administrator's RemoteApp session

If a user has administrative access to the terminal server where the RemoteApp programs are installed, when the user starts a RemoteApp program, the Server Manager tool and Initial Configuration Tasks also start in the RemoteApp session.

You can control this behavior by using the following Group Policy settings in the **Computer Configuration \Administrative Templates\System\Server Manager** node of the Local Group Policy Editor on the terminal server:

- Do not display Initial Configuration Tasks window automatically at logon

You must enable this policy setting to prevent the Initial Configuration Tasks window from opening when a user with administrative access starts a RemoteApp session.

- Do not display Server Manager automatically at logon

You must enable this policy setting to prevent Server Manager from opening when a user with administrative access starts a RemoteApp session.

Configure Remote Desktop Web Connection behavior

Terminal Services Remote Desktop Web Connection enables a user to connect to the desktop of a remote computer from the TS Web Access Web site. To connect to a remote computer, the following conditions must be true:

- The remote computer must be configured to accept Remote Desktop connections.
- The user must be a member of the Remote Desktop Users group on the remote computer.

A user can access Remote Desktop Web Connection by clicking the **Remote Desktop** tab on the TS Web Access page. As an administrator, you can configure whether the **Remote Desktop** tab is available to users. Additionally, you can configure settings such as which TS Gateway server to use, and the default device and resource redirection options.

Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

To configure Remote Desktop Web Connection behavior

1. On the TS Web Access server, start Internet Information Services (IIS) Manager. To do this, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
2. In the left pane, expand the server name, expand **Sites**, expand **Default Web Site**, and then click **TS**.
3. In the middle pane, under **ASP.NET**, double-click **Application Settings**.
4. To change Remote Desktop Web Connection settings, modify the values in the **Application Settings** pane.
 - To configure a default TS Gateway server, double-click **DefaultTSGateway**, enter the fully qualified domain name of the server in the **Value** box (for example, **server1.contoso.com**), and then click **OK**.
 - To specify the TS Gateway authentication method, double-click **GatewayCredentialsSource**, type the number that corresponds to the desired authentication method in the **Value** box, and then click **OK**. The possible values include:
 - 0** = Ask for password (NTLM)
 - 1** = Smart card
 - 4** = Allow user to select later
 - To configure whether the **Remote Desktop** tab appears on the TS Web Access page, double-click **ShowDesktops**. In the **Value** box, type **true** to show the **Remote Desktop** tab, or type **false** to hide the **Remote Desktop** tab. When you are finished, click **OK**.
 - To configure default device and resource redirection settings, double-click the setting that you want to modify (**xClipboard**, **xDriveRedirection**, **xPnPRedirection**, **xPortRedirection**, or **xPrinterRedirection**). In the **Value** box, type **true** to enable the redirection setting by default, or type **false** to disable the redirection setting by default, and then click **OK**.
5. When you are finished, close IIS Manager.

Your changes should take effect immediately on the TS Web Access Web site. If the Web page is open, refresh the page to view the changes.

 **Note:**

You can also configure these settings by modifying the %windir%\Web\ts\Web.config file directly by using a text editor such as Notepad.

[↑Top of page](#)

Change the install location of the default TS Web Access Web site

By default, when you install TS Web Access, the TS Web Access Web site installs to the Default Web Site in IIS (to the /TS virtual path). To specify a different Web site to install TS Web Access, you can configure a different target Web site in the registry. You must do this before you install the TS Web Access role service.

Caution:

Serious problems might occur if you modify the registry incorrectly by using Registry Editor or by using another method. These problems might require that you reinstall the operating system. Microsoft cannot guarantee that these problems can be solved. Modify the registry at your own risk.

To change the location of the TS Web Access Web site

1. If you do not already have IIS installed, install IIS. To do this, follow these steps:
 1. Start Server Manager. To open Server Manager, click **Start**, point to **Administrative Tools**, and then click **Server Manager**.
 2. Under **Roles Summary**, click **Add Roles**.
 3. On the **Before You Begin** page, click **Next**.
 4. On the **Select Server Roles** page, select the **Web Server (IIS)** check box, click **Add Required Features**, and then click **Next**.
 5. On the **Web Server (IIS)** page, click **Next**.
 6. On the **Select Role Services** page, click **Next**.
 7. On the **Confirm Installation Selections** page, click **Install**.
 8. On the **Installation Results** page, verify that the installation succeeded, and then click **Close**.
2. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.
3. In Internet Information Services (IIS) Manager, expand the server name, right-click **Sites**, and then click **Add Web Site**.

4. In the **Add Web Site** dialog box, add the information for the new Web site, such as the site name. Ensure that you do the following:
 - In the **Physical path** box, specify the path **C:\Windows\Web**, where "C:" represents the drive where you installed Windows.
 - To not conflict with the Default Web Site, you should either specify a different IP address in the **IP address** list, or specify a port other than port 80 in the **Port** box. (If you specify another port, ensure that the firewall is configured to permit HTTP or HTTPS traffic on that port, depending on your configuration.)
5. When you are finished, click **OK**.
6. Start Registry Editor. To do this, click **Start**, type **regedit** in the **Start Search** box, and then press ENTER.
7. Locate the following registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
8. To specify a new install location for the TS Web Access Web site, do the following:
 - 1.Right-click **Microsoft**, point to **New**, and then click **Key**.
 - 2.Type **Terminal Server Web Access** as the subkey name, and then press ENTER.
 - 3.Right-click **Terminal Server Web Access**, point to **New**, and then click **String Value**.
 - 4.Type **Website** as the entry name, and then press ENTER.
 - 5.Right-click **Website**, and then click **Modify**.
 - 6.In the **Value data** box, type the name of the Web site where you want to install the TS Web Access Web site (the site name that you specified in step 4 of this procedure), and then click **OK**.
9. Close Registry Editor.
10. Install TS Web Access. For more information, see [Install the TS Web Access role service](http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_InstallTSWebAccess) [http://technet2.microsoft.com/WindowsServer2008/en/library/61d24255-dad1-4fd2-b4a3-a91a22973def1033.msp#BKMK_InstallTSWebAccess] earlier in this guide.

[Manage Your Profile](#)

© 2008 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

