Realtime
publishers
"Leading the Conversation"

# The Definitive Guide™ To

# Building a Windows Server 2008 Infrastructure

*sponsored by*

triCerat

Greg Shields

## Copyright Statement

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

# Chapter 8: Advanced Topics in Terminal Services

Terminal Services and Terminal Server aren't new technologies. Originally available with the release of Windows NT as Windows NT Terminal Server Edition, the bits that make up Terminal Server have been around since 1998, making this most recent operating system (OS) release a 10 year celebration of Windows' remote application support. But Terminal Server has always had a complex history in relation with its related product Citrix XenApp (also previously called Citrix Presentation Server and Citrix MetaFrame).

Due to long-standing agreements between Microsoft and Citrix, the two applications have been tied to each other throughout their history. Citrix's product and its features have traditionally been targeted for environments with higher-end requirements, with the Citrix product including extra management features like Published Applications, transport level security, a customizable web front-end, multiple mechanisms for deploying applications, and a rich load balancing engine for distributing incoming client session requests. These and other feature sets have historically only been available in the higher-end and higher-cost Citrix product.

Contrast this to Terminal Services, which over its history has usually been relegated to uses within smaller environments, those that cannot afford the added features of Citrix, or have no needs for them. A major factor in this decision is that Terminal Services is significantly less expensive than the Citrix solution, owing to the fact that no extra license costs are required other than for the TS CALs discussed in our last chapter. In contrast, using Citrix in the environment requires additional per concurrent user licenses along with their accompanying maintenance costs over and above Terminal Services' TS CALs, Windows licenses, and maintenance. This makes Citrix's features a natural up-sell for those that find themselves needing its extra functionality.

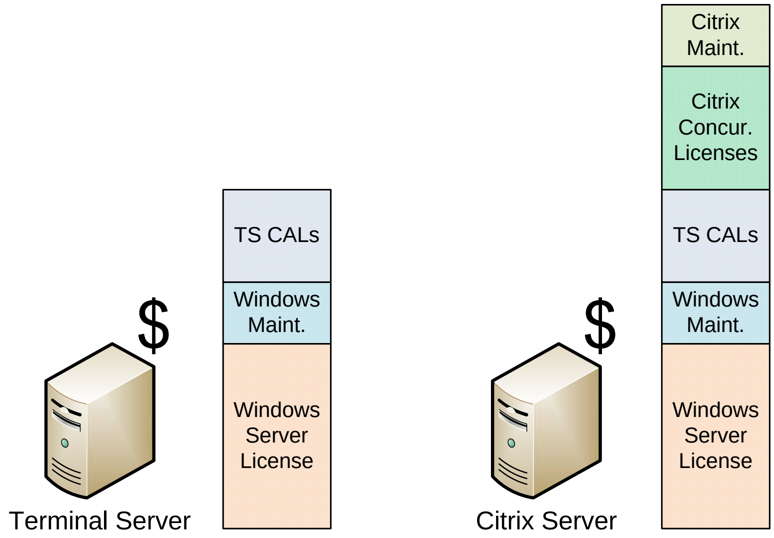


***Figure 8.1: A Terminal Server has a lower cost of entry and recurring cost of ownership than does a comparable Citrix server.***

## Advanced New Functionality for Terminal Services in Windows Server 2008

The relationship between these two products changes substantially with the release of Windows Server 2008. Specifically, the difference in functionality between what is available in the Citrix solution and what Terminal Services includes gets closer than ever before:

- With Windows Server 2008, Terminal Services adds application publishing through TS RemoteApps. Adding to this are multiple new ways in which applications can be deployed to clients, through the sharing of RDP files, direct installation, or hosting via a web site.
- Certificate-based transport level security as well as the ability to proxy session traffic arrives with the inclusion of TS Gateway.
- Microsoft gains its own pre-built web front-end for hosting Terminal Server connections through the addition of TS Web Access.
- Load balancing of multiple Terminal Servers gets greatly improved with the new TS Session Broker.

Though not all the features that differentiate Microsoft and Citrix are now aligned, Terminal Server administrators who have been looking longingly from the sidelines at the exciting features previously only available with Citrix can now add some of them into their Terminal Services environment for no added cost. In this chapter, we'll talk in detail about how to set up and use each of these new "advanced" features, and how each has the ability to significantly improve your users' experience.

> If you are considering an upgrade to Citrix XenApp, consider carefully the features you need. Those features may now be available with Terminal Services alone.

## Deploying Applications with Terminal Services

In Chapter 7 we talked about how to use the Remote Desktop Client to connect to a Terminal Server desktop session. This process can be done by any user with the correct permissions to connect to a full server desktop along with its installed applications. But sometimes you the administrator don't want to provide access to that entire server desktop. Instead, you may want to provide access to only a specified few applications on the server. There are a number of reasons why enabling access to specified applications can be a superior solution than with deploying full desktops:

- *Enabling access to specified applications can be easier for users to understand.* Users know they need access to their applications. Giving them a secondary desktop with a full Start bar and all the other accouterments can be confusing.
- *Enabling access to specified applications can consume fewer resources on the server.* Because the full desktop and explorer.exe shell along with the other processes it relies upon does not need to be rendered for each user, fewer resources are consumed per user than with full desktops.
- *Enabling access to specified applications can consume more predictable levels of resources.* When users are given access to a full desktop, they typically have the ability to use any of the applications on that server. This makes it very difficult to profile resource consumption by users because their actions are less controllable. This inability to profile makes it more difficult to understand and plan for resource use, and thereby ensure the best possible user's experience.
- *Enabling access to specified applications can be easier to secure.* When full desktops are provided for users, administrators must undergo a securing activity to restrict what activities users can do while logged in. When applications are provided, this activity needs be done per application instead of per desktop, a process that is much easier to accomplish.

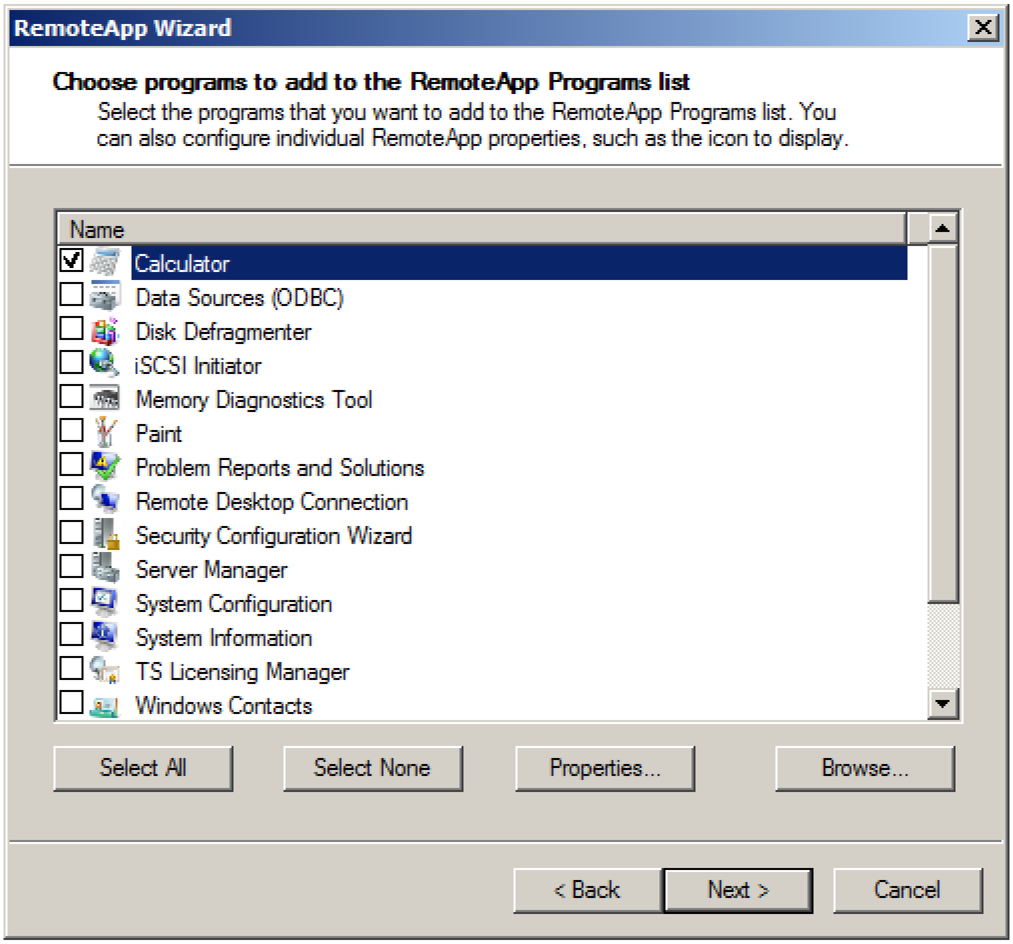
These benefits aren't the only factors that should drive your decision about how to make applications available to your users. There are a few gotcha's associated with distributing applications rather than full desktops. For example, enabling access to specified applications can be more challenging when applications need to work with each other. This is the process whereby one application spawns a second application to process some form of data.

Imagine the situation where Microsoft Outlook needs to launch Microsoft Word in order for Word to display an attached document. For this down-level application spawning to function correctly, each potential application that could be spawned must be collocated on the same server. A TS RemoteApp will automatically launch the second application when necessary, but only if it resides on the same Terminal Server.

> Make sure that all applications potentially required by applications you plan to host are also located on your Terminal Servers. You may not necessarily need to create them as TS RemoteApps, but they must be installed.

### TS RemoteApps

TS RemoteApps are configured from the TS RemoteApp Manager, and any application that will be configured as a TS RemoteApp must be first installed to the server. Once installed, right-click the *TS RemoteApp Manager* in Server Manager and choose *Add RemoteApp Programs*. This will launch the *RemoteApp Wizard*. Clicking *Next* will present a screen that lists the applications currently installed to the server, similar to what is seen in Figure 8.2. If the application you wish to distribute is available, select it from the list and click *Next*.



RemoteApp Wizard

**Choose programs to add to the RemoteApp Programs list**

Select the programs that you want to add to the RemoteApp Programs list. You can also configure individual RemoteApp properties, such as the icon to display.

| Name |
|---|
| ☑ Calculator |
| □ Data Sources (ODBC) |
| □ Disk Defragmenter |
| □ iSCSI Initiator |
| □ Memory Diagnostics Tool |
| □ Paint |
| □ Problem Reports and Solutions |
| □ Remote Desktop Connection |
| □ Security Configuration Wizard |
| □ Server Manager |
| □ System Configuration |
| □ System Information |
| □ TS Licensing Manager |
| □ Windows Contacts |

***Figure 8.2: The RemoteApp Wizard interrogates the server to populate a list of available applications that can be distributed via Terminal Services.***

Occasionally, the specific application you wish to distribute is not available in the list. When this occurs, click the *Browse* button and select the primary executable for launching the application. For this example, we'll choose the *Calculator* application, click *Next*, and then click *Finish* to create the TS RemoteApp.

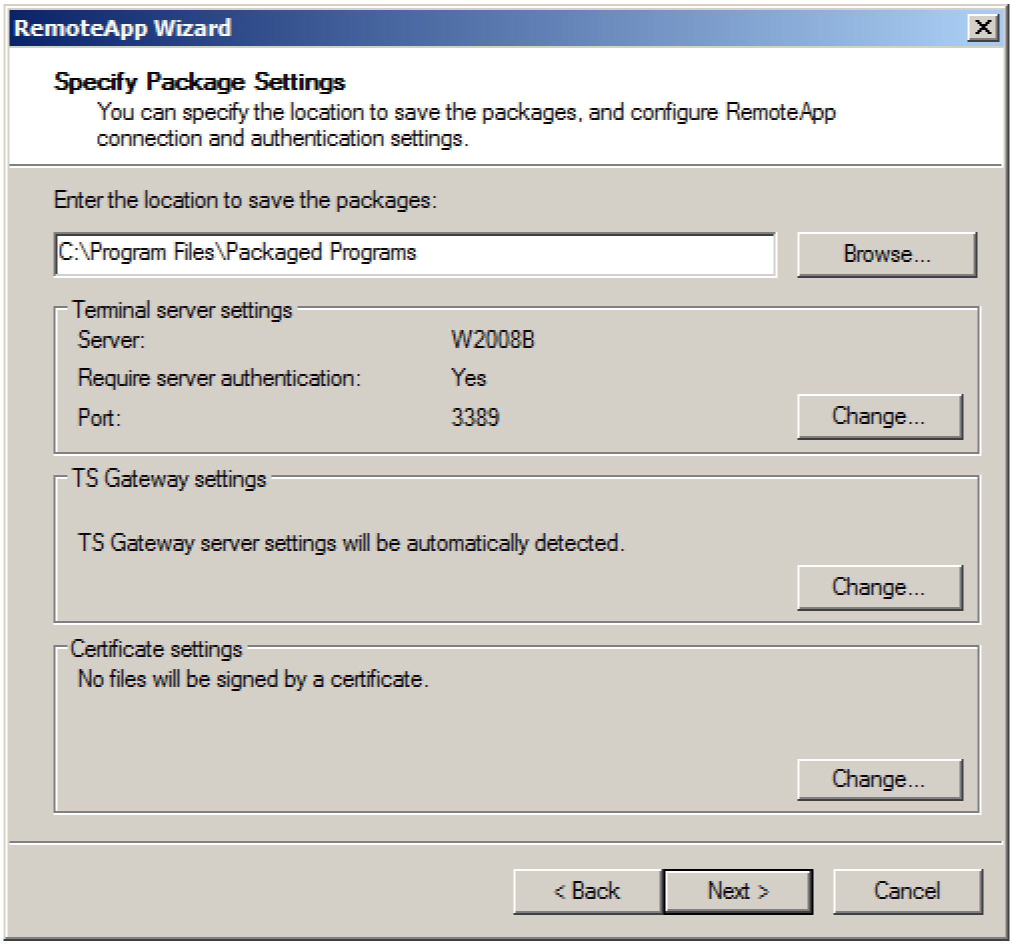
☞ Sometimes you may wish to host an application with special parameters or command line arguments. These arguments launch the application with special configurations or automatically launch a specific document. As an example, you can launch Microsoft Excel with a specific spreadsheet automatically loaded. Do this by clicking the Properties button. In the resulting screen, change the selection for Command-line arguments. In this same screen it is also possible to change the program's name, icon, location, or alias.

### TS RemoteApp Distribution Options

Once created, there are three major mechanisms through which TS RemoteApps can be deployed to your users. Depending on how you want your users to interact with their applications, you may make available one or more of these options to users. Multiple distribution options can be used simultaneously as well if desired. The three distribution options are distribution of RDP files, RDP installation to local desktops, and hosting via TS Web Access. We'll talk about each of these in the sections below.

### RDP File Distribution

The easiest mechanism for distribution is one that's been used with previous OS versions for distributing published desktops. Providing access to RDP files through storage on a file share or distribution through email or other medium is one way to connect users to Terminal Services hosted applications. Once a TS RemoteApp has been created, right-click the application in the list of RemoteApp Programs and choose *Create .rdp file*. A wizard will appear that looks similar to Figure 8.3.



RemoteApp Wizard

**Specify Package Settings**

You can specify the location to save the packages, and configure RemoteApp connection and authentication settings.

Enter the location to save the packages:

C:\Program Files\Packaged Programs

Terminal server settings

Server: W2008B

Require server authentication: Yes

Port: 3389

TS Gateway settings

TS Gateway server settings will be automatically detected.

Certificate settings

No files will be signed by a certificate.

***Figure 8.3: A wizard is available for configuring RDP files at the time of creation.***

Within this wizard, it is possible to configure where the resulting RDP file will be stored, as well as settings for the Terminal Server itself, TS Gateway, and any certificate settings used. By clicking the *Change* button under *Terminal server settings* it is possible to make modifications to the server or RDP port used by the RDP file in connecting to the server. For our example, we'll also remove the check next to *Require server authentication*.

Although we'll talk in a later section about the integration of RemoteApps with TS Gateway, be aware that with Windows Server 2008 it is possible—and suggested—to digitally sign RDP files using certificates. Signing an RDP file enables the client to authenticate your identity as its publisher. It allows clients to verify the organization that authored the RDP file, and enables them to make informed decisions about whether to attempt a connection using the file.

Click *Next* and *Finish* to complete the wizard. Once complete, any RDP client that can resolve the Terminal Server will be able to double-click the resulting file to launch the Calculator RemoteApp. Distributing this file to prospective users or storing it on a file share will make the connection available for users who need to access the program.

> ☞ If you plan to enable access to RemoteApps from computers in other DNS zones such as from the Internet, ensure that the server name within the RDP file is fully qualified and that the client can resolve the Fully Qualified DNS Name (FQDN) of the Terminal Server from those network locations. This is particularly important if you plan to enable Internet-based access to applications.

## Local Desktop Installation

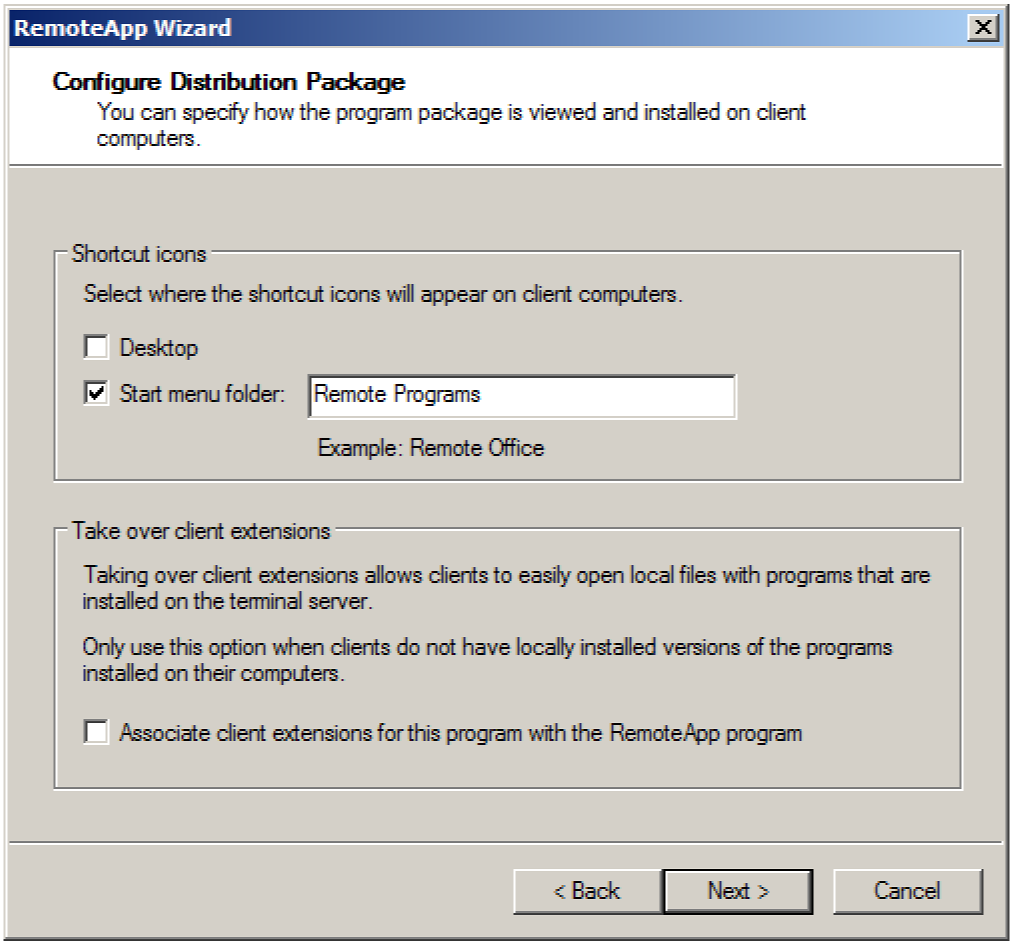
In terms of usefulness, RDP file distribution is arguably the least interesting of the distribution options available. Another more exciting option available once a RemoteApp has been created is to wrap the RDP file into an MSI file installation. This process enables the administrator to "install" the RDP file onto the desktop of users that may need to access the RemoteApp. To make this option even more useful, multiple options are available for the administrator to include with the MSI installation:

- *Start Menu shortcut.* This option adds a link to the RemoteApp into the desktop's Start Menu, allowing the user to launch the RemoteApp just like they would a typical, locally-installed program. Like all Start Menu shortcuts, it is possible to specify a Start Menu folder where the link will be stored.

- *Desktop shortcut.* In addition to the Start Menu link, it is also possible to include a shortcut on the user's desktop.

- *Take over client extensions.* Every Windows desktop and server includes client extension associations. These associations allow a user to double-click a file to automatically launch the application that is configured to use that file. As an example, when a file with a .DOC extension is double-clicked, computers will automatically launch Microsoft Word—if it is installed—with the file loaded. By selecting the option *Associate client extensions for this program with the RemoteApp program*, this will instruct the MSI installation to re-associate client extensions to launch the remote application rather than the local instance when a file is double-clicked.

To create an MSI installation file, click the *Create Windows Installer Package* link in the TS RemoteApp Manager. While the first screen of the resulting wizard looks similar to what we've already seen in Figure 8.3, click *Next* to see the additional configuration information shown in Figure 8.4. On this screen of the wizard you can choose the installation parameters noted above. Click *Next* and *Finish* to create the MSI installation file.



RemoteApp Wizard

Configure Distribution Package

You can specify how the program package is viewed and installed on client computers.

Shortcut icons

Select where the shortcut icons will appear on client computers.

☐ Desktop

☑ Start menu folder: Remote Programs

Example: Remote Office

Take over client extensions

Taking over client extensions allows clients to easily open local files with programs that are installed on the terminal server.

Only use this option when clients do not have locally installed versions of the programs installed on their computers.

☐ Associate client extensions for this program with the RemoteApp program

***Figure 8.4: The Configure Distribution Package screen enables choices for how the RDP file will be installed.***

Once complete, the resulting MSI installation file will need to be installed to all clients who will use the remote application. This installation can be done manually, using a software deployment solution like Microsoft System Center Configuration Manager or others, or distributed using Active Directory's native software distribution capabilities.

### Hosting via TS Web Access

The last option for distribution is to host the application on a TS Web Access web site. We'll talk more about the installation and configuration of TS Web Access in the next section. But, for now, know that the process to make a TS RemoteApp available through TS Web Access is to right-click the application in RemoteApp Programs and select *Show in TS Web Access*. Doing this immediately makes the application available in the TS Web Access instance currently configured for this Terminal Server.

If you wish to make a full desktop connection available in TS Web Access, right-click the *TS RemoteApp Manager* in Server Manager and choose *Terminal Server Settings*. In the resulting screen, check the box for *Show a remote desktop connection to this terminal server in TS Web Access*. Like with RemoteApps, this will immediately make an icon for the full desktop connection available in TS Web Access.

One of the benefits of using TS Web Access for user access to RemoteApps is in the ease of adding and removing applications as they evolve over time. For example, if you have a Terminal Server-hosted application that regularly changes versions over time, using TS Web Access as the location for hosting its access is handy because the old version can be simply "turned off" when it is no longer relevant. At the same time, the new version can be "turned on" when it is ready for use. This is different than with the MSI deployment option, where changes to a hosted application can force a change to the installed MSI.

This same situation holds true for applications that you want to disable for maintenance periods. It is very easy to remove the RemoteApp's link in TS Web Access during its maintenance period through a single click.

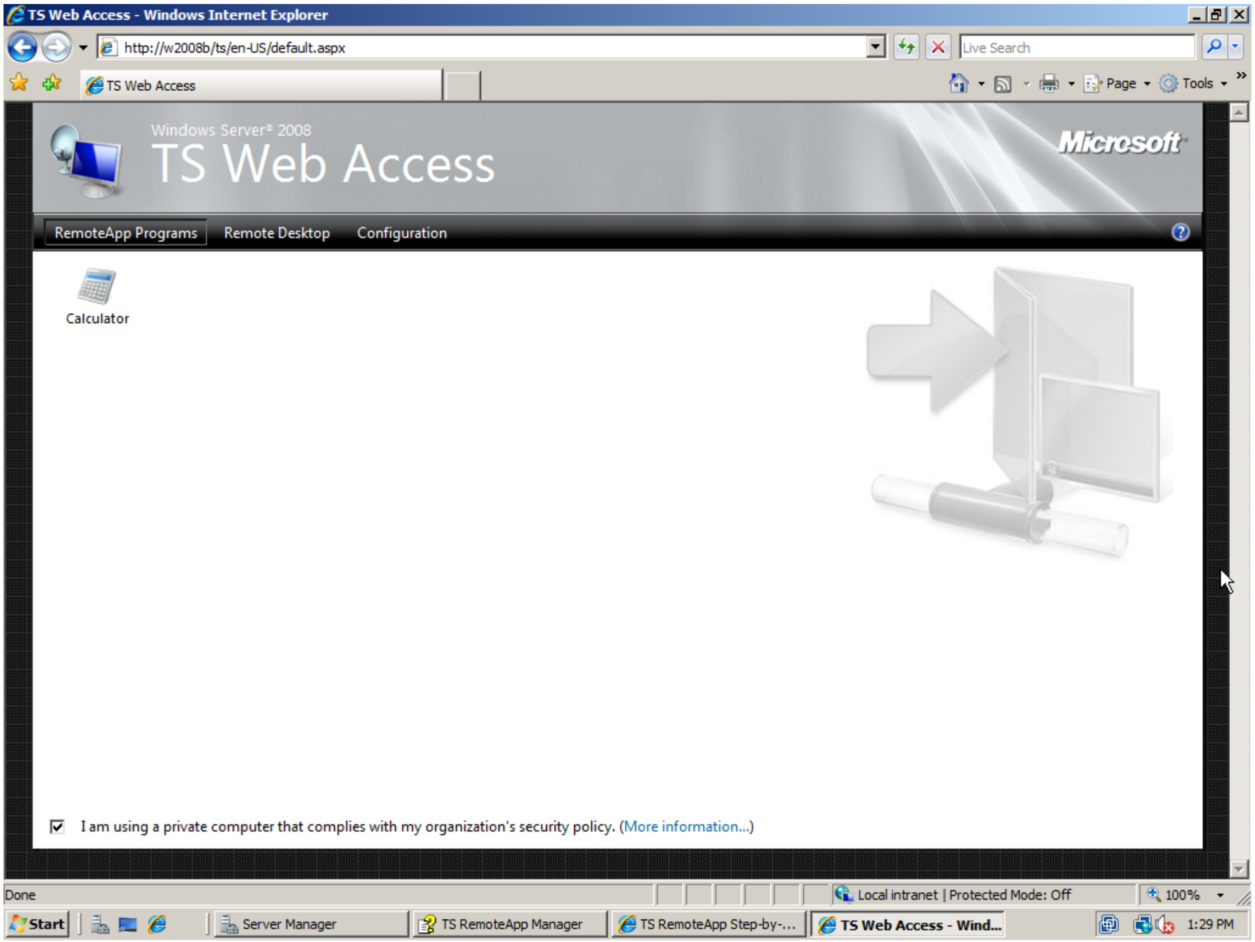
Before making applications available to your users, consider well the ways in which you plan to distribute RemoteApp access to your users, as each mechanism has its own benefits and drawbacks.

## TS Web Access

Before applications can be hosted via a TS Web Access site, the Role Service must be installed to a Windows Server 2008 computer somewhere within your domain. This computer need not be the same computer that acts as a Terminal Server, and for larger or more complex installations it is often a best practice to use a separate server. Installing TS Web Access to an existing web server is another option for environments that already have a dedicated web server in place. Installing the *TS Web Access* Role Service is done in the same way that other Role Services are installed through Server Manager. If not already present, adding the Role Service will install the necessary IIS components required to host the web site as well.

### Installing and Using TS Web Access

If you add TS Web Access to an existing Terminal Server, installing the Role Service is the only step that must be completed for users to begin using the web site. Once installed, clients can access the TS Web Access site by navigating to the URL *http://{serverName}/ts*. An example of this web site with our Calculator application already available can be seen as Figure 8.5.



TS Web Access - Windows Internet Explorer

http://w2008b/ts/en-US/default.aspx

☑ I am using a private computer that complies with my organization's security policy. (More information...)

Done

Local intranet | Protected Mode: Off

***Figure 8.5: The TS Web Access web site connects users to their applications and desktops.***

Three buttons are made available at the top of the screen: RemoteApp Programs, Remote Desktops, and Configuration. Under the tab marked *RemoteApp Programs* will be displayed any RemoteApps that have been configured to show in TS Web Access. After logging in, users will be able to double-click any listed applications to automatically launch them. Clicking on the *Remote Desktop* link brings forward an entry box that allows a user to connect to the desktop of a selected server. Options there are provided for customizing the connection in terms of screen size, devices and resources pulled into the session, as well as additional options like sounds, keyboard shortcuts, and performance.

For installations where the TS Web Access Role Service is not installed to a Terminal Server, the third button named Configuration is important. Once installed, an administrator needs to first navigate to this button and input the name of the Terminal Server or Terminal Server farm to be used as the TS Web Access site's source for listed applications. By default, TS Web Access is limited to pulling its list of available applications from only a single Terminal Server or Terminal Server farm that is hosted via TS Session Broker.

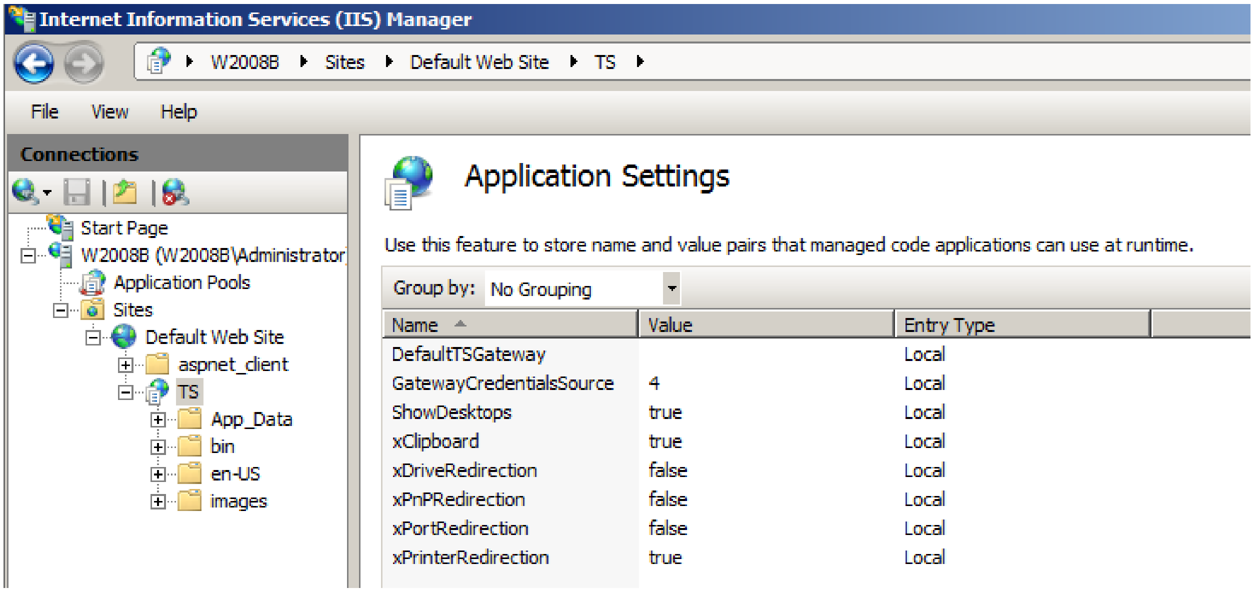
> ☞ As we'll discover later on when we talk about TS Session Broker, for a set of Terminal Servers to operate as a load balanced "farm" they must have the exact same configuration with the exact same TS RemoteApps on each instance.
>
> If you need to connect your TS Web Access instance to multiple Terminal Servers with different configurations, it is possible to programmatically configure multiple web parts to display at the same time. However, this is a complex task out of scope for this chapter. For more information on how to accomplish this using a Windows SharePoint Services integration see the web site: http://technet2.microsoft.com/windowsserver2008/en/library/7929a12e-552c-4409-9100-5a774a4cfa171033.mspx?mfr=true.

Lastly, for installations where the TS Web Access Role Service is not installed to a Terminal Server, one final task must be completed prior to making the TS Web Access site available for use by users. On the remote Terminal Server, navigate to *Administrative Tools* | *Computer Management* | *Local Users and Groups* | *Groups* and look for the group *TS Web Access Servers*. In this group add the computer account for the newly-created TS Web Access Server to the group and reboot the computer. Accomplishing this task enables the correct permissions for the Terminal Server and the TS Web Access server to work together.

> ☞ Remember that the RDC v6.1 is required for clients to work with TS Web Access. Although no additional work is required for Windows Vista, for Windows XP the ActiveX component of the RDC client must be specifically enabled. Do this within Internet Explorer by navigating to Tools | Manage Add-ons | Enable or Disable Add-ons. Enable the Add-on named Microsoft Terminal Services Client Control (redist). If multiple Add-ons of the same name are present, enable each instance.

### *Configuring TS Web Access*

TS Web Access is a relatively light application, with few configurations available for the administrator and none that are easily accessible. Available configurations can be found within IIS Manager by navigating to the *TS* website and double-clicking the IIS control panel item *ASP.NET* | *Application Settings*. There you should see a screen similar to Figure 8.6 which displays those limited configurations available for TS Web Access. These settings relate to the connected TS Gateway server and credentials source, as well as a few settings that configure master toggle switches for how sessions are displayed to connected users. Double-click any setting to change its value.


Internet Information Services (IIS) Manager
W2008B ▸ Sites ▸ Default Web Site ▸ TS ▸
File
View
Help
Connections
Start Page
W2008B (W2008B\Administrator
Application Pools
Sites
Default Web Site
aspnet_client
TS
App_Data
bin
en-US
images

Application Settings

Use this feature to store name and value pairs that managed code applications can use at runtime.

Group by: No Grouping

| Name | Value | Entry Type |
|---|---|---|
| DefaultTSGateway | | Local |
| GatewayCredentialsSource | 4 | Local |
| ShowDesktops | true | Local |
| xClipboard | true | Local |
| xDriveRedirection | false | Local |
| xPnPRedirection | false | Local |
| xPortRedirection | false | Local |
| xPrinterRedirection | true | Local |

***Figure 8.6: TS Web Access' Limited Configuration Settings are set within IIS Manager.***

The style elements that make up the TS Web Access page can be customized if desired, however this process involves a bit of coding. All files that make up the web page are stored in the folder *C:\Windows\web\ts*. By modifying the default images in the *\images* subfolder, it is possible to change the individual graphical elements that make up the web page.

It is also possible to change the text at the top of the screen that by default says "Windows Server 2008, TS Web Access". For the English language, do this by modifying the file *C:\Windows\web\ts\en-US\Default.aspx*. Look for two lines that resemble the following:

```
string L_WindowsServer2008_Text = "Windows Server<sup
style=\"font-size:8px;\">&reg;</sup> 2008";

string L_TSWebAccess_Text = "TS Web Access";
```

By changing the text marked in italics above to your desired alternate text, you can customize the default text at the top of the TS Web Access screen to something that is relevant to your environment or organization.

## TS Gateway

Throughout the history of Terminal Services, making available applications over the Internet or through high-security environments has traditionally been a problem because good encryption for the RDP protocol hasn’t been available. Additionally, without some form of proxy between the Terminal Server and its clients, the only way to enable access was through a direct connection—a solution that many security administrators will not support.

With the release of Windows Server 2008, both of these problems get a resolution in the form of TS Gateway. The TS Gateway Role Service is designed to provide certificate-based transport level security for network traffic between clients and servers, while also serving as a proxy between clients out in other networks and the Terminal Server within your protected intranet.

Figure 8.7 shows an example of how TS Gateway can be implemented within a DMZ environment for the purposes of proxying traffic between the Internet and Terminal Servers within the protected intranet. As you can see in the picture, the TS Gateway operates like a gateway that receives traffic from clients on the unprotected Internet (or other untrusted networks) and passes this traffic on to Terminal Servers in the protected internal intranet. This gateway functionality is necessary to obfuscate the internal workings of the internal Terminal Servers while at the same time protecting them from external attack.

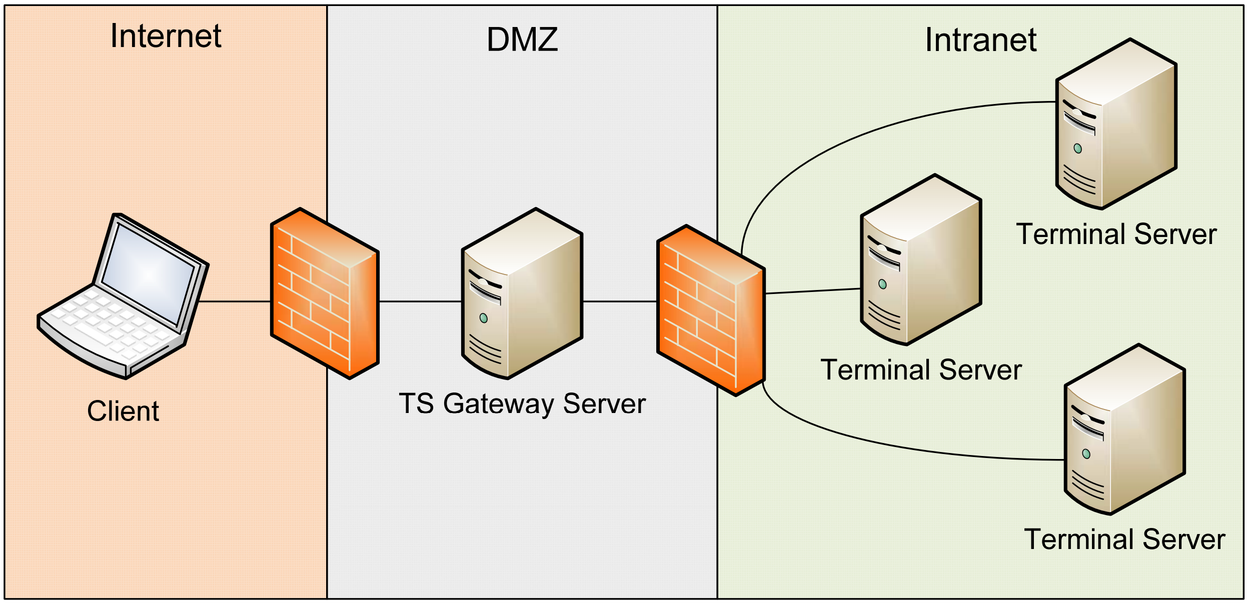


***Figure 8.7: The TS Gateway Server proxies traffic between clients in the unprotected Internet and Terminal Servers in the protected intranet.***

The typical series of events that occurs when a client attempts to connected to a Terminal Services environment that includes TS Gateway functionality resembles the following:

1. The client starts the connection by invoking a preconfigured RDP file or via an installed remote program. In either case, information necessary to locate and connect to the TS Gateway server is included within the RDP file.
2. The client then creates an SSL tunnel between itself and the TS Gateway server. This tunnel is established through the use of a preinstalled digital certificate. This certificate is used in authenticating the TS Gateway server as well as encrypting the connection.
3. Once authentication has successfully completed, the user is requested for their credentials to authorize their connection into the environment. Using a *TS Connection Authorization Policy* (TS CAP) that authorization is checked against an available authentication store (such as Active Directory) to verify access.
4. When server authentication and user authorization have completed successfully, the client then requests access to an internal Terminal Server resource. On the TS Gateway are one or more *TS Resource Authorization Policies* (TS RAPs) that instruct the TS Gateway which resources are available.
5. If the TS Gateway locates the user's resource within a TS RAP, it then establishes a connection on behalf of the client with the Terminal Services resource. From this point on, all communication between the client and the Terminal Services resource is proxied through the TS Gateway server. Inbound communication from the client occurs over TCP/443, while communication outbound from the TS Gateway occurs over the standard Terminal Services port TCP/3389.
6. Once the proxied connection is established, the client then attempts a Windows logon and authentication to the resource. If this process completes successfully, the client is granted access to use the resource.

In short, in order for the TS Gateway to function a TS CAP is required to identify and authorize the user to access the TS Gateway itself. Once this has completed successfully, the TS Gateway uses a TS RAP to identify which Terminal Server resources the user has access to use. Both of these are in addition to the standard permissions required at the Terminal Server to permit the user access to use resources.

### Installing TS Gateway

The TS Gateway Role Service does not need to be installed to a Terminal Server, although it must be installed as a member of the Windows domain in which it will be used to authenticate. The TS Gateway server can be located within the DMZ, as is shown in Figure 8.7 and explained in this chapter's example, or it can be located inside the protected intranet. There are security implications to both scenarios, and your architecture will depend on your corporate security policies as well as the level of security you wish to provide for connections to the TS Gateway server.

> ☞ If you wish to locate the TS Gateway server within your protected intranet but still require the added bridging and security gained through a DMZ-based device, consider using an ISA server located in the DMZ as an SSL bridging device. More information on how to accomplish this can be found at: http://technet2.microsoft.com/windowsserver2008/en/library/9f293f18-b0fd-48f8-b103-957fad92d70b1033.mspx?mfr=true.

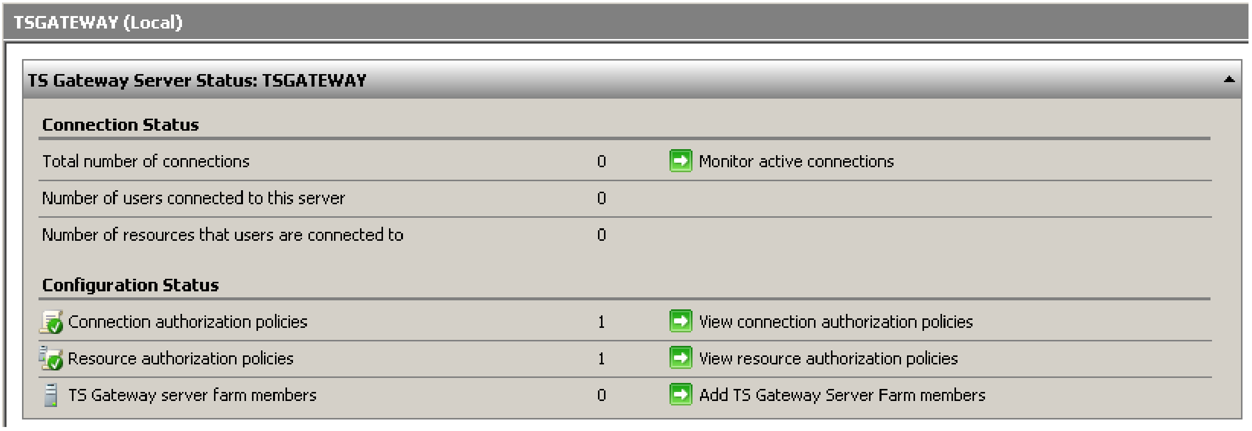
Installing the *TS Gateway* Role Service is done in the same way as with all the other Role Services we've discussed to date. Installing the TS Gateway Role Service additionally installs IIS as well as the Network Policy and Access Services used for authenticating users. The installation of the Role Service also involves a number of initial questions that need to be answered as part of the installation:

- *Server authentication certificate.* A certificate must be used for TS Gateway to successfully authenticate and encrypt network traffic as it passes. This certificate must either be signed by an external certification authority or a certification authority that is trusted by incoming clients. An option to use a self-signed certificate is available if other certificates are unavailable. However, that self-signed certificate must be manually installed to clients and is only suggested for use in very small or testing environments.
- *TS Gateway User Groups*. This selection identifies user groups that are allowed to access internal resources through the TS Gateway server.
- *TS CAP*. The TS CAP identifies how users will authenticate to the TS Gateway server. Options are exposed that include password and smart card authentication.
- *TS RAP*. Once users have been authenticated through a TS CAP, the TS RAP is used to identify which internal Terminal Server resources they are allowed to connect.
- *Network Policy and Access Services and Web Server (IIS) Services.* For both of these, the individual Role Services required by TS Gateway are already identified. For most installations, accepting the defaults here will successfully install the necessary prerequisite components.

> ☞ Digital certificates and the authentication and encryption that they provide are a critical component of a TS Gateway installation. More information about the certificate requirements for TS Gateway can be found at: http://technet2.microsoft.com/WindowsServer2008/en/library/5fdeb161-31c7-41b2-aaa3-7a4d5f5e3cda1033.mspx#BKMK_ObtainCertTSGateway.

### *Configuring TS Gateway*

Once TS Gateway is installed, the TS Gateway Manager node will appear under Terminal Services in Server Manager. This console looks similar to Figure 8.8. As you can see here, the console provides little in the way of configuration, enabling access to view active connections, modify TS CAPs and TS RAPs, change the assigned certificate for the TS Gateway, and manage the creation of TS Gateway Server Farms.



TSGATEWAY (Local)

TS Gateway Server Status: TSGATEWAY

**Connection Status**

| | | |
|---|---|---|
| Total number of connections | 0 | Monitor active connections |
| Number of users connected to this server | 0 | |
| Number of resources that users are connected to | 0 | |

**Configuration Status**

| | | |
|---|---|---|
| Connection authorization policies | 1 | View connection authorization policies |
| Resource authorization policies | 1 | View resource authorization policies |
| TS Gateway server farm members | 0 | Add TS Gateway Server Farm members |

***Figure 8.8: The TS Gateway Manager node in Server Manager includes minimal configurations.***

Let's take a look at the TS Gateway's server-specific configurations. All can be modified by right-clicking the *TS Gateway* node in Server Manager and choosing *Properties*:

- *General tab*. Under the *General* tab is the option to select the maximum number of allowed simultaneous connections that can be run through the TS Gateway server. This is done in order to throttle the level of incoming connections for performance reasons. Be aware that the Standard Edition of Windows Server 2008 has a maximum of 250 simultaneous connections through TS Gateway, while the Enterprise Edition has no such restrictions. Also possible here is the selection to *Disable new connections*. Like with the Terminal Server "drain mode" discussed in the last chapter, this allows the administrator to prevent new connections from initiating while not forcing existing connections closed.

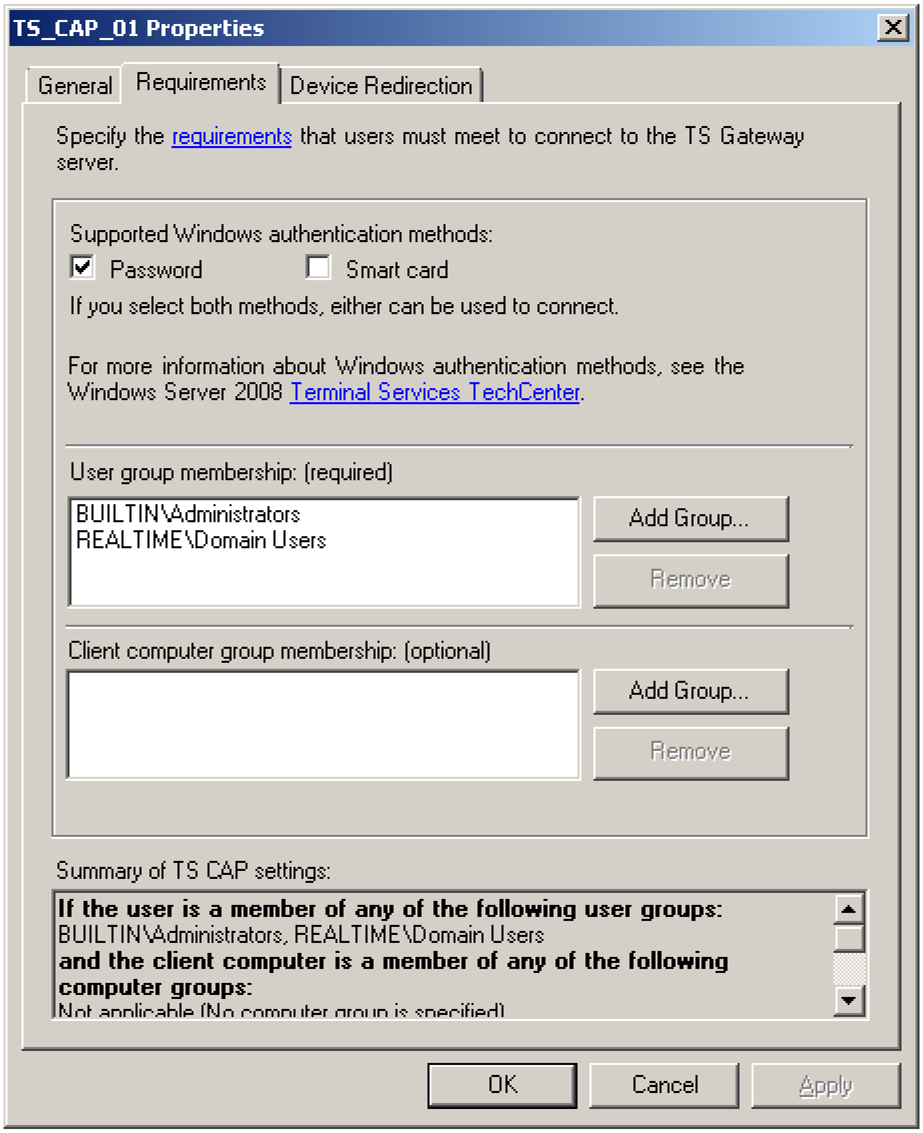
- *SSL Certificate*. This tab identifies the certificate currently assigned to the TS Gateway and allows an administrator to change the assigned certificate.

- *TS CAP Store*. Under this tab is selected whether the local server will serve as a Network Policy and Access Services (NPS) server or if a central NPS server will be used. If this TS Gateway is used as part of a Network Access Protection infrastructure, it is possible here to select whether this server will request clients to submit statements of health upon connection.

- *Server Farm.* It is possible to connect multiple, similarly-configured TS Gateway servers together to create a load balanced farm. This farm provides for greater performance during periods of high load and ensures that the loss of a single TS Gateway does not impact clients' ability to connect to Terminal Server resources. A separate load balancing solution must be implemented prior to creating a TS Gateway server farm and each must have identical configured TS CAPs and TS RAPs.
- *Auditing.* TS Gateway events are logged to the Event Log located at *Application and Services Logs | Microsoft | Windows | Terminal Services-Gateway*. This tab enables or disables the types of events that are logged to this location.
- *SSL Bridging.* This tab configures HTTPS to HTTP bridging on the TS Gateway server for situations where the TS Gateway is positioned inside the protected intranet and an ISA Server is located in the DMZ to perform SSL bridging.

Once the server has been configured as appropriate for your environment, the next step is to ensure that TS CAPs and TS RAPs are properly configured. If you created these during the TS Gateway installation, they should be already be equipped for connecting clients. Verify this within Server Manager by navigating to *TS Gateway Manager | {serverName} | Policies | Connection Authorization Policies*. In this location should be the policy created at installation. Double-click this policy to see three tabs:

- *General.* Here the name of the TS CAP can be changed and the policy can be enabled or disabled as necessary. TS Gateway has the ability to create multiple policies for different classes of users, computer, and authentication methods. Policies are processed in the order presented in the console.
- *Requirements.* This tab, shown in Figure 8.9, shows the types of authentication mechanisms available and configured as well as the user groups and computer groups that have been granted access to the TS Gateway. Granting access by user group is required. Locking down users to particular computers by configuring computer groups adds an additional layer of authentication to incoming connections.



Specify the requirements that users must meet to connect to the TS Gateway server.

Supported Windows authentication methods:

☑ Password ☐ Smart card

If you select both methods, either can be used to connect.

For more information about Windows authentication methods, see the Windows Server 2008 Terminal Services TechCenter.

User group membership: (required)

BUILTIN\Administrators
REALTIME\Domain Users

Client computer group membership: (optional)

Summary of TS CAP settings:

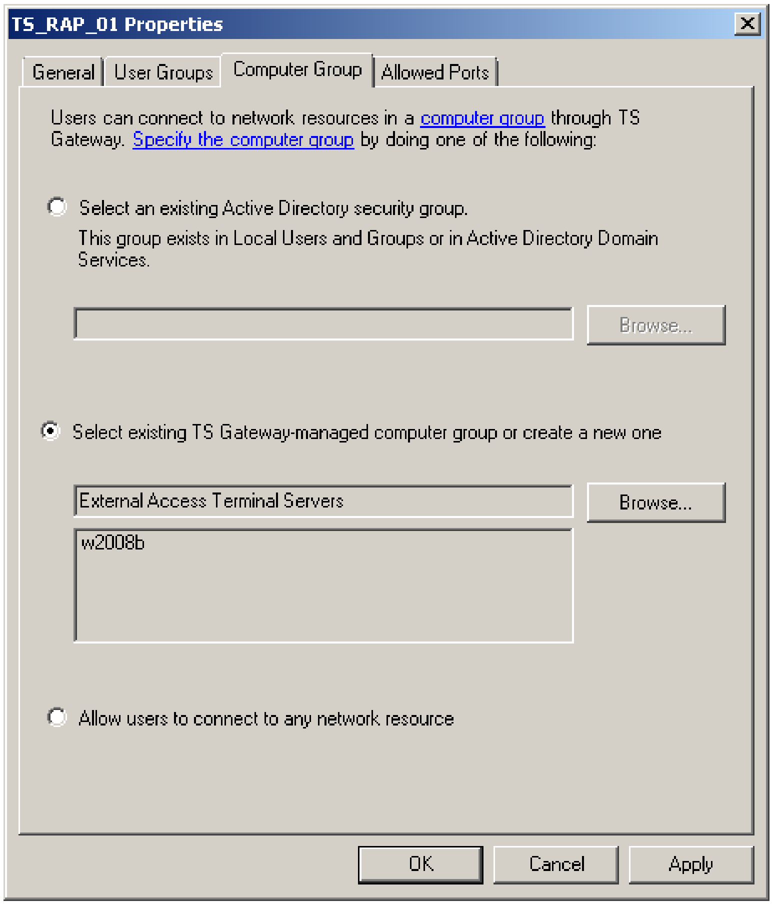
**If the user is a member of any of the following user groups:**
BUILTIN\Administrators, REALTIME\Domain Users
**and the client computer is a member of any of the following computer groups:**
Not applicable (No computer group is specified)

***Figure 8.9: The TS CAP identifies the user and computer groups that have access to connect to Terminal Server resources through the TS Gateway.***

- *Device redirection*. This tab allows or prevents specified types of device redirection to occur for connections made through the TS Gateway. The device redirection policy identified here will supersede any policies set at the individual Terminal Server. Setting device redirection here is useful for preventing users from downloading documents, printing, and using their local clipboard when they are outside the protected intranet.

In addition to verifying the TS CAP, we also need to ensure that the TS RAP is properly configured for external connections. Navigate to *TS Gateway Manager | {serverName} | Policies | Resource Authorization Policies* and double-click the policy (if present) to view four more tabs:

- *General.* As with the TS CAP, the General tab provides a location for changing the policy name as well as enabling or disabling the policy.
- *User Groups.* This tab identifies the user groups whose members are granted access to Terminal Services resources through the TS Gateway.
- *Computer Group.* Shown in Figure 8.10, once users have been authorized for connecting to Terminal Server resources, they are limited to connecting only to those computers identified in this tab. Computers can be selected via an Active Directory group, a local group that is managed by the TS Gateway itself, or all computers on the protected intranet.



Users can connect to network resources in a computer group through TS Gateway. Specify the computer group by doing one of the following:

○ Select an existing Active Directory security group.

This group exists in Local Users and Groups or in Active Directory Domain Services.

● Select existing TS Gateway-managed computer group or create a new one

External Access Terminal Servers

w2008b

○ Allow users to connect to any network resource

*Figure 8.10: The TS RAP identifies which resources on the protected intranet can be accessed by authorized users.*

- *Allowed ports.* By default, all traffic inbound to a Terminal Server is received on port TCP/3389. However, for some high security environments or in other situations it may be desired to change this to an alternate port. This tab configures the TS Gateway to attempt connecting to these computers over specified alternate ports.

Don't forget that TS Gateway must have the appropriate network connectivity to an Active Directory Domain Controller in order to authenticate users. If you locate your TS Gateway server within your DMZ, those ports must be opened in order to enable this authentication to occur.

### *Configuring Terminal Services for TS Gateway*

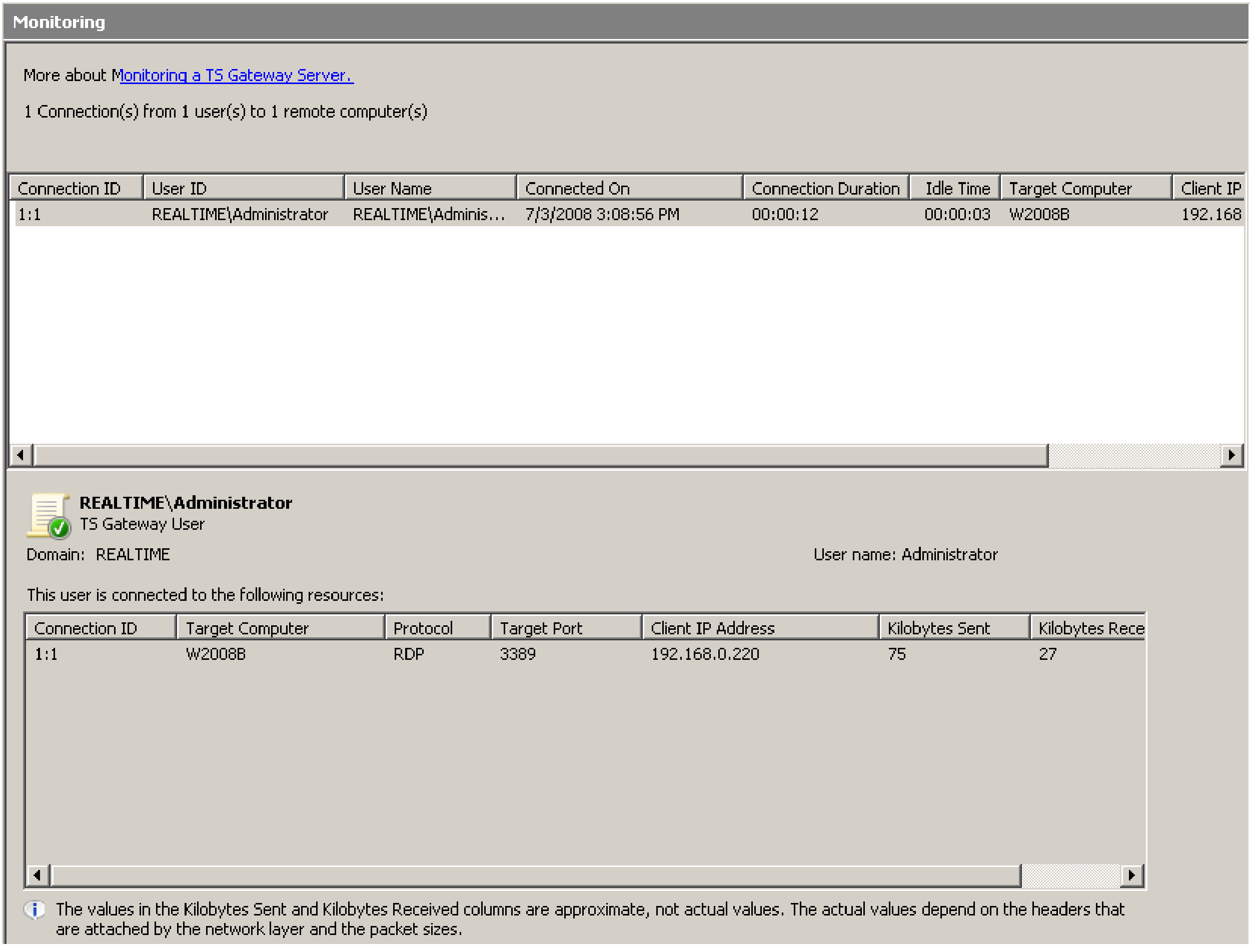
Once the TS Gateway is setup and ready for use, each client must be configured to use the TS Gateway. Any RDP files that were created prior to the TS Gateway configuration must be replaced or updated to include the correct TS Gateway connection information. This information can be supplied to the clients in one of two ways:

- *Manually supplying TS Gateway settings.* From the TS RemoteApp Manager node click the *Change* link next to *TS Gateway Settings*. In the resulting window enter the connection information for the TS Gateway server and set the assigned logon method assigned. Once credentials have been added, new RDP files must be created for clients to recognize that they will connect through the TS Gateway server.
- *Automatically detect TS Gateway server settings.* Alternatively, it is possible to use Group Policy as the mechanism for populating TS Gateway server settings. The Group Policy for doing this can be found within the GPME by navigating to *User Configuration | Policies | Administrative Templates | Windows Components | Terminal Services | TS Gateway*. Three policies are provided: *Set TS Gateway authentication method*, *Enable connection through TS Gateway*, and *Set TS Gateway server address*. The combination of these three policies, when applied to target machines, accomplishes the same as the manual steps above. Since the default configuration for supplying TS Gateway settings is to automatically detect settings, using this method may not require all RDP files to be recreated. This is because they may have been initially created with this default setting already enabled.

The last step in this process is to ensure that the TS Gateway's root certificate assigned at the beginning of this process has been added to the Trusted Root Certification Authorities certificate store on each of the clients that will connect through this TS Gateway server. This can be done either manually or using Group Policy.

Once complete, you can begin creating new RDP files that contain the necessary TS Gateway connection information and subsequently launch those file from external clients. It is possible to monitor Terminal Server connections going through the TS Gateway from within the TS Gateway Manager by navigating to the *{serverName} | Monitoring* node. If you've done everything right, the external client will connect to the Terminal Server resource supplied in the RDP file and the Monitoring node will include information about the connection similar to what is shown in Figure 8.11.

On the TS Gateway tab of the RemoteApp Deployment Settings wizard is a checkbox called Bypass TS Gateway server for local addresses. Ensure that this checkbox is not selected if you want to ensure that all traffic passes through the TS Gateway indifferent of its origin.



Monitoring

More about Monitoring a TS Gateway Server.

1 Connection(s) from 1 user(s) to 1 remote computer(s)

| Connection ID | User ID | User Name | Connected On | Connection Duration | Idle Time | Target Computer | Client IP |
|---|---|---|---|---|---|---|---|
| 1:1 | REALTIME\Administrator | REALTIME\Adminis... | 7/3/2008 3:08:56 PM | 00:00:12 | 00:00:03 | W2008B | 192.168 |

**REALTIME\Administrator**
TS Gateway User

Domain: REALTIME

User name: Administrator

This user is connected to the following resources:

| Connection ID | Target Computer | Protocol | Target Port | Client IP Address | Kilobytes Sent | Kilobytes Rece |
|---|---|---|---|---|---|---|
| 1:1 | W2008B | RDP | 3389 | 192.168.0.220 | 75 | 27 |

The values in the Kilobytes Sent and Kilobytes Received columns are approximate, not actual values. The actual values depend on the headers that are attached by the network layer and the packet sizes.

***Figure 8.11: If everything is set up correctly, the TS Gateway Manager's Monitoring node will show a successful connection.***

## TS Session Broker

Our last subject in this chapter helps with solving the problem of Terminal Server scalability. TS Session Broker is an update to the service previously called TS Session Directory in previous OS versions. TS Session Broker actually adds the functionality previously found in TS Session Directory to the clustering capabilities previously only found within Network Load Balancing clustering. Whereas the two individual services were required to operate together in previous OS versions, with TS Session Broker all the necessary components are built in.

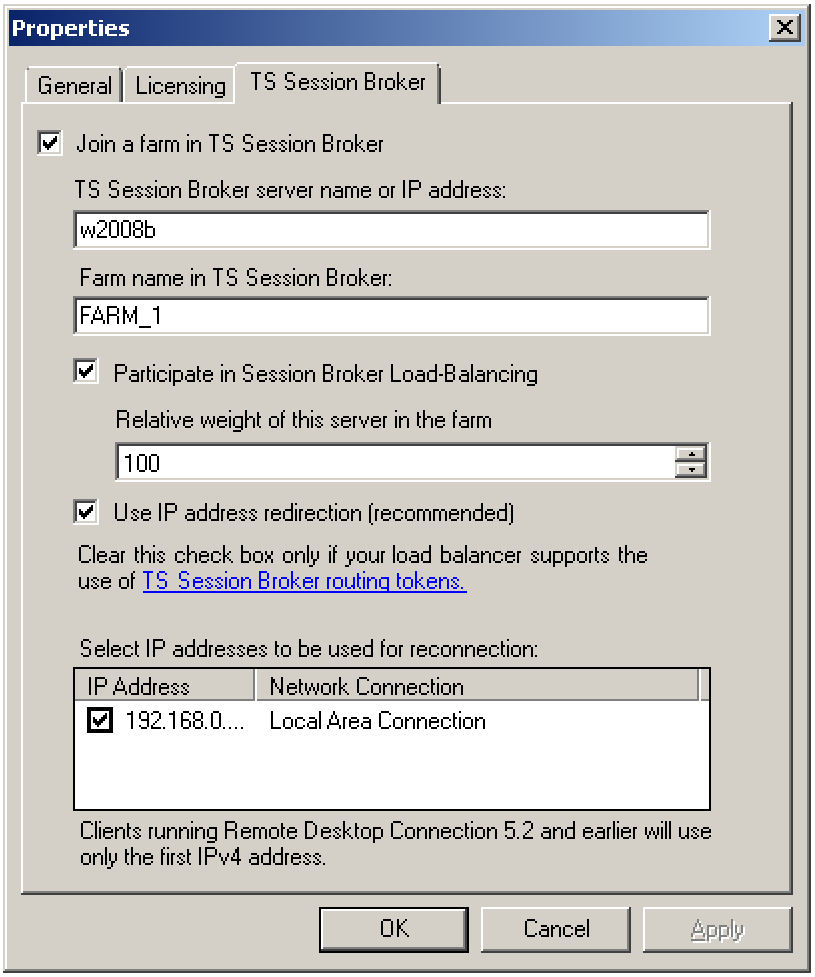
TS Session Broker is a rudimentary load balancing solution that enables multiple Terminal Servers to operate as a “farm”. Each Terminal Server must be identically configured with the exact same applications and configurations. TS Session Broker leverages either the native round robin DNS found in Windows Server 2008 or can use a third-party load balancer to handle balancing incoming client session requests. For servers that are not homogeneous in terms of hardware composition, TS Session Broker has the ability to weight servers in the farm. This has the result of sending fewer clients to servers that are less powerful. The end result is that servers in a TS Session Broker farm operate as a single unit, and clients are able to point to a single FQDN that takes them to one of many possible servers.

### Installing and Configuring TS Session Broker

TS Session Broker is installed to only one Terminal Server of those that will participate in the farm. Installing the *TS Session Broker* Role Service is completed in the same way we've installed each of the other Role Services thus far. Its installation through Server Manager has no initial questions that need to be answered as part of the installation. Once the installation is complete, there are a few steps that must be completed in order to aggregate a series of Terminal Servers into a farm:

1. *Build and configure Terminal Servers.* Prior to installing TS Session Broker to one of the farm members, build and configure the full set of Terminal Servers to be used in the farm. These servers must have the same set of applications as well as an identical configuration.
2. *Install TS Session Broker.* Install the Role Service to only one of the servers that will be a member of the farm. This server will handle monitoring inbound session requests and tracking session information across all servers in the farm.
3. *Add Servers to the correct group.* After installation, a new Local Group will be found on the TS Session Broker server named *Session Directory Computers*. Add the computer accounts for the computers that will participate in the farm to this Local Group. Once complete, the computers may require a reboot to recognize that they have been added to the group.
4. *Join Terminal Servers to the farm.* In Server Manager, navigate to *Terminal Services Configuration* and double-click the link titled *Member of farm in TS Session Broker*. A screen will appear similar to Figure 8.12. Check the box next to *Join a farm in TS Session Broker*. Provide the server name of the server which has had the TS Session Broker Role Service installed and provide a name for the farm to be created. Check the box next to *Participate in Session Broker Load Balancing* and provide a relative weight for this server. Lastly, determine if IP address redirection will be used and provide IP addresses to be used for redirection. Most networking equipment has the ability to support IT address redirection. The steps here will need to be done for each server that will participate in the farm.

> ✎ The absolute value of the number entered for relative weight is unimportant. What is important is the relative value of this number in comparison with the other numbers set in the farm. Thus, a server with a value of 50 will be sent half the number of clients than will a server with a value of 100.



Properties

General | Licensing | TS Session Broker

☑ Join a farm in TS Session Broker

TS Session Broker server name or IP address:

w2008b

Farm name in TS Session Broker:

FARM_1

☑ Participate in Session Broker Load-Balancing

Relative weight of this server in the farm

100

☑ Use IP address redirection (recommended)

Clear this check box only if your load balancer supports the use of TS Session Broker routing tokens.

Select IP addresses to be used for reconnection:

| IP Address | Network Connection |
|---|---|
| ☑ 192.168.0.... | Local Area Connection |

Clients running Remote Desktop Connection 5.2 and earlier will use only the first IPv4 address.

***Figure 8.12: TS Session Broker enables multiple Terminal Servers to operate as a single unit.***

5. *Enable DNS round robin.* If you will not be using a third-party load balancing solution for handling the load balancing portion, you will need to create a round-robin entry in Windows Server 2008 DNS to accomplish this portion. To enable this, create an A or AAAA record named after the farm name that includes each IP address for each server that will participate in the farm.

Once complete, reconfigure any RDP files to point to the farm name rather than an individual Terminal Server. TS Session Broker will ensure that clients are sent to servers as is appropriate based on the relative weighting configured for that server. Additional specifics about the configuration of TS Session Broker can be found at http://technet2.microsoft.com/windowsserver2008/en/library/8aa35e7d-bcff-4998-8ac2-6a8c5702c4161033.mspx?mfr=true.

## Terminal Services in Windows Server 2008 Narrows the Gap

The gap between the functionality previously only available with third-party products like those from Citrix grows a little closer with the release of Windows Server 2008. With Terminal Services in this new operating system (OS), a number of the long-desired features and capabilities have been folded into the native Windows OS for no extra charge. While there remains a compelling justification to move to the Citrix product lineup for environments that require its added management functionality and high-end capabilities for users, Terminal Services gains a lot in the transition. The topics discussed in this chapter bear out that statement. Your mileage will vary.

After two chapters on this topic, we shift gears in Chapter 9 to talk about securing our new servers along with the domain. There, we'll discuss the new and improved security features that you'll find in Windows Server 2008, as well as some controversial ones like User Account Control and the Windows Firewall with Advanced Security. Windows Server 2008 is reported to be the most secure OS Microsoft has released to date. In our next chapter, we'll discover exactly how and why.

## Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.