

Deployment Guide

**Deploying Microsoft Windows Terminal Services  
and F5's FirePass Controller**



---

# Introducing the FirePass and Windows Terminal Services configuration

Welcome to the FirePass and Microsoft® Windows® Terminal Services Deployment Guide. This guide shows you how to configure F5's FirePass controller for secure remote access to Microsoft Windows Terminal Services.

Microsoft Terminal Services lets you deliver Windows-based applications, or the Windows desktop itself, to virtually any computing device, including those that cannot run Windows.

F5's FirePass® controller is the industry leading SSL VPN solution that enables organizations of any size to provide ubiquitous secure access for employees, partners and customers to applications such as Microsoft Windows Terminal Services, while significantly lowering support costs associated with legacy client-based VPN solutions.

For more information on Microsoft Terminal Services, see <http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx>

For more information on the FirePass controller, see <http://www.f5.com/products/firepass/>.

## Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The FirePass controller should be running version 5.4.2 or later.
- ◆ This deployment was tested using Microsoft Windows Server 2003 and 2000 Terminal Services.
- ◆ All of the configuration procedures in this document are performed on the FirePass controller. For information on how to deploy or configure the Windows Server 2003, see the appropriate Microsoft documentation.
- ◆ This configuration uses previously defined Active Directory groups to provide authentication and simple user maintenance. For information on how to configure Active Directory groups, consult the proper documentation.
- ◆ Briefly review the basic configuration tasks and the few pieces of information, such as IP addresses, that you should gather in preparation for completing this configuration.

- ◆ This Deployment Guide is written to the scenario outlined in the following section. It is meant as a template; modify the configuration as necessary for your deployment.

◆ **Note**

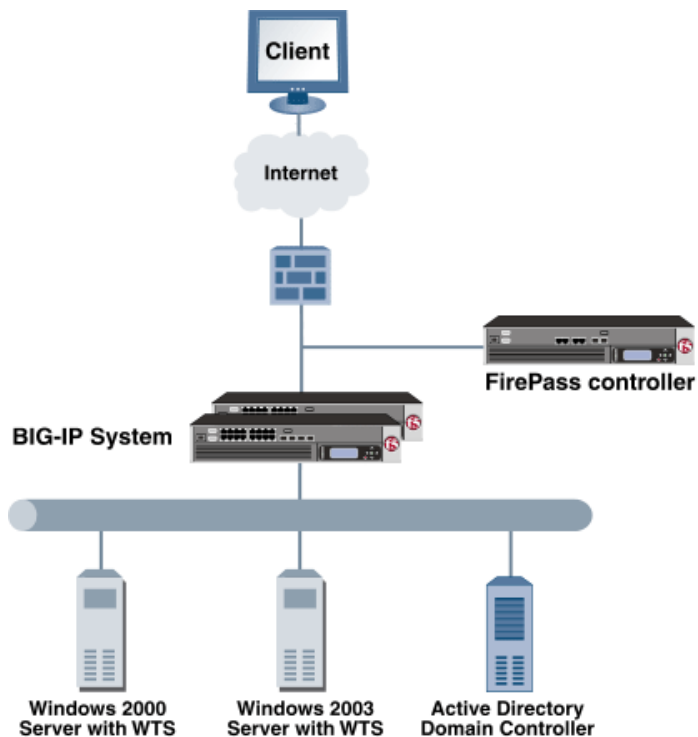
*This document is written with the assumption that you are familiar with both the FirePass controller and Windows Terminal Services. For more detailed information on these products, consult the appropriate documentation.*

## Configuration scenario

For the scenario used in this Deployment Guide, the Microsoft Terminal Services deployment, along with an Active Directory instance, resides behind a BIG-IP system. A single group on the FirePass controller is given access to Windows Terminal Servers on the corporate network.

This Deployment Guide describes how to configure the FirePass controller to allow secure remote access to the Windows Terminal Services device(s), using the Active Directory for authentication. In our deployment, the FirePass device and the Windows servers use a common Active Directory Domain Controller. This guide also contains procedures on configuring some endpoint security features, including antivirus checks.

The following figure is a logical representation of our deployment.



*Figure 1.1 FirePass WTS logical configuration*

---

# Configuring the FirePass controller for deployment with Windows Terminal Services

To configure the FirePass controller for allowing secure remote access to the Windows Terminal Services deployment, you need to complete the following procedures:

- *Connecting to the FirePass controller*
- *Creating groups on the FirePass controller*
- *Configuring Windows Terminal Services through the FirePass device*
- *Configuring access to a single application on the terminal server*
- *Configuring single sign-on for the FirePass WTS deployment*
- *Configuring Endpoint security*

## Connecting to the FirePass controller

To perform the procedures in this Deployment Guide you must have administrative access to the FirePass controller.

To access the Administrative console, in a browser, type the URL of the FirePass controller followed by **/admin/**, and log in with the administrator's user name and password.

Once you are logged on as an administrator, the Device Management screen of the Configuration utility opens. From here, you can configure and monitor the FirePass controller

## Creating groups on the FirePass controller

In this configuration, we configure two types of groups on the FirePass controller, Resource and Master groups. **Master groups** contain user information, including details about authentication methods. **Resource groups** contain information about applications (resources) that are available to FirePass controller users.

## Creating a Resource group

Resource groups allow you to preconfigure specific applications and access by group, and assign the group to a master group or an individual user. For this configuration, we create a single resource group for employees.

### ◆ Tip

---

*If you already have a resource group configured on the FirePass controller for employees, you can use that group and this procedure.*

### To configure a resource group

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.
2. Click the **Create new group** button.  
The Group Management - Create New Group screen opens.
3. In the **New group name** box, type a name for your group and click the **Create** button. In our example we type **employees\_wts**. The new group appears on the Resource Groups table.

### Creating a Master group

FirePass controller master groups are composed of users, authentication methods, and security and policy information. The next task is to create a Master group that will use the resource group we just created.

### To create a new Master Group

1. From the Administrative Console navigation pane, click **Users**, and expand **Groups**.  
The Master Groups screen opens.
2. Click the **Create new group** button.  
The Group Management Create New Group screen opens.
3. In the **New group name** box, type the name of your group. In our example we type **wtsAD**.
4. In the **Users in group** box, select **External**.
5. From the Authentication method list, select **Active Directory**.
6. In the **Copy settings from** list, make sure **Do not copy** is selected (see Figure 1.2).
7. Click the **Create** button.  
The General tab of the new Master Group displays.

Users : Groups : Master Groups	
<b>Group Management</b>	
<b>Create New Group</b>	
New group name:	<input type="text" value="wtsAD"/>
Users in group:	<input type="text" value="External"/>
Authentication method:	<input type="text" value="Active Directory"/>
Copy settings from :	<input type="text" value="Do not copy"/>
<input type="button" value="Cancel"/> <input type="button" value="Create"/>	

*Figure 1.2 Creating a new Master Group*

- 
8. Click the Resource Groups tab.  
The Resource Groups screen opens.
  9. From the **Available** box, select the name of the Resource group you created in the *Creating a Resource group* section. In our example, we select **employees\_wts**.
  10. Click the **Add** button to move the group to the **Selected** box, and click the **Update** button. The Resource group is now associated with the Master group.

## Configuring the Master group for Active Directory authentication

The next step is to configure the Master group to use Active Directory authentication.

### To configure the FirePass Master group to use Active Directory Authentication

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Master Groups**.
2. Click the name of the Master group you created in the *Creating a Master group* section. In our example, we select **wtsAD**.
3. Click the Authentication tab.  
The Active Directory Authentication tab opens.
4. In the Configure Active Directory Settings section, configure the appropriate settings for your Active Directory deployment. Type the fully qualified domain name in the **Domain name** box, and IP addresses or DNS names for the Kerberos and WINS servers in their respective boxes.
5. Click the **Save Settings** button.

Users : Groups : Master Groups      Realm: Full access      Help ?      Ask      Logout

Master Group: wtsAD      [Back to group list >>](#)

---

General      **Authentication**      Resource Groups      Signup Templates      User Experience

**Active Directory Authentication**

[Convert authentication method >>](#)

Configure Active Directory Settings	
Domain name:	DEMO.COMPANY.COM
Kerberos server name (optional):	demo.company.com
WINS server IP address (optional):	10.10.100.210
Require user logon in form DOMAIN\username:	<input type="checkbox"/>
User must belong to Domain group (optional):	

[Select Domain group >>](#)

Domain admin name:	administrator
Domain admin password:	•••••

*Figure 1.3 Active Directory Authentication settings*

6. Click **Select Domain Group**.  
The Active Directory Authentication screen opens.  
**Important:** Be sure you have entered the **Domain admin name and password** and saved the settings before clicking **Select Domain Group**.
7. From the list, select the Active Directory Domain group the user must belong to in order to authenticate, and click the **Select Group** button (see Figure 1.4).
8. Click the **Save Settings** button again. You can also click the **Test Saved Settings** button to test the configuration.

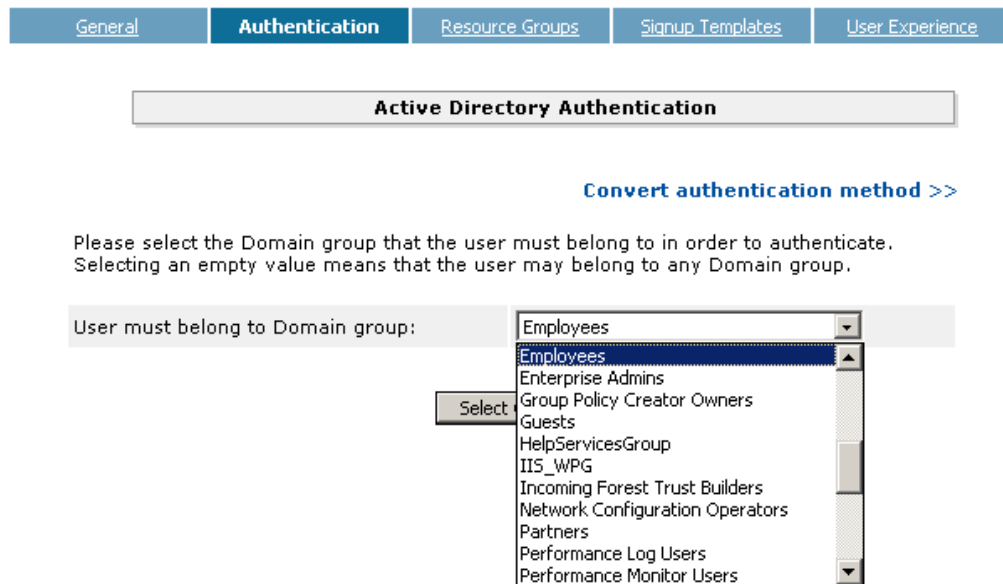


Figure 1.4 Selecting the Active Directory Domain Group

## Configuring Windows Terminal Services through the FirePass device

In the following procedures, we show two ways to give secure remote access to Windows Terminal Services servers. In the first procedure, we use the Application Access feature to give complete access to the WTS device and the applications running on it.

In the second procedure, we configure an application tunnel on the FirePass to a specific application running on the Terminal Server.

### To configure Windows Terminal Services through the FirePass

1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.
2. From the Resource Groups table, find the row with the name of the Resource group you created in the *Creating a Resource group* section (**employee\_wts** in our example). In this row, from the **Application access** column, click **Edit** (see Figure 1.5). The App Tunnel tab of the Resource Group page opens.

Users : Groups : Resource Groups				
Resource groups				
Group Name	Network access	Portal access	Application access	Role
Default_resource	<a href="#">Edit</a>	<a href="#">Edit</a>	<a href="#">Edit</a>	
DemocenterUsers	<a href="#">Edit</a>	<a href="#">Edit</a>	<a href="#">Edit</a>	
employees_email	<a href="#">Edit</a>	<a href="#">Edit</a>	<a href="#">Edit</a>	

Figure 1.5 The Resource groups table

3. Click the Terminal Servers tab.  
The Terminal Server Favorites screen opens.
4. Click **Add New Favorite**.  
The Favorite configuration options display.
5. Type a name for the Favorite. In our example, we type **Windows Terminal Server**. This Favorite link only displays for members of the Employee group.
6. In the **Host** box, type the host name or IP address.  
This can also be the Virtual Server address that is load balancing a Terminal Server cluster.
7. In the Port section, from the **Default for** list, select **Microsoft Terminal Server**. The Port box is automatically populated.
8. If connecting to a Windows 2003 server, clicking a check in the **Redirect local resources** box causes the FirePass device to map local disk drives, printers and other resources, in a similar manner to Windows Remote Desktop.  
***Important:** This feature is only supported for Win2003 Terminal Server.*
9. The rest of the settings are optional, configure them applicable to your deployment, and then click the **Update** button (see Figure 1.6).  
The new Favorite is added to the list.

---

Resource Group:  [Back to group list >>](#)

[App Tunnels](#) | [Legacy Hosts](#) | **Terminal Servers** | [X11](#)

**Terminal Server Favorites**

[Add New Favorite](#)

<b>Type:</b>	<input type="text" value="Favorite"/>
<b>Name:</b>	<input type="text" value="Windows Terminal Server"/>
<b>Host:</b>	<input type="text" value="10.10.100.5"/>
<b>Port:</b>	<input type="text" value="3389"/> <input type="text" value="Microsoft Terminal Server"/>
<b>Select a program:</b>	<input type="text"/>
<b>Working Dir:</b>	<input type="text"/>
<b>Open in new window:</b>	<input checked="" type="checkbox"/>
<b>Redirect local resources (drives, printers, COM ports):</b>	<input checked="" type="checkbox"/>
<b>Encryption (Citrix-only):</b>	<input type="text" value="Basic (default)"/>
<b>Color Depth:</b>	<input type="text" value="256 Colors (default)"/>
<b>Endpoint protection required:</b>	<input type="text"/>
	<input type="button" value="Add New"/>

*Figure 1.6 Adding a Terminal Server Favorite to the Resource group*

## Configuring access to a single application on the terminal server

In this procedure, we configure an application Favorite that launches a specific application on the terminal server. In the following example, we use MS paint as the application we are launching.

### To configure access to a single application on the terminal server

1. From the navigation pane, click **Application Access**, expand **Terminal Server**, and then click **Resources**. The Terminal Server Favorites screen opens.
2. Click **Add New Favorite**.
3. In the **Name** box, type a meaningful name for the Favorite. In our example, we type **MS Paint**.
4. In the **Host** box, type the host name or IP address. This can also be the Virtual Server address that is load balancing a Terminal Server cluster.
5. In the Port section, from the **Default for** list, select **Microsoft Terminal Server**. The Port box is automatically populated.

6. In the **Select a Program** box, type the full path to the application on the server. In our example, we type:  
**%SystemRoot%\System32\mspaint.exe.**
7. If necessary for the application, in the **Working Dir** box, type the working directory for the application. In our example, we type:  
**C:\WINDOWS\System32.**
8. Configure the rest of the options as applicable for your deployment.
9. Click the **Add New** button.

You can optionally configure the FirePass device to limit access to the terminal server to only administrator configured favorites, like the one above. This access is configured on a Master Group level, so if you do not want all users in your Master Group limited in this way, you may first need to configure additional Master and Resource Groups.

### **To limit terminal server access only to administrator-defined favorites**

1. From the navigation pane, click **Application Access**, expand **App Tunnels**, and then click **Master Group Settings**.
2. From the Master Group list, select the name of the group you created in the *Creating a Master group* section. If you created a new Master group for this feature, use that Master group.
3. Ensure there is a check in the **Limit AppTunnels Access to Favorites only (for Extranets, partner and customer access, etc.)** box.

This prohibits the creation of custom favorites and limits access to App Tunnels that are defined by the administrator.

## Configuring single sign-on for the FirePass WTS deployment

Allows auto-login (single sign-on) to the terminal servers with user's FirePass credentials. In our scenario, we configure this option to allow single sign-on.

### **To configure single sign-on for the deployment**

1. From the navigation pane, click **Application Access**, expand **Terminal Server**, and then click **Master Group Settings**.
2. From the Master Group list, select the name of the group you created in the *Creating a Master group* section.
3. Click a check in the **Auto-login to applicable Terminal Servers using FirePass user login credentials** box.  
The Domain/Workgroup box appears.

- 
4. Type the default domain as applicable for your configuration and click the **Update** button.

## Configuring Endpoint security

One of the new security features in the 5.4.2 release of the FirePass controller is the ability to set endpoint security on an extremely granular level. For this Deployment Guide, we illustrate how to configure a pre-logon sequence for inspections before a user logs on. For more information on endpoint security, see the online help.

### Pre-logon sequence

The pre-logon sequence allows administrators to create one or more sequences of inspections for items such as installed antivirus programs or OS patch levels. For this Deployment Guide, we configure a Windows Antivirus Checker.

#### To configure a pre-logon sequence

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Pre-Logon Sequence**.
2. In the New Sequence section at the bottom of the page, type a name for the sequence in the **Create New Sequence** box. In our example, we type **wtsBasic**.
3. From the **Based on** list, select **template: Collect information with no pre-logon actions**.
4. Click the **Create** button.  
The new sequence appears in the Select Sequence to Use table.
5. In the row of the sequence you just created, click the **Edit** button.

***Important** - Do not click the radio button next to the sequence yet. If you click the radio button, the **Edit** link will be replaced with the **View** link, and you are not able to edit the sequence.*

The Pre-Logon Sequence Editor opens.

6. Move the cursor between **Sequence Start** and **Logon Allowed Page**. An add [+] link appears on the arrow (see the circle marked 1 in Figure 1.7). Click the Add link.  
The Change Sequence panel appears on the right.
7. Click the **Check for Antiviruses** option button, and click the **Apply Changes** button.  
The Edit Action panel opens.

***Note:** The Check for Antiviruses is an optional feature on the FirePass controller. If your device does not have this license, you will not see this option.*

8. Under **Inspectors**, click **Windows Antivirus Checker**.  
The Endpoint Inspector Details page opens in a new window.
9. Configure these options as applicable for your deployment. For more information, click **Help**.
10. Click the **Update** button.
11. In the Sequence pane, find **AV installed**, and click the associated Logon Denied Page link (see the circle marked 2 in Figure 1.7).  
The End Page Properties pane appears on the right.
12. From the Type box, select **Logon Allowed Page**. This allows a user to logon if they have an antivirus checker installed. You can optionally type a message for failed logons.
13. **Optional:** You can click the Logon Allowed Page or Logon Denied Page links for the other options to produce a custom message when a user is denied access. You can also change the actions taken as a result of the virus checker's findings. For example, you might still want to allow a user to login if there is virus checking software installed, but not currently running.

In our example, we click **Logon Denied Page** next to **Virus Detected**, and type a message informing the user there is a virus on their computer.

14. When you are finished, click **Back to Console** in the upper right corner of the screen (see the circle marked 3 in the following figure).  
You return to the Pre-Logon Sequence main page.

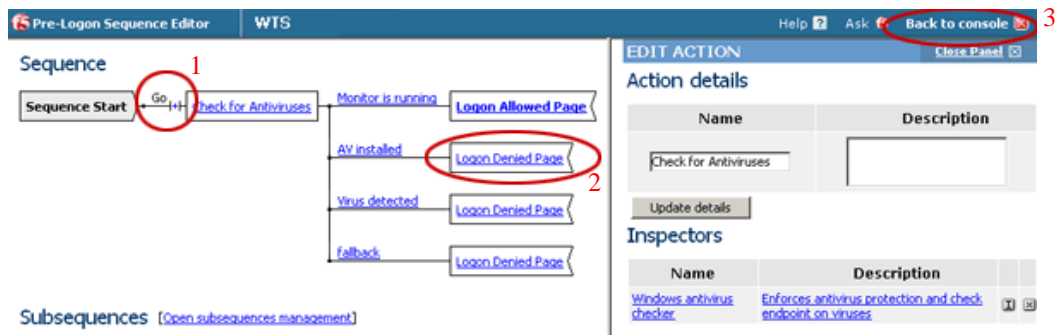


Figure 1.7 The Pre-Logon Sequence Editor

15. From the **Select Sequence to Use** section, click the option button next to the sequence you just created. In our example, we click **wtsBasic**.
16. Click the **Apply** button.

---

## Conclusion

The FirePass controller is now configured to allow secure remote access to the Windows Terminal Services deployment. Remember that the procedures in this Deployment Guide are specific to the scenario described in *Configuration scenario*, on page 1-2. Use this guide as a template, and modify the configuration as applicable to your deployment.