Deployment Guide

Deploying Microsoft SharePoint Portal Server and F5's FirePass Controller

Introducing the FirePass and SharePoint Portal Server configuration

Welcome to the FirePass SharePoint Deployment Guide. This guide shows you how to configure F5's FirePass controller for secure remote access to Microsoft® SharePoint® Portal Server deployments. Microsoft SharePoint Portal Server enables enterprises to develop an intelligent portal that seamlessly connects users, teams, and knowledge so that people can take advantage of relevant information across business processes to help them work more efficiently.

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 SharePoint Portal Server, while significantly lowering support costs associated with legacy client-based VPN solutions.

For more information on the Microsoft SharePoint Portal Server, see **http://www.microsoft.com/office/sharepoint/prodinfo/default.mspx.**

For more information on the FirePass controller, see **http://www.f5.com/f5products/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 SharePoint Portal Server 2003, load balanced by a BIG-IP system.
  For information on how to deploy the BIG-IP system with SharePoint Portal Server, see
  http://www.f5.com/solutions/deployment/sharepoint_dg.html
- All of the configuration procedures in this document are performed on the FirePass device. For information on how to configure the SharePoint Portal Server, consult 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 Microsoft SharePoint. For more detailed information on these products, consult the appropriate documentation.

Configuration scenario

For the scenario used in this Deployment Guide, the Microsoft SharePoint deployment, along with an Active Directory instance, resides behind a BIG-IP system. There is a requirement to allow employees remote access to all internal resources using the FirePass device. There is also a requirement for trusted partners to access the SharePoint deployment, although only to a limited subset of the portal, with no other access.

This Deployment Guide describes how to configure the FirePass controller to allow secure remote access to the SharePoint device(s), using Active Directory for authentication and how to configure the FirePass to give one group of users full access, and restrict users in the partner group to a certain directory. In our deployment, the FirePass device and the SharePoint deployment use a common Active Directory Domain Controller. This guide also contains procedures on configuring some endpoint security features, including antivirus checks.

Figure 1.1 shows a logical representation of this configuration.

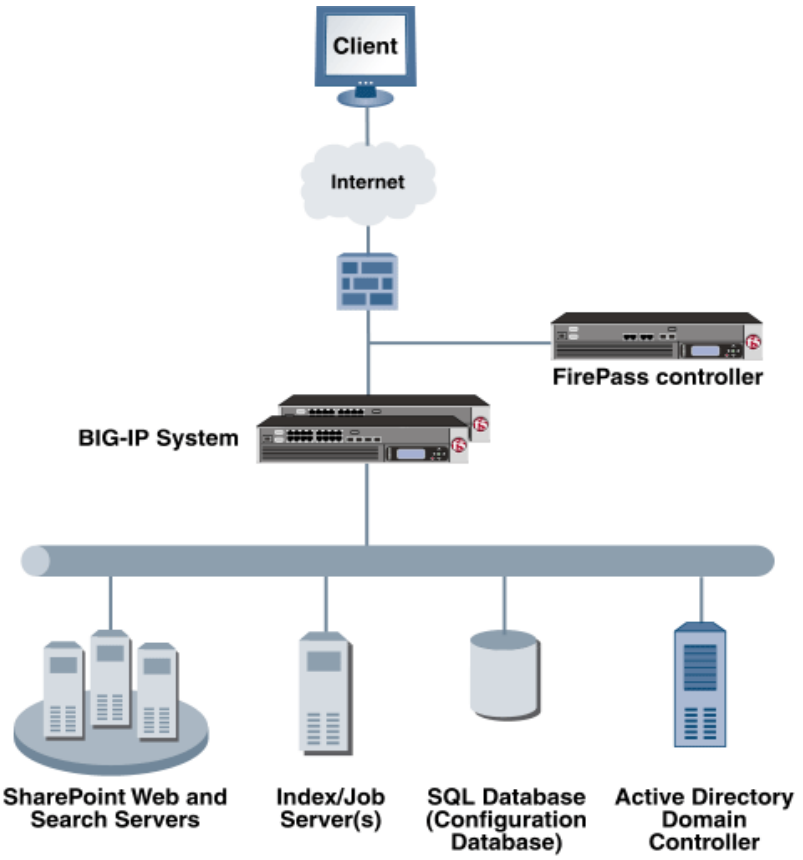

Figure 1.1 *FirePass SharePoint logical configuration*

Configuring the FirePass controller for deployment with SharePoint Portal Server

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

- *Connecting to the FirePass controller*
- *Creating groups on the FirePass controller*
- *Limiting access for the Partner group*
- *Configuring auto-logon*
- *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 the Resource groups

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 two resource groups, one for employees and one for partners, in order to create different Favorite links to the SharePoint deployment.

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_SP**. The new group appears on the Resource Groups table.
4. From the Resource Groups table, find the row with the name of the group you just created. In this row, from the Portal access column, click **Edit** (see Figure 1.2). The Web Applications section of the Resource Group page opens.

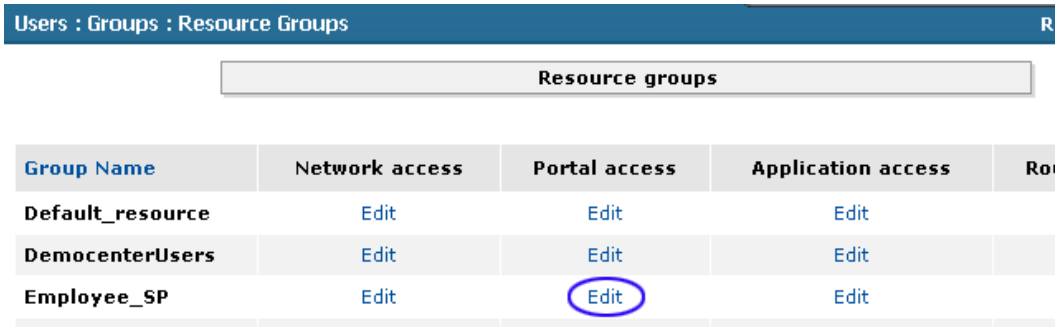

Figure 1.2 *The Resource groups table*

5. Under Web Application Favorites, click **Add New Favorite**. The Favorite options display.
6. Type a name for the Favorite. In our example, we type **SharePoint - Employee Access**. This Favorite link only displays for members of the Employee group.
7. In the URL box, type the URL used to access the SharePoint deployment. If you are using a BIG-IP system in front of the SharePoint deployment, this URL should point to the SharePoint virtual server address. In our example, we type **http://sharepoint.company.com/default.aspx**.
8. Configure the rest of the settings as applicable to your deployment.
9. Click the **Add New** button. The new Favorite is added to the list. (see Figure1.3)

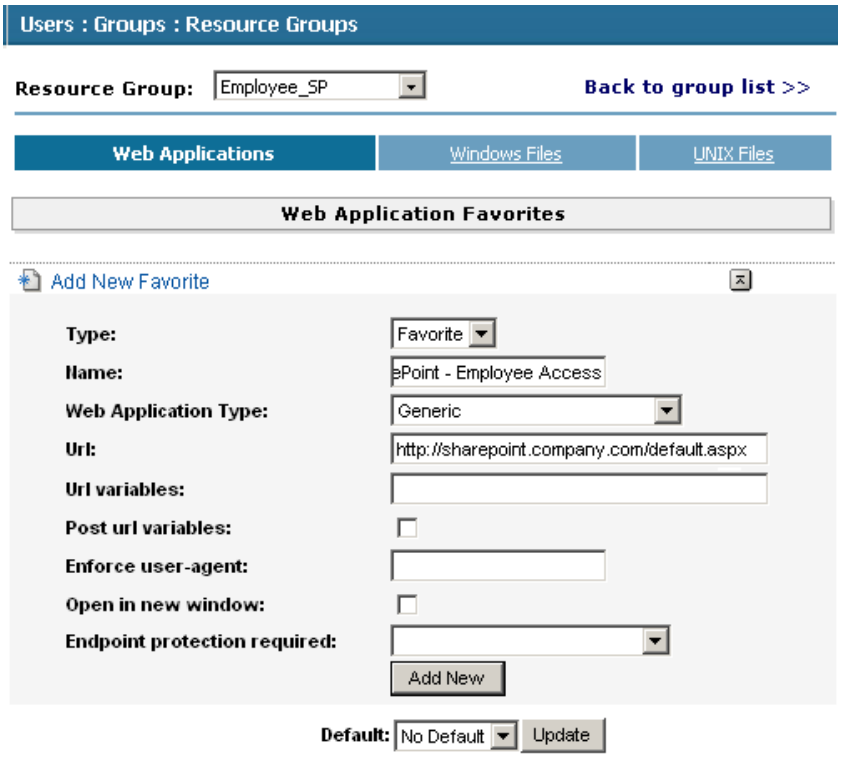

Figure 1.3 *Adding a Web Application Favorite to the Employee group*

10. Repeat this procedure for the **Partner** resource group, typing appropriate names for the group and the Favorite. In step 7, type the path to the appropriate section of the SharePoint deployment that Partners are entitled to access.
    For example, the employee Favorite might point to **http://sharepoint.company.com/default.aspx**, while the partner Favorite would point to **http://sharepoint.company.com/sites/partners/default.aspx**

Creating the Master groups

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

To create a new Master Group

1. From the navigation pane, click **Users**, and expand **Groups**.
   The Master Groups list 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 **SharepointAD**.
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 1.4).
7. Click the **Create** button.
   The General tab of the new Master Group displays.

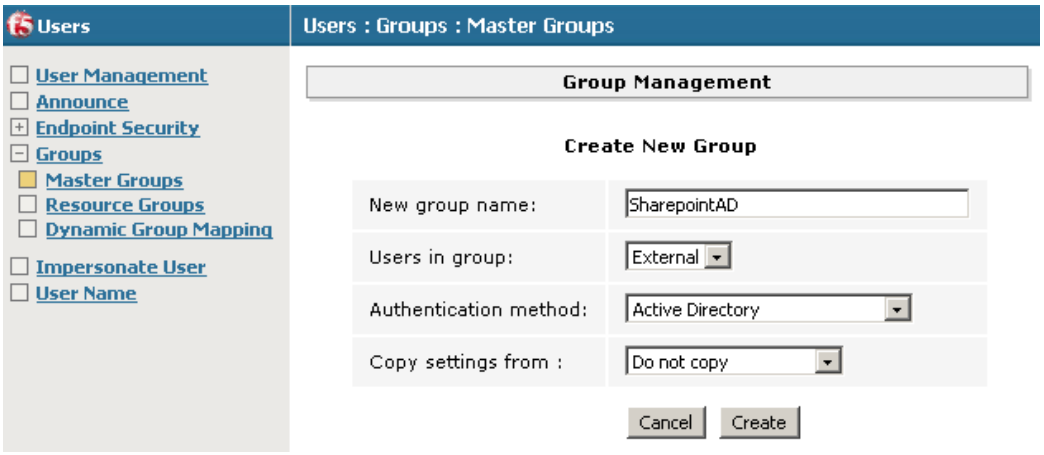

Figure 1.4 *Creating a new Master Group*

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 the Resource groups* section. In our example, we select **Employees_SP**.
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 the Master groups* section. In our example, we select **SharepointAD**.

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 (Domain Controller) and WINS servers in their respective boxes.
5. Click the **Save Settings** button.

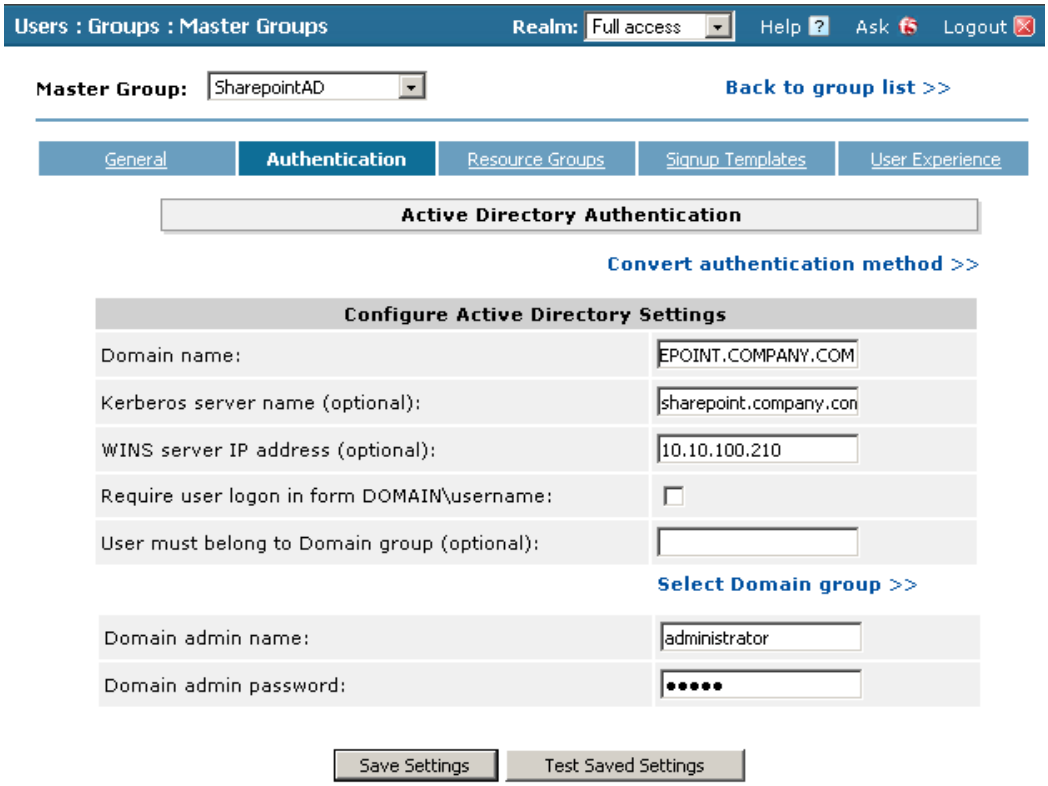

Figure 1.5 *Active Directory Authentication settings*

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 1.6).
8. Click the **Save Settings** button again. You can also click the **Test Saved Settings** button to test the configuration.

9. Repeat this procedure to create a Master group for the Partners. In our example, we name the group **SharepointADPartners**. Be sure to select the appropriate Active Directory Domain group in step 13.

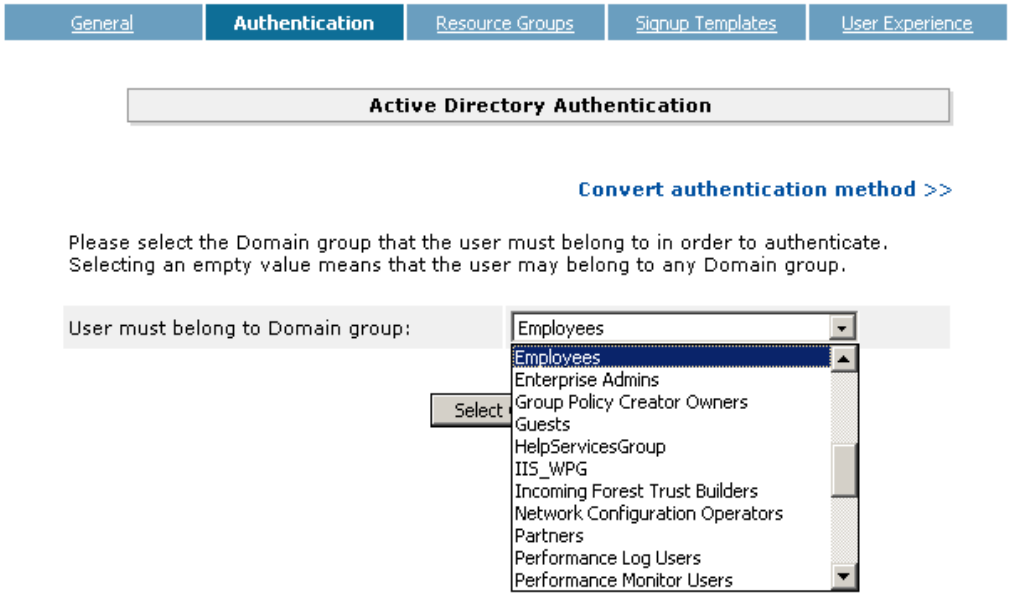

Figure 1.6 *Selecting the Active Directory Domain Group*

Limiting access for the Partner group

The FirePass controller allows you to limit access for specific groups on a very granular level. In this scenario, we limit access for the Partner group to only the Favorite we configured earlier, as well as restricting the areas of SharePoint they can access by URL.

To limit access for the Partner group

1. From the navigation pane, click **Portal Access**.
2. Under Web Applications, click **Master Group Settings**.
3. From the **Master Group** list at the top of the page, select the Master Group you created in the *Creating the Master groups* section. In our example, we select **SharepointADPartners**.
   The configuration settings for the Master group open.
4. In the **Access limitation** section, make sure there is a check in the **Limit Web Applications Access to Intranet Favorites only,...** box.
5. In the Accessibility Scope, click a check in the **Restrict resources accessible via Web Applications** box.
   Allow and Deny text boxes display.

6. Configure URL pattern matches to allow and deny based on your deployment. In our example, we type the following (separated by commas) in the **Allow** box to restrict the Partner group to these areas of our SharePoint deployment:

   /_vti*bin/*,*/sites/partners/*,*/_layouts/*,*/MySite/

   We leave the **Deny** box blank, which allows access to all URLs that pass the allow test (see Figure 1.7).
   For more information on configuring the Accessibility Scope, see the online help.

7. Click the **Update** button.

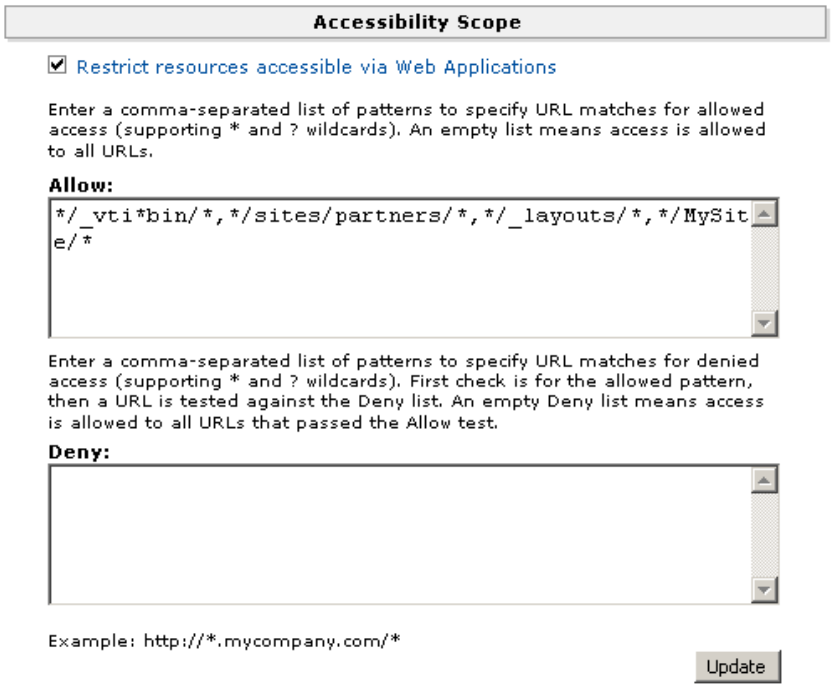

Figure 1.7 *Restricting access to the SharePoint deployment*

Configuring auto-logon

The FirePass device allows auto-logon (single sign-on) to sites supporting basic or NTLM authentication with user's FirePass credentials. In our scenario, we configure this option to allow single sign-on (SSO).

To configure SSO/NTLM for auto-login

1. From the navigation pane, click **Portal Access**.
2. Under Web Applications, click **Master Group Settings**.

3. From the **Master Group** list at the top of the page, select the Master Group you created in the *Creating the Master groups* section. In our example, we select **SharepointAD**.
   The configuration settings for the Master group open.
4. In the **NTLM and Basic Auth Proxy** section, click a check in the **Auto-login to Basic and NTLM auth protected sites using FirePass user credentials** box.
   The NTLM and Basic Auth domain boxes display.
5. In the **NTLM Auth Domain (optional)** box, you can type the default Domain to be used in conjunction with the auto-login support.
6. In the **Basic Auth Domain (optional)** box, you can type the default Domain to be used in conjunction with the auto-login support. When specified, this value is prepended to the user name in the during Basic authentication (for example MYDOMAIN\username).
7. Click the **Update** button.

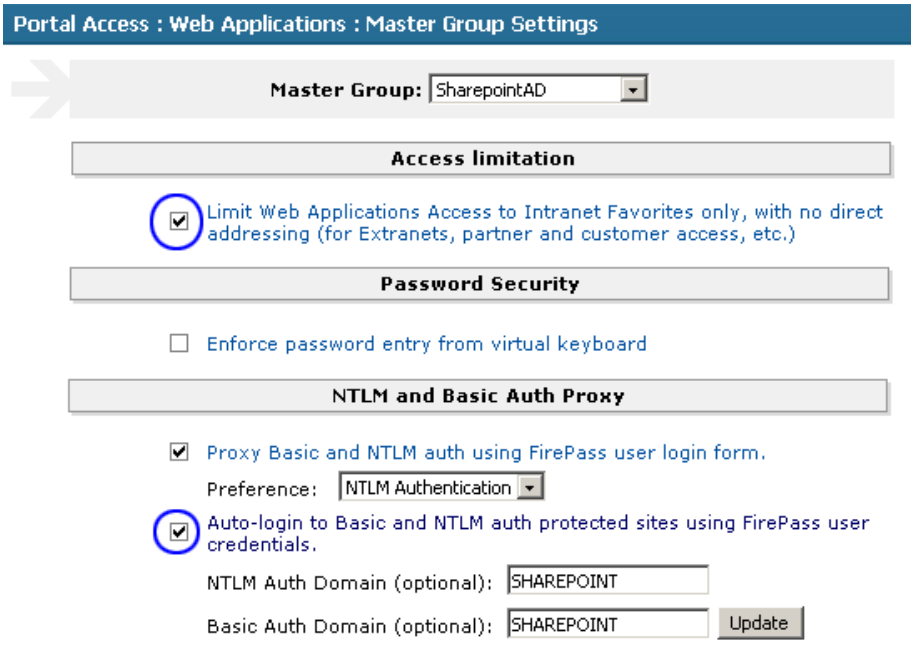

Figure 1.8 *Configuring NTLM Master Group Settings*

8. Repeat this procedure for the other Master group. In our example, we select **SharepointADPartners** from the **Master Group** list.

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 a extremely granular level.

In the following procedures, we configure a pre-logon check for anti-virus software on Windows machines. The FirePass controller uses this information to deny SharePoint access for members of the Partner Resource group if they do not have the appropriate software. In this configuration example, the FirePass device also denies access to *any* client that is determined to have a virus.

For more information on endpoint security, see the online help.

Creating a 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.

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 **sharepointBasic**.
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 curser between **Sequence Start** and **Logon Allowed Page**. An add **[+]** link appears on the arrow (see the circle marked **1** in Figure 1.9). Click **Add**.
   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 1.9).
    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. Repeat steps 11 and 12 for the **Fallback** option.
14. ***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.
15. 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.

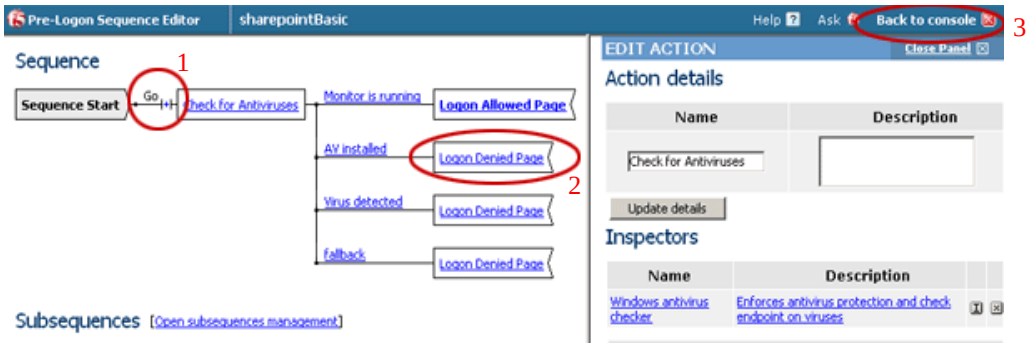

Figure 1.9 *The Pre-Logon Sequence Editor*

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

Protected Configurations

Protected Configurations allow administrators to specify the criteria the endpoint systems must meet to enable access to the various resources**.** In this procedure, we create a protected configuration for the partner group in order make additional security requirements for that group.

To configure Protected Configurations

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protected Configurations**.
2. Click **New Protection Configuration**.
3. In the Protected configuration ID box, type a name for this configuration. In our example, we type **Partner_config**. You can optionally type a description.
4. Leave the Mode list at the default setting, **Check endpoint protection, grant access if check passed** (see Figure 1.10).

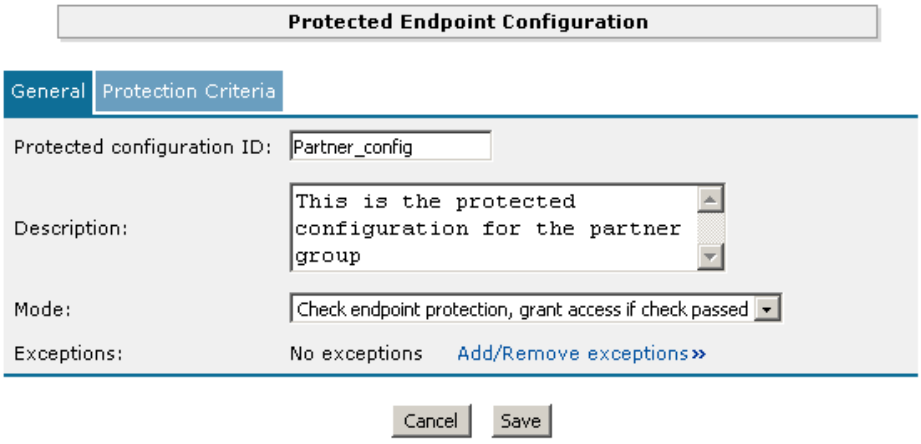

Figure 1.10 *The General tab of the Protected Endpoint Configuration screen*

5. Click the Protected Criteria tab.
6. On the menu bar, click **Information Leaks**.
7. From the Required safety measures or checks list, select **Cache Cleaner** and click the **Add** button. This will remove content from the cache when a user logs off.

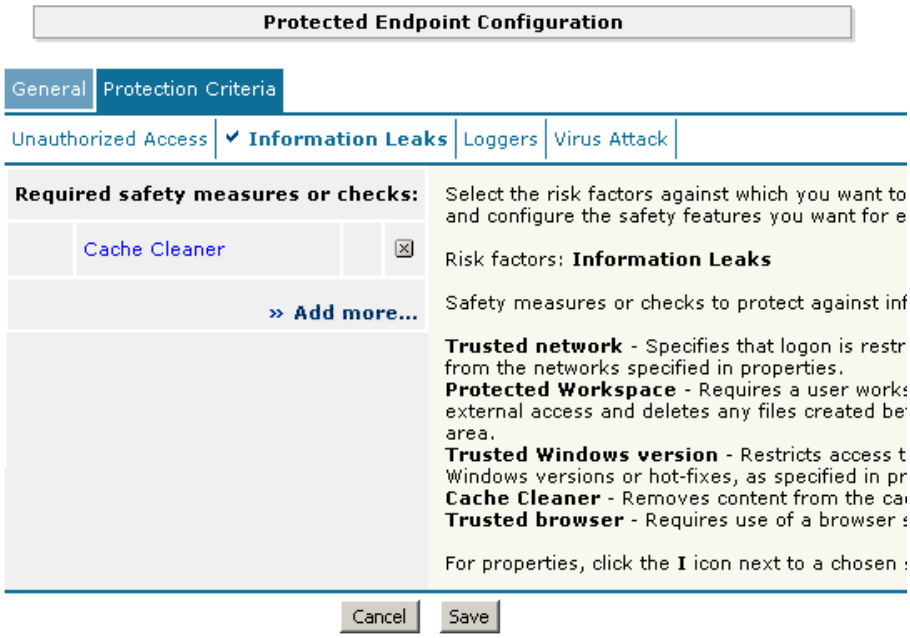

Figure 1.11 *The Protection Criteria tab of the Protected Endpoint Configuration screen*

Important*: The Cache Cleaner feature is currently Windows only. It does not work with Apple Macintosh or Linux systems.*

8. On the menu bar, click **Virus Attack**
9. From the list, select **Antivirus** and click the **Add** button.
10. Click the **I** icon next to Antivirus to configure the antivirus properties (see Figure 1.12). The Select trusted anti-viruses screen opens. Configure these properties as applicable for your configuration, and click the **Save** button.

    You return to the Protection Criteria tab of the Protected Endpoint Configuration page.
11. Click the **Save** button.

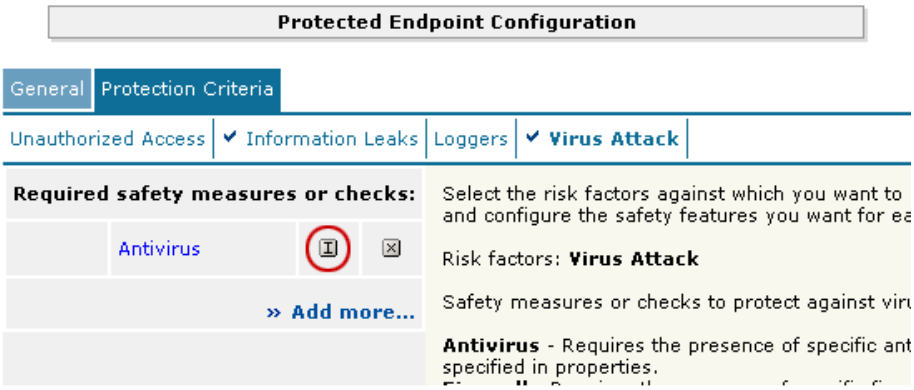

Figure 1.12 *The Edit button for Antivirus properties*

Protecting the Resources

The next step is to associate the protected configuration you just created with a resource.

To protect the resources

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Protect Resources**.
2. From the Resource Table, expand **Web Applications**.
3. Find the **Partners** resource group (in our example, **Partners_SP**), and click the **Select** link next to the Favorite you configured.
4. From the **Configuration to protect selected resources** list, select the name of the configuration you created in the preceding procedure. In our example, we select **Partner_config**.
5. Click the box next to the Favorite name, and click the **Select** button. A shield image appears in the row.

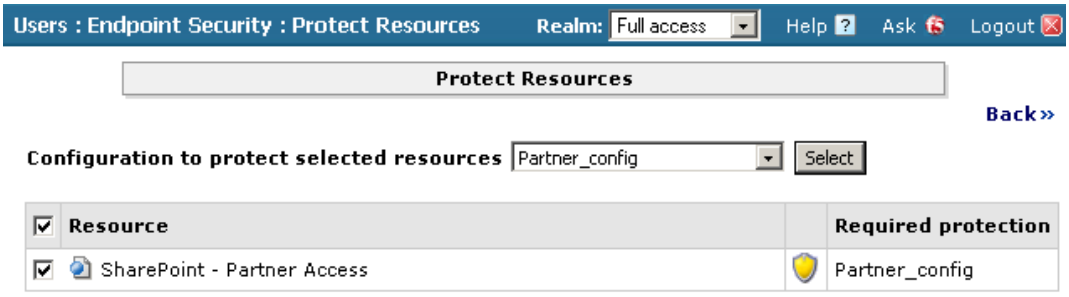

Figure 1.13 *Adding the Protected Configuration to the Resource*

Configuring post-logon actions

The final step is to configure a post-logon action in which the FirePass device injects an Active X control or plug-in to clean the client browser's web cache.

To configure the post-logon action

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Post-Logon Actions**.
2. Click a check in the **Inject ActiveX/Plugin to clean-up client browser web cache** box. A list of options displays.
3. Configure these options as applicable for your deployment. In our example, we leave these options at their default settings.

Conclusion

The FirePass controller is now configured to allow secure remote access to the SharePoint 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.