

Deployment Guide

**Deploying Microsoft Exchange Server/Outlook
Web Access and F5's FirePass Controller**



Introducing the FirePass and Microsoft Exchange Server configuration

Welcome to the FirePass Exchange Server Deployment Guide. This guide shows you how to configure the F5 FirePass controller for secure remote access to Microsoft® Exchange Server, including Outlook® Web Access (OWA).

Microsoft Exchange Server helps increase knowledge worker productivity while helping organizations reduce their total cost of ownership (TCO) in areas such as server and site consolidation.

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

For more information on the Microsoft Exchange Server, see <http://www.microsoft.com/exchange/default.mspx>

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 Exchange Server 2003.
- ◆ All of the configuration procedures in this document are performed on the FirePass controller. For information on how to deploy or configure the Exchange Server 2003 or Outlook Web Access, 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 Exchange Server. For more detailed information on these products, consult the appropriate documentation.

Configuration scenario

For the scenario used in this Deployment Guide, the Microsoft Exchange deployment, along with an Active Directory instance, resides behind a BIG-IP system. A group on the FirePass controller is given three access methods for reading Microsoft Exchange/Outlook Web Access email:

- Through an Outlook Web Access Portal Favorite on the FirePass device.
- Through the Network Access adapter, with a locally installed Microsoft Outlook client.
- Through the Mobile Email feature, which provides lightweight, pure HTML access to Exchange mailboxes using IMAP/POP3 and SMTP.

This Deployment Guide describes how to configure the FirePass controller to allow secure remote access to the Exchange device(s), using Active Directory for authentication. In our deployment, the FirePass device and the Exchange deployment 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.

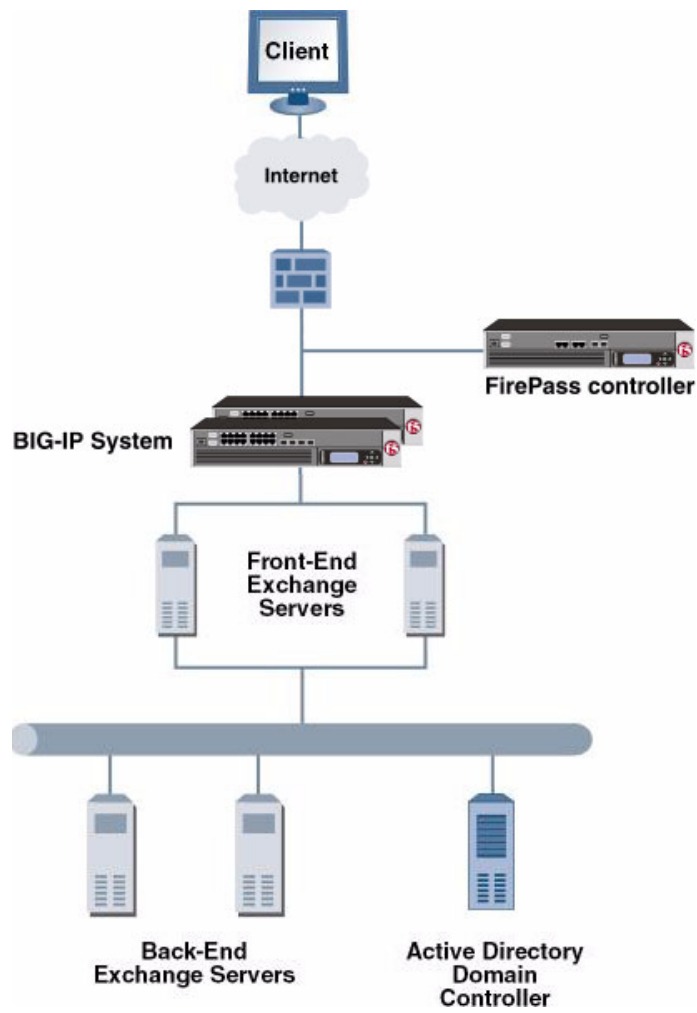


Figure 1.1 FirePass Exchange Server logical configuration

Configuring the FirePass controller for deployment with Microsoft Exchange Servers

To configure the FirePass controller for allowing secure remote access to the Microsoft Exchange Servers deployment, use the following procedures:

- *Connecting to the FirePass controller*
- *Creating groups on the FirePass controller*
- *Configuring auto-logout*
- *Configuring Outlook Web Access through the FirePass device*
- *Configuring Mobile Email for HTML-based access to email*

- *Configuring Network Access to the Exchange server*
- *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

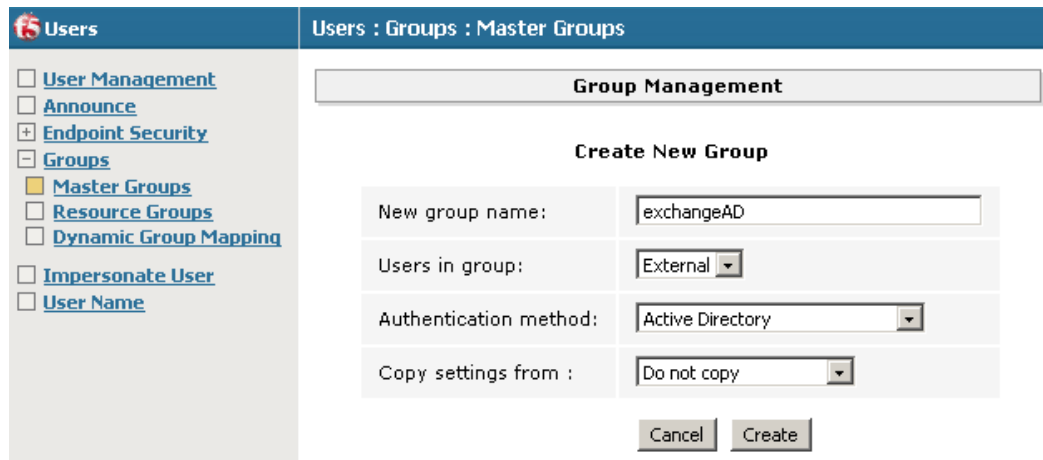
1. From the navigation pane, click **Users**, expand **Groups**, and then click **Resource Groups**.
2. Click the **Create new group** button.
The Group Management - Create New Group screen opens.
3. In the **New group name** box, type a name for your group and click the **Create** button. In our example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

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



The screenshot displays the FirePass Administrative Console interface. On the left, a navigation pane under 'Users' shows 'Groups' expanded, with 'Master Groups' selected. The main content area is titled 'Users : Groups : Master Groups' and contains a 'Group Management' section. Within this section, the 'Create New Group' form is visible. The form includes the following fields and values:

- New group name:** exchangeAD
- Users in group:** External
- Authentication method:** Active Directory
- Copy settings from:** Do not copy

At the bottom of the form are 'Cancel' and 'Create' buttons.

Figure 1.2 Creating a new Master Group

7. Click the Resource Groups tab.
The Resource Groups screen opens.
8. 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_email**.
9. 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 Group* section. In our example, we select **exchangeAD**.
3. Click the Authentication tab.
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 (see Figure 1.3).
5. Click the **Save Settings** button.

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

Master Group: exchangeAD [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: | ••••• |

[Save Settings](#) [Test Saved Settings](#)

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.

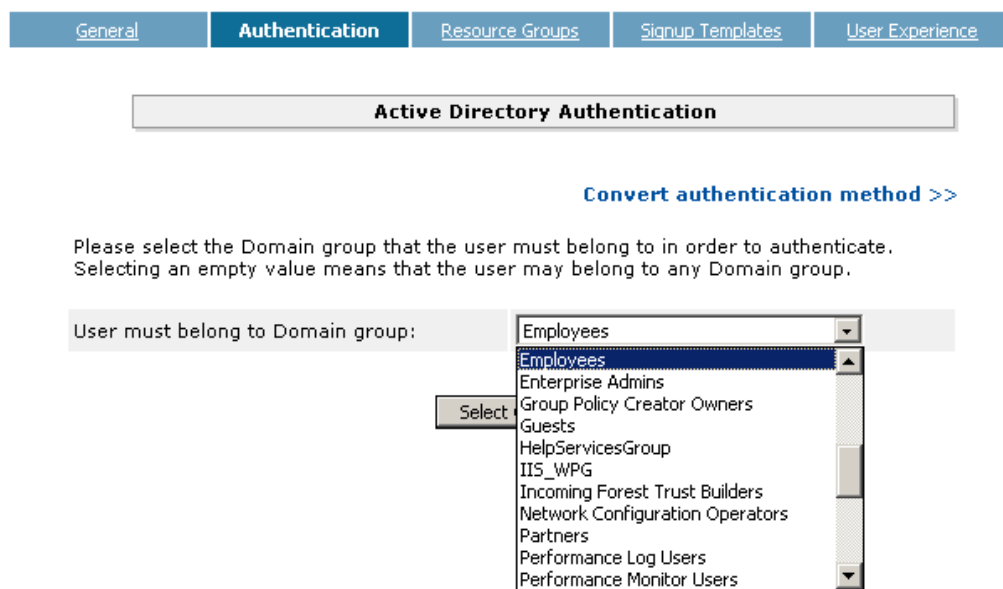


Figure 1.4 Selecting the Active Directory Domain Group

Configuring auto-logout

The FirePass allows auto-logout (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-logout

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 Group* section. In our example, we select **exchangeAD**.
The configuration settings for the Master group open.

4. To ensure members of the group only have access to the administrator-configured Favorites, make sure that the check box under **Access limitation** is checked.
5. 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.
6. In the **NTLM Auth Domain (optional)** box, you can type the default Domain to be used in conjunction with the auto-login support.
7. 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).
8. Click the **Update** button.

Portal Access : Web Applications : Master Group Settings

Master Group: exchangeAD

Access limitation

Limit Web Applications Access to Intranet Favorites only, with no direct addressing (for Extranets, partner and customer access, etc.)

Password Security

Enforce password entry from virtual keyboard

NTLM and Basic Auth Proxy

Proxy Basic and NTLM auth using FirePass user login form.
Preference: NTLM Authentication

Auto-login to Basic and NTLM auth protected sites using FirePass user credentials.

NTLM Auth Domain (optional): DEMO

Basic Auth Domain (optional): DEMO

Figure 1.5 Configuring NTLM Master Group Settings

Configuring Outlook Web Access through the FirePass device

For organizations who want an added layer of security for their Outlook Web Access deployment, want to require antivirus or other pre-logout checks, or do not want to make Outlook Web Access directly accessible from the Internet, the FirePass can be configured to render Outlook Web Access inside the FirePass user window.

To configure Outlook Web Access 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_email** in our example). In this row, from the **Portal access** column, click **Edit** (see Figure 1.6). The Web Applications section of the Resource Group page opens.

| Users : Groups : Resource Groups | | | | |
|----------------------------------|----------------------|----------------------|----------------------|----|
| Resource groups | | | | |
| Group Name | Network access | Portal access | Application access | Rc |
| Default_resource | Edit | Edit | Edit | |
| DemocenterUsers | Edit | Edit | Edit | |
| employees_email | Edit | Edit | Edit | |

Figure 1.6 The Resource groups table

3. Under Web Application Favorites, click **Add New Favorite**. The Favorite options display.
4. Type a name for the Favorite. In our example, we type **Outlook Web Access**. This Favorite link only displays for members of the **employee_email** group.
5. From the **Web Application Type** box, select **Microsoft Outlook Web Access**.
6. In the URL box, type the URL used to access the Outlook Web Access. If you are using a BIG-IP system in front of the deployment, this URL should point to the virtual server address. In our example, we type **http://webmail.company.com/**.
7. Configure the rest of the settings as applicable to your deployment (see Figure1.7).
8. Click the **Add New** button.
The new Favorite is added to the list, and will appear in the Portal Access Favorite section when the end user's logs onto the FirePass device.

The screenshot shows the FirePass configuration interface. At the top, there is a navigation bar with 'Users : Groups : Resource Groups' and a 'Realm' dropdown set to 'Full access'. Below this, the 'Resource Group' is set to 'employee_email'. The main content area is titled 'Web Application Favorites' and contains a form to 'Add New Favorite'. The form fields are as follows:

- Type:** Favorite (dropdown)
- Name:** Outlook Web Access (text input)
- Web Application Type:** Microsoft Outlook Web Access (dropdown, circled in blue)
- Url:** http://webmail.company.com/ (text input)
- Url variables:** (empty text input)
- Post url variables:**
- Enforce user-agent:** (empty text input)
- Open in new window:**
- Endpoint protection required:** (dropdown)

At the bottom of the form, there is an 'Add New' button and a 'Default:' section with a 'No Default' dropdown and an 'Update' button.

Figure 1.7 Adding a Web Application Favorite to the Resource group

Configuring Mobile Email for HTML-based access to email

As an alternative (or in addition to) using Outlook Web Access, you can use the FirePass controller's Mobile Email feature as a lightweight and extremely secure way of viewing Microsoft Exchange email.

To configure mobile access

1. From the navigation pane, click **Portal Access** and then click **Mobile E-Mail**.
2. Under Corporate mail account, click a check in the **Enable corporate mail account box**.
3. In the **Account Name** box, type a name for this email account. In our example, we type **Exchange Server**.
4. In the **Mail Server** box, type the name or IP address of the Exchange server. In our example, we type **exchange1**.
5. In the **Type** box, select **IMAP**.
6. In the IMAP Folders box, type the folders that should be displayed. A user can add to this list independently. Adding the folders is done to avoid the common confusion created by Exchange servers that

display non-email items such as contacts, calendar, etc, as empty folders. In our example, we type **Inbox,Drafts,Notes,Sent Items**. In the **Sent Folder** box, type **Sent Items**.

7. From the Login Information box, choose the setting appropriate for your configuration. In our example, we select **User supplies display and login information during the first logon**.
8. Click the **Update** button.
9. Configure the rest of the options as applicable for your deployment, making sure to click the appropriate **Update** button if you make changes.

Configuring Network Access to the Exchange server

For remote users with an Outlook client on their PC, the FirePass can be configured to grant access to the corporate network to communicate directly with the Exchange server.

To configure Network access to the Exchange Server

1. From the navigation pane, click **Network Access**, and then click **Global Settings**.
2. From the **Add new IP Address Pool** section, in the Name box, type a name for this pool of IP addresses.
3. In the **IP Address** box, type the Network address for this pool. In our example, we type **10.10.101.0**.

***Important:** Using Network Access requires you have one internal IP address for each concurrent user, so make sure this Network address can handle all possible concurrent users.*

***Warning:** To prevent routing problems, ensure the Network address pool does **not** contain the FirePass device's IP address.*

4. In the **Mask** box, type the appropriate subnet mask. In our example, we type **255.255.255.0**.
5. Click the **Add** button. In our example, this creates enough addresses for 254 users.
6. Leave the **Use NAPT to Access LAN** box checked.
7. Click the **Apply these rules now** button.
The IP address pool is now configured.
8. From the navigation pane, click **Resources**.
The Network Access Resource screen opens.
9. In the **Connection Name** box, type a name for the connection. This is the name the end user sees in the Favorites list. In our example, we type **internal exchange**.

10. In the **DNS** and **WINS** server boxes, type the appropriate IP addresses.
11. You can optionally configure split tunneling. To configure split tunneling, click a check in the **Use split tunneling** box. The LAN and DNS address space boxes display. Configure these options as applicable for your deployment.
12. If you want the FirePass device to perform GZIP compression, click a check in the **Use gzip compression** box.
13. Click the **Update** button.
14. In the Configure IP Address Assignment section, make sure there is a check in the **Assign IP address dynamically using IP address pool (lowest priority: Enabled by default)** box.
15. From the Select IP Address Pool list, select the pool you created in step 2, 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-logout sequence for inspections before a user logs on. For more information on endpoint security, see the online help.

Pre-logout sequence

The pre-logout 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-logout sequence

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Pre-Logout 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 **exchangeBasic**.
3. From the **Based on** list, select **template: Collect information with no pre-logout 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 1.8). 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 1.8). 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, and they cannot log in.

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.

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

16. Click the **Apply** button.

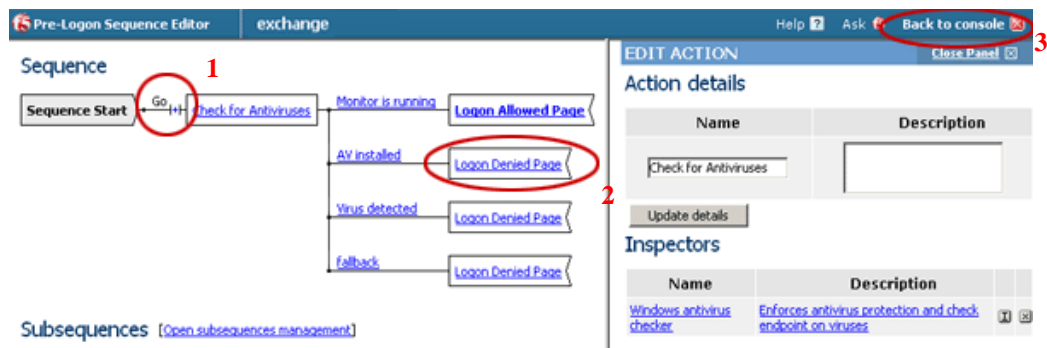


Figure 1.8 The Pre-Logon Sequence Editor

Conclusion

The FirePass controller is now configured to allow secure remote access to Exchange-based email. 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.