

Deployment Guide

**Deploying IBM Lotus Domino Web Access
(iNotes) and F5's FirePass controller**



Introducing the FirePass and IBM Domino Web Access configuration

Welcome to the FirePass Domino Web Access Deployment Guide. This guide shows you how to deploy the F5 FirePass controller with IBM® Lotus Domino® Web Access servers.

Domino Web Access (formerly IBM Lotus iNotes™ Web Access) is a sophisticated web application that gives end users leading Domino messaging and collaboration features that were previously available only with a Lotus Notes client. Users get all this, with the reliability and security features of IBM Lotus Domino server -- delivered through a web browser.

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 Domino Web Access, while significantly lowering support costs associated with legacy client-based VPN solutions.

For more information on the Domino Web Access, see <http://www.lotus.com/products/product1.nsf/wdocs/webaccesshome>

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 Domino Web Access version 6.5.3.
- ◆ This deployment was tested using clients running Microsoft® Windows®.
- ◆ All of the configuration procedures in this document are performed on the FirePass controller. For information on how to deploy or configure the Domino Web Access, consult the appropriate documentation.
- ◆ This configuration uses LDAP searches to the Domino Servers Authentication database.
- ◆ 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 the FirePass controller, Domino Web Access, and LDAP. For more detailed information on these products, consult the appropriate documentation.

Configuration scenario

For the scenario used in this Deployment Guide, the IBM Lotus Domino Web Access (DWA) deployment, using LDAP authentication, resides behind a firewall, with the FirePass device in the DMZ. A single user group on the FirePass controller is given the following ways to access email:

- Through a Domino Web Access Portal Favorite on the FirePass.
- Through the Network Access adapter, with a locally installed Lotus Notes client.

This Deployment Guide describes how to configure the FirePass controller to allow secure remote access to the Domino device(s), using LDAP for authentication. In our deployment, the FirePass device uses the Domino authentication database via LDAP. This guide also contains procedures on configuring some endpoint security features, including antivirus checks. These features provide an intelligent layer of security, and are ideal for organizations using DWA that want to require antivirus or other pre-logout checks, or do not want to DWA directly accessible from the Internet.

The following figure is a logical representation of our deployment.

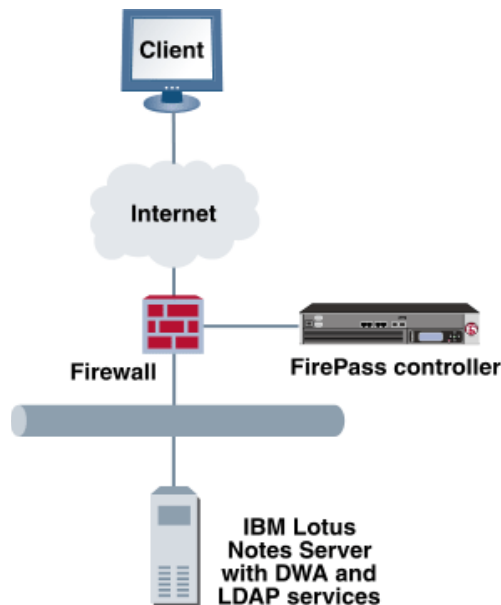


Figure 1.1 FirePass Domino Web Access logical configuration

Configuring the FirePass controller for deployment with IBM Domino Web Access

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

- *Connecting to the FirePass controller*
- *Creating groups on the FirePass controller*
- *Configuring auto-logout to web Favorites*
- *Configuring content processing*
- *Configuring access to DWA using a Portal Access Favorite*
- *Configuring Network Access to the Domino 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 **DWA_Resources**. 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 **DWA_LDAP**.
3. In the **Users in group** box, select **External**.
4. From the Authentication method list, select **LDAP**.
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 shows the 'Create New Group' dialog box in the FirePass Administrative Console. The navigation pane on the left is expanded to 'Users > Groups > Master Groups'. The dialog box has a title bar 'Group Management' and a subtitle 'Create New Group'. It contains four input fields: 'New group name:' with the text 'DWA_LDAP', 'Users in group:' with a dropdown menu showing 'External', 'Authentication method:' with a dropdown menu showing 'LDAP', and 'Copy settings from:' with a dropdown menu showing 'Do not copy'. At the bottom of the dialog 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 **DWA_Resources**.
 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 LDAP authentication

Next, we configure the Master group to use LDAP authentication from our external LDAP server.

To configure the FirePass Master group to use LDAP 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 **DWA_LDAP**.
3. Click the Authentication tab.
The LDAP Authentication screen opens.
4. In the **Host** box, type the IP address of the Notes server.
5. In the **Port** box, type the Port of the LDAP server. In our example, we type **389**, the default LDAP port. If you want to use LDAP over SSL, click a check in the LDAP over SSL
6. From the Protocol version list, select the appropriate version. In our example, we select **3** (see Figure 1.3).
This is the version that Lotus Notes requires; older versions may not require version 3.
7. Click the **Lookup user's DN using template** option button.
8. In the User DN template, type the template. We create the template by examining LDAP records (as found in an LDAP browser), and extracting the DN. The following is an excerpt from an LDAP record:

```
# Billy Bob, F5 Demo Center, F5, US  
dn: CN= Bob,OU=F5 Demo Center,O=F5,C=US
```

Your DN will be different based on your Notes configuration.

The FirePass controller substitutes the user's FirePass logon as part of the Bind DN, and supplies the entered password as the Bind password. If the bind operation succeeds, the user is validated.

In our example, we type:

```
CN=%logon%,OU=F5 Demo Center,O=F5,C=US
```

If the CN is a multi-valued attribute on the user record, the FirePass device uses the first value returned for that attribute.

Note: Use an LDAP browser to explore the records, or contact your Lotus Notes or Domino administrator for more details on this step.

LDAP Authentication

[Convert authentication method >>](#)

Host:

Port: Use SSL connection

Protocol version:

Lookup user's DN using template

User DN template:
use %logon% in the DN template to insert an user logon. For example "cn=%logon%,ou=it,o=uroam"

Lookup user's DN using query

User DN for query:

Figure 1.3 LDAP authentication settings

9. Click the **Save Settings** button.
10. Click the **Test** button to test the LDAP configuration. The LDAP Authentication test screen opens.
11. Type the Username and Password of a valid user, and click the **Test** button. The test results page displays. If the test was successful, you see green text saying the test passed (see Figure 1.4). If the test was not successful, you see red text saying the test did not pass. Try again, or modify the settings as applicable.

LDAP Authentication

[Convert authentication method >>](#)

| | |
|---------------|--|
| LDAP server | 10.10.100.6 |
| LDAP port | 389 |
| LDAP protocol | 3 |
| Lookup method | template |
| Template | CN=%logon%,OU=F5 Demo Center,O=F5,C=US |
| User's DN | CN=jordan,OU=F5 Demo Center,O=F5,C=US |
| User bind | OK |

LDAP test: passed.

Figure 1.4 Testing the LDAP configuration

-
12. When you are finished testing, click the **Cancel** button.

Configuring auto-logout to web Favorites

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 Domino Web Access for ease of integration, using basic authentication.

To configure 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 **DWA_LDAP**.
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 **Proxy Basic and NTLM auth using FirePass user login form**, and select **Basic Authentication** from the **Preference list**.
Also click a check in the **Auto-logout to Basic and NTLM auth protected sites using FirePass user credentials** box.
The NTLM and Basic Auth domain boxes display.
6. If required, in the **Basic Auth Domain (optional)** box, you can type the default Domain (realm) to be used in conjunction with the auto-logout support (see Figure 1.5).
7. Click the **Update** button.

Portal Access : Web Applications : Master Group Settings

Master Group:

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:

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

NTLM Auth Domain (optional):

Basic Auth Domain (optional):

Figure 1.5 Configuring Master Group Settings

Configuring content processing

For effective access, some web applications like Domino Web Access require a special access mode. Enter host name or comma-separated list of host names for which you want to switch to this special mode. The optimal caching and compression settings will be used for these applications overwriting the global settings in the Caching and Compression page.

To configure SSO/NTLM for auto-login

1. From the navigation pane, click **Portal Access**.
2. Under Web Applications, click **Content Processing**.
3. Click the Global Settings tab.
4. In the **Feature Web Application** section, in the **IBM iNotes** box, type the host name of the DWA server.
5. Click the **Update** button.

Configuring access to DWA using a Portal Access Favorite

In this procedure, we configure a Favorite on the FirePass controller to the Domino Web Access deployment using Portal Access. With Portal Access, the FirePass device acts as a proxy between the browser client and the DWA

server. This mode doesn't require the download of any special software, and the FirePass controller has built-in support for Portal Access to Domino Web Access devices.

To configure Domino 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 (**DWA_Resources** 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 | Resource access |
| Default_resource | Edit | Edit | Edit | |
| DWA_Resources | Edit | Edit | Edit | |
| employee_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 **Domino Web Access**. This Favorite link only displays for members of the **DWA_Resources** group.
5. From the **Web Application Type** box, select **IBM iNotes**.
6. In the **URL** box, type the URL used to access Domino Web Access. This should be the URL of the redirect page (database). Domino Web Access Redirect uses Domino authentication methods to redirect a user's browser to their mail file based on their user name/password.

Important: In order for this integration to function properly, the URL must be the Domino Web Access Redirect page. If you do not already have a redirect page, you can create one from the Lotus Domino Designer using the **Domino Web Access Redirect** template database. For more specific information, refer to the Domino documentation.

In our example, we type **http://www.company.com/WA.nsf**.

7. Configure the rest of the settings as applicable to your deployment (see Figure 1.7).
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 'Add New Favorite' form in the FirePass configuration interface. The form is titled 'Add New Favorite' and has a close button in the top right corner. The fields are as follows:

- Type:** Favorite (dropdown menu)
- Name:** Domino Web Access (text input)
- Web Application Type:** IBM iNotes (dropdown menu, circled in blue)
- Url:** http://www.company.com/WVA.nsf (text input)
- Url variables:** (empty text input)
- Post url variables:**
- Enforce user-agent:** (empty text input)
- Open in new window:**
- Endpoint protection required:** (empty dropdown menu)

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 Network Access to the Domino server

For remote users with an Lotus Notes client on their computer, the FirePass device can be configured to grant access to the corporate network to communicate directly with the Domino server.

To configure Network access to the Domino 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 **10.10.201.0**.

Important: Using Network Access requires you have one internal IP address for each concurrent user, so make sure the defined network has enough possible host addresses to 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 concurrent users.
6. Leave the **Use NATP 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 DWA**.
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 a 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-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 **DWABasic**.
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 1.8). 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 **DWABasic**.
16. Click the **Apply** button.

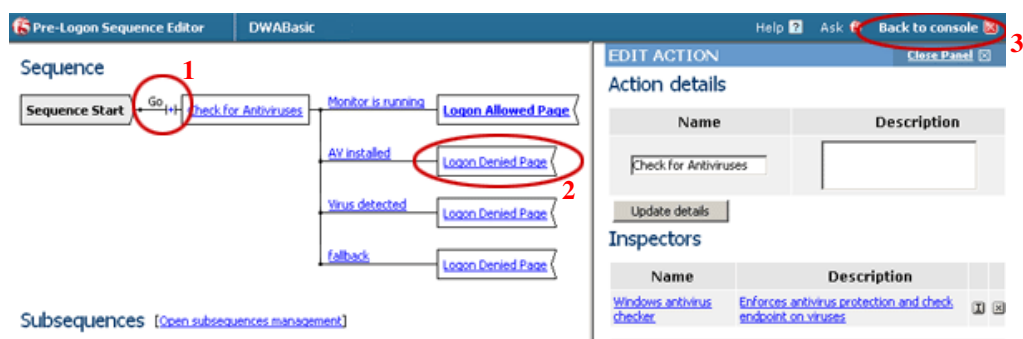


Figure 1.8 The Pre-Logon Sequence Editor

Conclusion

The FirePass controller is now configured to allow secure remote access to Domino Web Access 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.