

Deployment Guide

Integrating the FirePass Controller and WholeSecurity Confidence Online Server





Integrating the FirePass and WholeSecurity Confidence Online Server

- Introducing the FirePass and WholeSecurity Confidence Online Server configuration
- Configuring the FirePass controller for integration with the Confidence Online server

Introducing the FirePass and WholeSecurity Confidence Online Server configuration

This document is intended to be a quick installation and configuration guide integrating the FirePass controller and WholeSecurity (now Symantec) Confidence Online™ server.

The WholeSecurity Confidence Online™ solutions employ patent-pending behavioral detection technology that automatically identifies and eliminates both known and unknown threats without requiring users to install or update signatures. Confidence Online's proven zero-hour detection capabilities prevent the electronic theft of confidential corporate and personal data by eliminating eavesdropping threats, while mitigating the significant losses that stem from widespread worm infections.

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

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

For more information on the WholeSecurity Confidence Online solution, see <http://www.wholesecurity.com/>.

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The WholeSecurity Confidence Online server must be using version 4.1 or later. This Deployment Guide was tested using versions 4.1 and 4.2.
- ◆ The FirePass controller must be running version 5.4.2 or later. Earlier versions of the FirePass device are not supported. You must also have the following F5 files relevant to your Confidence Online Server:
 - Confidence Online Server v4.1: **events.zip**
 - Confidence Online Server v4.2: **f5files.zip**
- ◆ If you are running version 5.4.2 of the FirePass controller, the following HotFixes must be installed:
 - HF-47720-47749-49767-1, which adds support for bypass mode
 - HF-47995-1, which adds support for integration with the WholeSecurity Confidence Online Server

For information on how to install these HotFixes, see the following Solution on the Ask F5 Technical Support site:

<http://tech.f5.com/home/firepass/solutions/instupg/sol3430.html>

Versions of the FirePass controller *after* 5.4.2 already include these HotFixes.

◆ **Important**

Only integration with WholeSecurity and the Microsoft Windows platform is currently supported.

◆ **Note**

This document is written with the assumption that you are familiar with both the FirePass controller and the Confidence Online server. For more detailed information on these products, consult the appropriate documentation.

Configuring the FirePass controller for integration with the Confidence Online server

To configure deployment, you need to complete the following procedures:

- ◆ *Configuring the WholeSecurity Confidence Online Server*
 - *Replacing the Confidence Online Server files*
- ◆ *Configuring the FirePass controller*
 - *Connecting to the FirePass controller*
 - *Resetting caching and compression*
 - *Configuring the Endpoint Inspectors*
 - *Configuring a pre-logon sequence*

Configuring the WholeSecurity Confidence Online Server

Use the following procedure to create a new Deployment on the WholeSecurity Confidence Online Server.

To configure the Confidence Online Server

1. Logon to Confidence Online Management console as an administrator.
2. From the navigation pane, under Deployments, click **add new deployment**.
The New Deployment screen opens.
3. This step is slightly different depending on which version of the Confidence Online Server you are using:
 - For version 4.1, from the list, select **Netscreen SSL VPN**, and click the **Next** button.

- For version 4.2, select **Juniper Networks NetScreen SSL VPN (post-login scan)**, and click the **Next** button.
The New Deployment screen opens.
4. In the **Deployment Name** box, type a name your deployment. In our example, we type **fp_integration**.
 5. *Optional:* In the **Description** box, you can type a description for this Deployment.
 6. In the **Confidence Online Server** box, review the default entry and modify it if necessary.
 7. In the **Netscreen IVE** box, type the IP address of the FirePass device. In our example, we type **192.168.200.217** (see Figure 1.1).
 8. Configure the rest of the options as applicable for your deployment. For more information, see the Online Help.
 9. Click the **Create** button. When the **Add New Deployment Result** message displays, click **OK**.
This creates a new file folder with the following format:
<Confidence Online installation dir>\llclient\<deployment name>
 10. Complete the rest of this New Deployment as applicable to your configuration. For more information, refer to the appropriate WholeSecurity manual.

New Deployment: Netscreen

Step 2 of 2: Specify Deployment Parameters

Complete this wizard to create a new deployment. This will automatically generate the client software for the deployment and the location of the software will be listed on the Current Deployments page.

| | |
|---------------------------|-------------------------|
| Deployment Name: | * fp_integration |
| Description: | F5 FirePass |
| Confidence Online Server: | * ee_server.company.com |
| NetScreen IVE: | * 192.168.200.217 |
| Protocol: | HTTPS |

| | |
|---|---|
| Assign Admins: | |
| Admins: | Assigned Admins: |
| <div style="border: 1px solid gray; height: 80px;"></div> | <div style="border: 1px solid gray; height: 80px;"></div> |
| <input type="button" value="MOVE SELECTION"/> | |
| <input type="button" value="MOVE ALL"/> | |
| <input type="button" value="MOVE ALL"/> | |
| <input type="button" value="MOVE SELECTION"/> | |

| | | | |
|---|---|---|---|
| Default Mitigation Policy: | | | |
| Trojans | Keyloggers | Remote Controls | Monitors |
| <input checked="" type="radio"/> Report | <input checked="" type="radio"/> Report | <input checked="" type="radio"/> Report | <input checked="" type="radio"/> Report |
| <input type="radio"/> Disable | <input type="radio"/> Disable | <input type="radio"/> Disable | <input type="radio"/> Disable |
| <input type="radio"/> Quarantine | <input type="radio"/> Quarantine | <input type="radio"/> Quarantine | <input type="radio"/> Quarantine |

* - required.

Figure 1.1 Creating a new Deployment on the Confidence Online Server

Replacing the Confidence Online Server files

The next step is to copy the F5 provided files into the directory that was created when you configured the Deployment in the preceding procedure (this is the directory described in step 9 of the previous procedure (<Confidence Online installation dir>\llclient\<deployment name>).

This procedure is performed from the Confidence Online Server command line, and the files and syntax depends on whether you are using version 4.1 or 4.2 of the Confidence Online Server.

To replace the events.js file for version 4.2

For version 4.2, there are three files to replace. Make sure you have downloaded and extracted the **f5files.zip** file before attempting this step.

From the command line on the Confidence Online Server v4.2, use the following syntax to copy the files:

```
xcopy "<Directory that contains the files provided by F5>/**"  
"<Confidence Online installation dir>\llclient\<name of  
Confidence Online Deployment>" /e
```

To replace the events.js file for version 4.1

For version 4.1, you only replace the **events.js** file. Make sure you have downloaded the **events.zip** file before attempting this step.

From the command line on the Confidence Online Server v4.1, use the following syntax to copy the **events.js** file:

```
copy <Directory where you saved the F5 events.js file>  
events.js <Confidence Online installation dir>\llclient\<name of  
Confidence Online Deployment>\include\events.js
```

Configuring the FirePass controller

In this section, we configure the FirePass controller for integration with the Confidence Online Server. All of the following procedures are performed on the FirePass controller.

Important

*If you are using version 5.4.2 of the FirePass controller, be sure you have installed the HotFixes (as described in the **Prerequisites and configuration notes** section) before continuing.*

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, 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.

Resetting caching and compression

In the following procedure we reset the web application cache, which is a critical step in this deployment.

To reset the FirePass web Application cache

1. On the FirePass admin console, from the navigation pane, click **Portal Access**, and from the expanded Web Applications menu, click **Caching and Compression**.
2. In the WebApplications cache section, click the **Clear Cache** button.

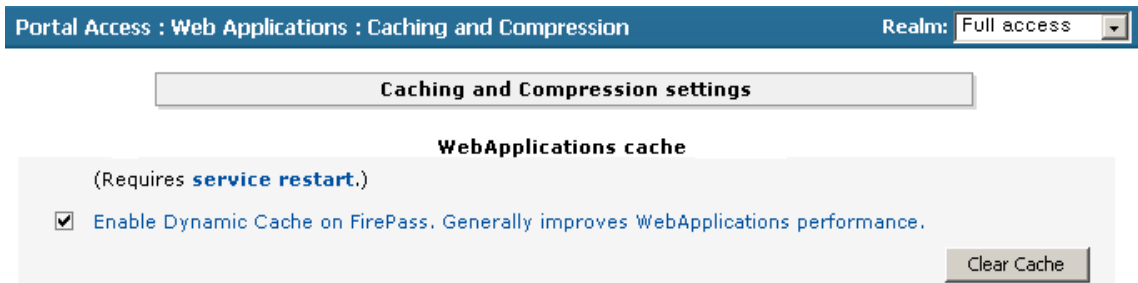


Figure 1.2 Clearing the WebApplications cache on the FirePass controller

◆ WARNING

If you do not clear the Web Application cache, the integration with the WholeSecurity Confidence server will not function properly.

Configuring the Endpoint Inspectors

The WholeSecurity integration relies on a correctly configured Endpoint Inspector on the FirePass device.

◆ Important

You must have already installed the hotfixes listed in the prerequisites section. If you have not, you cannot continue with the integration.

To configure an Endpoint Inspector

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Endpoint Inspectors**.

2. In the Inspector Name column, click **Far-end security integration**. The Endpoint Inspector details screen opens.
3. From the **Product name** list, make sure that **WholeSecurity Confidence Online Server** is selected.
4. In the **URL** box, type the entry point of the desired deployment. In our example we type:
http://192.168.200.217/lclient/QAtest/online.html
5. Leave the **URL for result verification** at the default setting.
6. Click the **Update** button.

| Integration with endpoint security | |
|---|--|
| Product name | WholeSecurity Confidence Online Server |
| URL | http://192.168.200.217/lclient/QAtest/online.html |
| URL for result verification | /integration/queryscanresult.cgi?timeout=3600&details=yes&scan |
| <input type="button" value="Cancel"/> <input type="button" value="Update"/> | |

Figure 1.3 Configuring endpoint security on the FirePass controller

7. For the changes to take effect, you need to restart the service. From the navigation pane, click **Device Management**, expand **Maintenance**, and click **Restart Services**.
8. Click the **Restart Services** link, and then click the **Restart** button to restart the services.

This creates the master group **Prelogon** and user **prelogon** is added to this group. This is a very restricted group, and only the users of this group are only allowed to access WholeSecurity Confidence Online Server, other resources are not inaccessible. The **Prelogon** user can not be authenticated through standard FirePass logon form.

You can return to the **Far-end security integration** inspector property page to recreate prelogon group and to configure the required settings. When you click the **Update** button, the configuration will be verified, and if something is absent, it will be recreated.

Configuring a pre-logon sequence

The final step is to configure or modify a pre-logon sequence on the FirePass controller to apply the WholeSecurity check. After the initial configuration, you can invoke the WholeSecurity check at any place in a FirePass pre-logon sequence.

1. From the navigation pane, click **Users**, expand **Endpoint Security**, and click **Pre-Logon Sequence**.

-
2. To modify an existing sequence, click the **edit** link that corresponds to the sequence you want to modify. If the sequence you want to edit is currently in use, click the **backup & edit** link.

To create a new sequence, from the New Sequence section, type a name in the **Create new sequence** box and select a value from the **Based on** list.

3. Choose where you want the WholeSecurity check to take place in the pre-logon sequence, and select the **External Far-end check** action, and click the **Apply Changes** button.

In our simple example, we move the cursor along the arrow following **Sequence Start**, and click the add **[+]** link that appears on the arrow. From the Change Sequence panel that appears on the right, we select **External Far-end check**, and click **Apply Changes**.

4. The **External Far-end check** action has two rules: **passed** and **fallback**. You can modify the actions as applicable to your configuration. For more information on pre-logon sequences, see the online help.

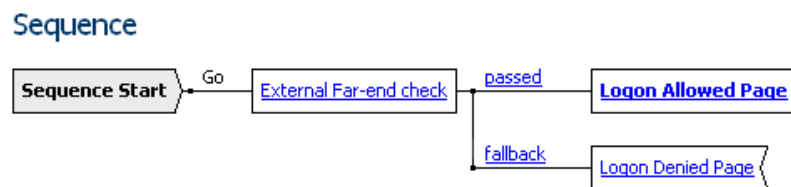


Figure 1.4 A simple pre-logon sequence using the External Far-end check

The integration between the WholeSecurity Confidence Online Server and the FirePass controller is now complete.

Setting Up the Confidence Online Server Confirmation Option

If the Server Confirmation option is enabled, the WholeSecurity Confidence Online Server confirms whether the FirePass controller should allow or deny access to the network based on the results of the second scan. A second scan always occurs after a process is detected and is mitigated on the user's system during the first scan. If the option not enabled, the client makes the determination based on the access policies in the last configuration file retrieved from the WholeSecurity Confidence Online Server.

To complete the setup of Server Confirmation function, the WholeSecurity Confidence Online Server must allow access to its integration directory.

To enable directory access, you need to complete the following procedures:

- ◆ For UNIX, edit the **httpd.conf** file.
- ◆ For Windows, modify the Directory Security settings in IIS.

To enable access to the integration directory on the WholeSecurity Confidence Online Server on UNIX

1. Locate the section of the **httpd.conf** file that defines the integration virtual directory.
2. In the **Allow From** directive, change the setting to the IP address or IP address range of the FirePass controller:

```
# # The Confidence integration interface # Edit the
'Allow from' directive to open it up # to whatever
internal boxes need access to this interface# Alias
/integration "/usr/local/confidence/integration"
<Directory /usr/local/confidence/integration> Options
ExecCGI AllowOverride None Order allow,deny Allow from
127.0.0.1 </Directory>
```

3. Restart Apache.

To enable access to the integration directory on the WholeSecurity Confidence Online Server on Windows

1. In IIS, expand **Default Web Site**.
2. Under **Default Web Site**, right click **integration** and select **Properties**.
3. Click the Directory Security tab.
4. In the IPAddress and domain name restrictions section, click the **Edit** button.
5. On the IP Address and Domain Name Restrictions screen, click the **Add** button, and then enter the IP address or IP address range for the FirePass controller web interface server in the Grant Access area.
6. To accept the entry, click **OK**, and then click all **OK** buttons until you exit IIS.
7. Restart IIS.