

Deployment Guide

Deploying RSA ClearTrust with the FirePass Controller



Deploying RSA ClearTrust with the FirePass controller

Welcome to the FirePass RSA ClearTrust Deployment Guide. This guide shows you how to configure the F5 FirePass controller for enabling Single Sign-On with RSA® ClearTrust® servers. To achieve Single-Sign-On (SSO) with RSA ClearTrust, the F5 FirePass controller can use several methods, including a centralized LDAP Directory server shared by both products. The user's ClearTrust credentials are subsequently used for SSO to any internal applications protected by RSA ClearTrust.

RSA ClearTrust software is designed to enable organizations to manage large numbers of users while enforcing a centralized security policy that ensures compliance, protects enterprise resources from unauthorized access and makes it easier for legitimate users to do their jobs.

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

For more information on the RSA ClearTrust, see <http://www.rsasecurity.com/node.asp?id=1186>

Prerequisites and configuration notes

The following are prerequisites for this deployment:

- ◆ The FirePass controller should be running version 5.5 or later.
- ◆ This deployment was tested using RSA ClearTrust version 5.5.3, and the RSA ClearTrust Agent version 4.6 for Microsoft® IIS 6.0.

◆ Note

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

Configuring the FirePass controller for deployment with RSA ClearTrust

To configure the FirePass controller with RSA ClearTrust, you must complete the following procedures:

- *Connecting to the FirePass controller*
- *Creating a Resource group with the ClearTrust protected sites*
- *Creating a Master group*
- *Choosing an authentication method*
- *Enabling Single Sign-On for the Master group*

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 a Resource group with the ClearTrust protected sites

The first task in configuring the FirePass controller is to create a Resource group on the FirePass controller for the ClearTrust protected web sites/servers.

To create a Resource group

1. In the navigation pane, click **Users**, expand **Groups**, and click **Resource Groups**.
2. In the **New group name** box, type a name for this group. In our example, we type **myresource**.
3. Click the **Create** button.
The new group appears in the list.

To add the ClearTrust protected web sites to the group

1. In the navigation pane, click **Portal Access**.
The Portal Access Web Application Favorites page opens.
2. From the **Resource Group** list, select the name of the Resource group you created in the preceding procedure. In our example, we select **myresource**.

3. Click **Add New Favorite**.
The New Favorite configuration options appear.
4. In the **Name** box, type a name for this favorite.
5. In the **URL** box, type the URL of the ClearTrust protected site.
The rest of the fields are optional; configure as applicable for your deployment. For more information on these options, see the *FirePass Controller Administrator Guide*.
6. Click **Add New**. The Favorite appears in the list.
7. Continue adding Favorites until you have Favorites for all of your ClearTrust protected sites (see Figure 1).

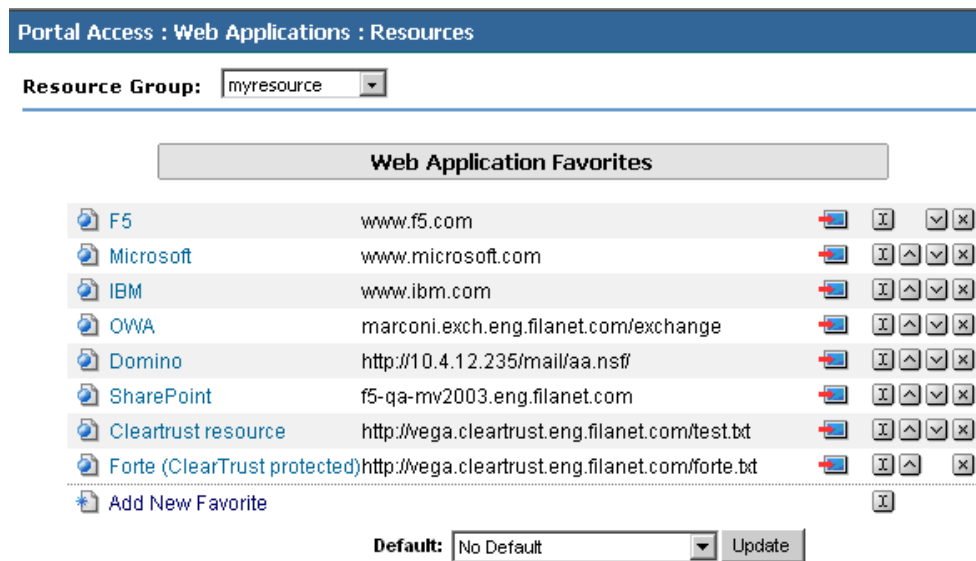


Figure 1 FirePass Web Application Favorites

Creating a Master group

The next task is to create a Master group on the FirePass controller. You configure the Master group to contain the Resource group you just created and one of the following authentication methods:

- *Using HTTP basic authentication and Single Sign-On*
- *Using HTTP form-based authentication and Single Sign-On*
- *Using HTTP form-based authentication with URI retention and Single Sign-On*
- *Using LDAP Authentication and Single Sign-On Support*

◆ Note

*Before you begin configuring the Master group, we recommend that you review **Choosing an authentication method**, on page 5, to determine what is appropriate for your configuration.*

To create a Master group

1. In the navigation pane, click **Users**, expand **Groups**, and then click **Master Groups**.
2. In the **New group name box**, type a name for this group. We recommend a name that is related to the authentication method, such as **cleartrust-basic** (see Figure 2).
3. From the **Authentication method** list, select an appropriate authentication method. See *Choosing an authentication method*, on page 5, for information about selecting an authentication method based on your deployment needs.
4. Configure the rest of the settings as applicable for your deployment. For more information on these settings, refer to the *FirePass Controller Administrator Guide*.
5. Click the **Create** button.

The screenshot shows a web interface for creating a new master group. The breadcrumb navigation at the top reads 'Users : Groups : Master Groups'. Below this is a 'Group Management' section with a 'Create New Group' form. The form has the following fields and values:

New group name:	cleartrust-basic
Users in group:	Local
Authentication method:	Basic HTTP using External Server
Routing Table:	main
Copy settings from :	Do not copy

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

Figure 2 Creating a new Master group on the FirePass controller

6. To associate the Resource group with the Master group, click the **Resource** tab.
7. From the **Available** list, select the Resource group you created for the ClearTrust protected web sites, and click the **Add** button. In our example, we select **myresource** (see Figure 3).
8. Click the **Update** button.

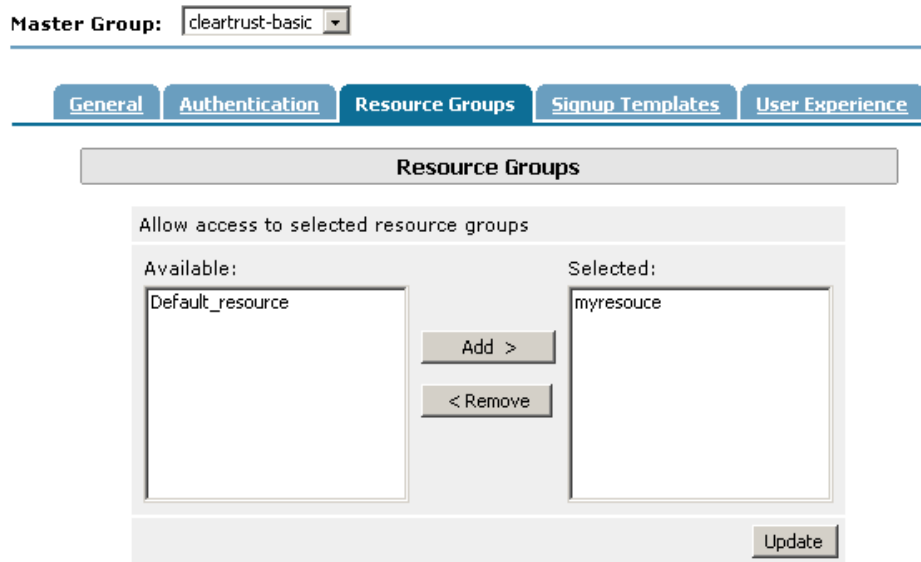


Figure 3 Adding the Resource group to the Master group on the FirePass controller

Choosing an authentication method

This section describes the four different authentication options for configuring the FirePass controller with RSA ClearTrust, and how to configure each one. The four authentication methods are:

- *Using HTTP basic authentication and Single Sign-On*
- *Using HTTP form-based authentication and Single Sign-On*
- *Using HTTP form-based authentication with URI retention and Single Sign-On*
- *Using LDAP Authentication and Single Sign-On Support*

Using HTTP basic authentication and Single Sign-On

You can configure basic HTTP authentication as the authentication method for the Master group. In this scenario, users authenticate with the RSA ClearTrust server using a HTTP basic authentication mechanism when they log on. After initial authentication, users have access to resources in the associated resource group without being prompted to re-authenticate.

To use HTTP basic authentication, select **Basic HTTP using External Server** when configuring the Master group. After configuring the Master group, return to this section and complete the following Additional Configuration section.

Additional configuration for HTTP basic authentication

To use HTTP basic authentication, you must ensure that form-based authentication on the ClearTrust agent is set to **False**. To check this parameter, open the **webagent.conf** file (C:\Program Files\RSA\ClearTrust\IIS Agent4.6\conf). Find the **cleartrust.agent.form_based_enabled** entry, and make sure it is set to **False**: **cleartrust.agent.form_based_enabled=False**.

If you modified this file, you must save it and restart the web server before continuing.

Configuring HTTP basic authentication requires a valid URL resource on the FirePass controller. This resource must respond with a challenge to a non-authenticated request.

To configure the URL resource for HTTP basic authentication

1. In the navigation pane, click **Users**, expand **Groups**, click **Master Groups**, and then click the name of the appropriate Master Group using HTTP basic authentication.
2. Click the Authentication tab.
3. In the **URL** box, type a URL that points to one of the protected resources defined on the ClearTrust server (see Figure 4).
4. Click the **Update** button.

The screenshot shows a configuration page titled "Basic HTTP Authentication to External Server". At the top, there are five tabs: "General", "Authentication", "Resource Groups", "Signup Templates", and "User Experience". The "Authentication" tab is selected. Below the tabs, there is a "Convert authentication method" link. A text input field labeled "URL" contains the text "http://vega.cleartrust.eng.filanet.com/test.txt". Below the input field are two buttons: "Update" and "Test".

Figure 4 Adding a URL to one of the protected resources on the ClearTrust server

◆ Important

*When you have finished configuring the Master group and this authentication method, be sure to go to the **Enabling Single Sign-On for the Master group** section to complete the FirePass controller configuration.*

Using HTTP form-based authentication and Single Sign-On

You can configure HTTP form-based authentication as the authentication method for the Master group. In this scenario, users authenticate with the RSA ClearTrust server using an HTTP form-based authentication

mechanism when they log on. After initial authentication, users have access to resources in the associated resource group without being asked to re-authenticate.

To use HTTP form-based authentication, select **HTTP form-based** when configuring the Master group. After configuring the Master group, return to this section and complete the following Additional Configuration section.

Additional configuration for HTTP form-based authentication

To use HTTP form-based authentication, you must ensure that form-based authentication on the ClearTrust agent is set to True. To check this parameter, open the **webagent.conf** file (C:\Program Files\RSA\ClearTrust\IIS Agent4.6\conf). Find the **cleartrust.agent.form_based_enabled** entry, and make sure it is set to **True: cleartrust.agent.form_based_enabled=True**.

If you modified this file, you must save it and restart the web server before continuing.

To use HTTP form-based authentication, you must complete the following procedure on the FirePass controller.

To configure HTTP form-based authentication

1. In the navigation pane, click **Users**, expand **Groups**, click **Master Groups**, and then click the name of the appropriate Master Group using HTTP form-based authentication.
2. Click the Authentication tab.
3. Leave the **Start URL** empty.
4. In the **Form Action** box, type a Form Action using the following syntax:

```
http://<web_server_protected_by_ClearTrust_Agent>/cleartrust/ct_logon.asp
```
5. In the **Form parameter for user name** box, type **user**.
6. In the **Form parameter for password** box, type **password**.
7. In the Hidden form parameters and values box, type the following:

```
auth_mode=BASIC  
orig_url=  
override_uri_retention=false
```
8. In the **Number of redirects to follow** box, type **0**.
9. Check the **Pass cookies to client browser** box.
10. In the Successful logon detection section, select the **By presence of specific cookie** option. In the Cookie Name box, type **CTSESSION** (see Figure 5).
11. Click the **Save Settings** button. You can also test the settings by typing a user name and password, and clicking **Test Saved Settings**.

[General](#)
[Authentication](#)
[Resource Groups](#)
[Signup Templates](#)
[User Experience](#)

HTTP Form-based Authentication

[Convert authentication method»](#)

HTTP Form-Based Authentication Settings

Start URL	<input type="text"/>
Form action	<input type="text" value="http://vega.cleartrust.eng.flanet.com/cleartrust/ct_log"/>
Form parameter for user name	<input type="text" value="user"/>
Form parameter for password	<input type="text" value="password"/>
Hidden form parameters and values	<div style="border: 1px solid gray; padding: 5px;"> <pre>auth_mode=BASIC orig_url= override_uri_retention=false</pre> </div> <p>Format is name=value. Each line should contain only one name/value pair. Example: TARGET=http://myhost.com/index.htm SMLOCALE=US-EN</p>
Number of redirects to follow	<input type="text" value="0"/>
Pass cookies to client browser	<input checked="" type="checkbox"/>

Successful logon detection

By resulting redirect URL

 URL

 By specific string in result body

 Specific string

 By presence of specific cookie

 Cookie name

Figure 5 Example of HTTP Form-Based Authentication settings

◆ Important

*When you have finished configuring the Master group and this authentication method, be sure to go to the **Enabling Single Sign-On for the Master group** section to complete the FirePass controller configuration.*

Using HTTP form-based authentication with URI retention and Single Sign-On

This scheme is the same as the HTTP form-based authentication scheme, but with URI retention, the user is returned to the original URL after authentication.

To use HTTP form-based authentication with URI retention, select **HTTP form-based** when configuring the Master group. After configuring the Master group, return to this section and complete the following Additional Configuration section.

Additional configuration for HTTP form-based authentication with URI retention

You must first ensure the retain URL setting on the ClearTrust agent is set to **True**. When enabled, the user is redirected back to the original URL once authentication is complete. To check this parameter, open the **webagent.conf** file (C:\Program Files\RSA\ClearTrust\IIS Agent4.6\conf). Find the **cleartrust.agent.retain_url** entry, and make sure it is set to **True**: **cleartrust.agent.retain_url=True**. If you modified this file, you must save it and restart the web server before continuing.

Configuring HTTP forms based authentication with URI retention on the FirePass controller is very similar to the Forms based authentication procedure. Follow the *To configure HTTP form-based authentication* procedure, with the following exception:

- ◆ In step 10, in the Hidden form parameters and values box, type the following:

```
auth_mode=BASIC
orig_url=
override_uri_retention=True
```

All of the rest of configuration steps for this section are the same as the previous section.

◆ Important

*When you have finished configuring the Master group and this authentication method, be sure to go to the **Enabling Single Sign-On for the Master group** section to complete the FirePass controller configuration.*

Using LDAP Authentication and Single Sign-On Support

You can configure LDAP authentication as the authentication method for the Master group. In this scenario, users authenticate with an LDAP server using an LDAP authentication mechanism when they log on.

For this configuration, the LDAP repository must be the same for user authentication and the RSA ClearTrust server. The tested configuration used RSA ClearTrust on Microsoft® Windows® 2003 (LDAP as the Data Adapter), therefore User management can be performed by either the RSA ClearTrust user interface or directly using the Active Directory snap-in.

After initial authentication, users have access to resources in the associated resource group without being asked to re-authenticate.

To use LDAP authentication, select **LDAP** when configuring the Master group. After configuring the Master group, return to this section and complete the following Additional Configuration section.

Additional Configuration for LDAP authentication

To use LDAP authentication, you must complete the following procedure:

Configuring LDAP authentication for master group

1. In the navigation pane, click **Users**, expand **Groups**, click **Master Groups**, and then click the name of the appropriate Master Group using LDAP authentication.
1. Click the **Authentication** tab. In the **Host** box, type the IP address or host name of the Active Directory server.
2. In the **Port** box, type the port for the Active Directory server.
3. From the **Protocol version** list, select a protocol version.
4. Select the **Lookup user's DN using query** option.
5. In the **User DN for query** box, type the User DN for query, using the following syntax:
cn=admin, cn=users, dc=mycompany, dc=com.
The distinguished name of the user with administrative rights is the same as the account on RSA ClearTrust data store.
6. In the **Password** and **Confirm password** boxes, type the password.
7. In the **Search base DN** box, type the Search base DN using the following syntax:
cn=users, dc=mycompany, dc=com.
8. In the **Search query template** box, type **sAMAccountName=%logon%** (see Figure 6).
9. Click the **Save Settings** button.

Important

*When you have finished configuring the Master group and this authentication method, be sure to go to the **Enabling Single Sign-On for the Master group** section to complete the FirePass controller configuration.*

Master Group: LDAPClearTrust

General Authentication Resource Groups Signup Templates User Experience

LDAP Authentication

[Convert authentication method»](#)

Host: star.cleartrust.eng.filane

Port: 389 Use SSL connection

Protocol version: 3

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: cn=adminstrator,cn=users,dc=cleartrust,dc=eng,dc=filanet,dc=com

Change password:

Password:

Confirm password:

Search base DN: cn=users,dc=cleartrust,dc=eng,dc=filanet,dc=com

Search query template: (&(sAMAccountName=%logon%))

use %logon% in the query template to insert an user logon. For example '{&(uid=%logon%)}'

Figure 6 Example of LDAP authentication settings

Enabling Single Sign-On for the Master group

After configuring one of the Master group, and one of the authentication methods, the final task is to modify the Master group settings for Single Sign-On.

To modify the Master Group settings on the FirePass controller

1. In the navigation pane, click **Portal Access**, expand **Web Applications**, and click **Master Group Settings**.
2. From the **Master Group** list, select the appropriate Master group you created.

3. In the NTLM and Basic Proxy Auth section, check the **Proxy Basic and NTLM auth using FirePass user login form** box. From the **Preference** list, select **Basic Authentication**.
4. In the same section, check the **Auto-login to Basic and NTLM auth protected sites using FirePass user credentials** box, and 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 7 Configuring NTLM and Basic Auth Proxy settings

The FirePass controller configuration is now complete.