

HP OpenView Select Access

Integration Paper for Citrix MetaFrame Presentation Server 3.0 Web Interface

**Software Version Tested Against: 6.0
for Windows Operating Systems**



November 2004

© Copyright 2000-2004 Hewlett-Packard Development Company, L.P.

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

© Copyright 2000-2004 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

HP OpenView Select Access includes software developed by third parties. The software HP OpenView Select Access uses includes:

- The OpenSSL Project for use in the OpenSSL Toolkit.
- Cryptographic software written by Eric Young.
- Cryptographic software developed by The Cryptix Foundation Limited.
- JavaService software from Alexandria Software Consulting.
- Software developed by Claymore Systems, Inc.
- Software developed by the Apache Software Foundation.

- JavaBeans Activation Framework version 1.0.1 © Sun Microsystems, Inc.
- JavaMail, version 1.2 © Sun Microsystems, Inc.
- SoapRMI, Copyright © 2001 Extreme! Lab, Indiana University.
- cURL, Copyright © 2000 Daniel Stenberg.
- Protomatter Syslog, Copyright © 1998-2000 Nate Sammons.
- JClass LiveTable, Copyright © 2002 Sitraka Inc.

For expanded copyright notices, see HP OpenView Select Access <install_path>/3rd_party_license directory.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Trademark Notices

Java™ is a US trademark of Sun Microsystems, Inc.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel®, Pentium®, and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux® is a U.S. registered trademark of Linus Torvalds.

Microsoft®, Windows, Windows NT®, and Windows XP®, are U.S. registered trademarks of Microsoft Corporation.

Unix® is a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Support

Please visit the HP OpenView web site at:

<http://www.managementsoftware.hp.com/>

This web site provides contact information and details about the products, services, and support that HP OpenView offers.

You can also go directly to the support web site at:

<http://support.openview.hp.com/>

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and log in. Many also require a support contract.

To find more information about access levels, go to the following URL:

http://support.openview.hp.com/access_level.jsp

To register for an HP Passport ID, go to:

<https://passport.hp.com/hpp2/newuser.do>

contents

Chapter 1	Understanding Your Select Access Integration	7
	Assumptions in this Document	7
	Integrating Select Access with MPS over Web Interface	8
	Understanding the Key Components of this Integration	8
	Example of an Integrated Network Architecture	11
	The Citrix User Authentication Process	11
Chapter 2	Integration Tasks	13
	Setting Up Citrix User Credentials	14
	Unique Credentials: Configuring User Credentials in a Directory Server	14
	Common Credentials: Creating a Common Windows Account	15
	Updating Citrix Files with Select Access-Specific Changes	16
	Files You Need to Replace	16
	To use HP-modified files	16
	Deploying Select Access	17
	Testing your Integration	22
	To test the integration solution	22

Understanding Your Select Access Integration

Select Access is an integral part HP's comprehensive Identity Management suite. It delivers a full solution for complex access management across the enterprise. Select Access:

- Automates access control and user life-cycle management.
- Extends the enterprise through federation.
- Delegates management to business owners and the end users themselves.

Along with robust workflow, user self-service, reporting, and delegated administration capabilities, Select Access is the most comprehensive access control system available. Select Access simplifies your ability to secure user access to Citrix MetaFrame Presentation Server (MPS) when using it's Web Interface to provide browser-based access to MPS resources.

Assumptions in this Document

This document assumes the following:

- That you have both the Web Interface and MPS installed and running on your network.
- That you understand the features and functions of Select Access.

- That you have a working knowledge of LDAP 3.0-compliant directory servers.
- That you have decided whether all your users can access a single home page or whether you require that access to applications be personalized.

Integrating Select Access with MPS over Web Interface

Because the Web Interface is an application deployment system, MPS resources are made available to users requesting access through a Web browser. Consequently, users can have the personalized, Web-based access to MPS tools, information, and applications they require—provided Select Access permissions and policies allow them to do so. To understand the integration between Select Access and MPS, you need to understand that most critical integration points lie in the Web Interface itself. Therefore a better than working knowledge of Citrix's interface is required.

Understanding the Key Components of this Integration

To use Select Access to authenticate and authorize access for MPS resources, means that you have to configure MPS to use Select Access as its security provider. Integration primarily occurs through the following mechanisms:

- **Citrix user credentials:** There are two types of credential configurations to choose from. These credentials determine whether or not the page that is displayed at login is personalized or not:
 - *Common* credentials are shared by every Citrix user. The credentials are those of a valid Windows account. To authenticate these credentials, Citrix, passes a shared username, password and domain to the Windows operating system for authentication. As a result, all users see the same page when they log into MPS.

- *Unique* credentials are unique for each user. MPS’s customization feature allows you to create custom pages for each user. As a result, each user has a personalized Web page and has access to different applications.



All credential details are stored in cleartext because Citrix requires unencrypted account details. Information about the user simply gets collected and passed by the Enforcer plugin as is. If you have concerns over this implementation, you may choose the common credential mechanism. However, you will lose the ability to personalize pages for individual users.

As part of the authentication and authorization process, Select Access employs a specific Citrix rule that determines when and how the Enforcer plugin passes these user credentials to Citrix for further processing.

- **An Independent Computing Architecture file:** This Citrix file is downloaded on the user’s local workstation. Users connect directly to the MPS using this file. This file contains information about the following:
 - the user
 - the remote server location
 - the requested application

MPS reads the ICA file and runs the application the user selected from a remote machine.



ICA files can be shared with unauthorized users, thereby giving them a method to connect directly to MPS servers and consequently bypass Select Access authentication and authorization mechanisms entirely.

Citrix has released software that prevents this security breach, which is called “ticketing”. For details on configuring ticketing, refer to Citrix documentation.

These Citrix security mechanisms must be coupled with the Select Access’s access management systems. Unique features and important components that are affected by this integration include:

- **A Citrix-specific decision point**—You must understand the implications of your credential configuration. By creating a conditional rule in the Rule Builder, you achieve Single Sign-on functionality between the Select Access and Citrix systems.

- **An LDAP 3.0-compliant directory server**—If you configured your Citrix system to use unique user credentials, you need to ensure that your user entries are set up to reflect the required elements that authenticate the user on the Citrix system. At minimum, all user entries must contain user attributes for the username, password, and domain values. The attributes required to capture these can vary depending on the directory server you choose.
- **Authentication method restrictions:** Although Select Access has multiple authentication methods, only the following methods are supported with Citrix's unique credential configuration implementation:
 - Certificate
 - Password
 - Registration
 - Integrated Windows Authentication (NTLM & Kerberos).

SecurID and RADIUS methods are not supported in unique credential deployments: transient user entries created by these methods do not have a specific user account. Therefore, there are no individual/unique credential information stored for them, and these users cannot be authenticated on Citrix. For more details on transient user entries, refer to the *HP OpenView Select Access 6.0 Policy Builder Guide*.

- **An Enforcer plugin**—That intercepts all access requests on the MPS application server. It:
 - Forwards the user credentials stored in either the:
 - Directory server, which are collected by the Policy Validator from a specific user entry (for unique credentials)
 - Windows account, which are collected by the Enforcer plugin from the Citrix decision point plugin (for common credentials)

These credentials are used to authenticate the user on the Citrix system.

 - Enforces the outcome of the access request that has been evaluated by the Policy Validator.

- **The Policy Builder**—The Java GUI that provides you with a view of all Citrix users and available MPS assets that are made available through the Web Interface. The combination is displayed as a hierarchical matrix which can be easily expanded and contracted to facilitate quick navigation and simply manage your access and authentication policies.

► For a complete overview of all Select Access components, refer to the *HP OpenView Select Access 6.0 Installation Guide*.

Example of an Integrated Network Architecture

Figure 1 shows a deployment of Select Access and MPS over the Web Interface on the same corporate network. Other components for both Select Access and Citrix can be deployed across the network as you require.

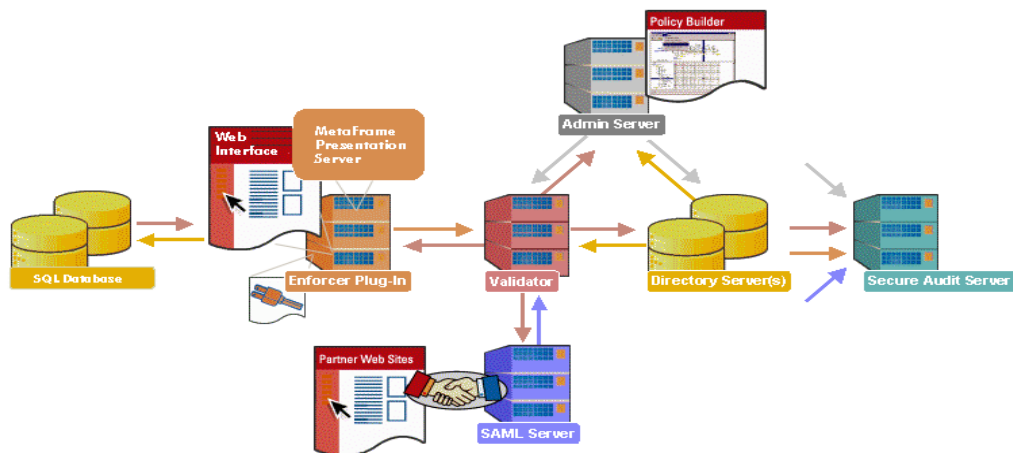


Figure 1 Select Access with the MPS Web Interface

The Citrix User Authentication Process

Select Access's authentication and authorization of Citrix users takes place within a small number of basic steps. Select Access components communicate via XML documents known as queries and responses. XML offers Select Access complete flexibility for data transmission and integration into existing

Citrix functions and/or other enterprise resources and applications. Select Access's authentication and authorization process for Citrix users and resources follows these steps:

- 1** A Citrix user makes a request to access an MPS application/resource with a Web browser over the Web Interface.
- 2** The Enforcer plugin intercepts this request, and passes details of the request to the Policy Validator, including any authentication information the user has provided.
- 3** The Policy Validator searches for the user account and checks the policy data for the function requested. Part of the policy data includes a conditional Citrix rule that contains the citrix decision point plugin. The Policy Validator caches the data from the directory for future retrieval.
- 4** Based on this combination of information, the Policy Validator returns a policy decision to the Enforcer plugin, including relevant personalization information (if applicable), which at minimum contains a username, password, and domain.
- 5** The Enforcer plugin enforces the validation result:
 - **If access is allowed:** The Enforcer plugin forwards the HTTP header that contains the username and any other personalization information to the Web Interface.
 - **If access is denied:** The Enforcer plugin displays the access denied page.
 - **If more data is required:** The Enforcer plugin displays the correct form to collect that data.

Integration Tasks

To ensure Select Access and the MPS function properly as a unit, you must follow a specific series of steps to integrate them correctly. [Table 1](#) summarizes the steps you need to perform, to configure and delegate all authentication and authorization responsibilities to Select Access.

Table 1 Integration Overview

Integration Tasks	Details
1 Set up user credentials that will be used to authenticate users on the Citrix system.	Setting Up Citrix User Credentials on page 14.
2 If you are deploying personalized content, configure MPS to use this feature.	Citrix documentation
3 To ensure authentication and authorization task are correctly configured and delegated to Select Access, replace certain Citrix files on your IIS Web server with those modified with Select Access-specific changes.	Files You Need to Replace on page 16
4 Deploy Select Access components to protect your Citrix assets.	Deploying Select Access on page 17

Setting Up Citrix User Credentials

[Understanding the Key Components of this Integration](#) on page 8 described the two different credential configurations you can employ with a Citrix system. Depending on your network environment, Select Access supports two different methods of delivering user credentials to MPS:

- Unique user credentials, which are stored in an LDAP directory server and accessed through the appropriate set of attributes.
- A common set of credentials that all Citrix users share.

Irrespective of the mechanism you choose, you configure properties for this authentication via a Citrix decision point plugin. This plugin is not part of the default installation of Select Access. You need to upload this plugin so that it is included as part of the plugins available to you in the Rule Builder.

Unique Credentials: Configuring User Credentials in a Directory Server

If you decide to implement the unique credential configuration, ensure the following credentials exist in your directory server for every user accessing MPS: username, password, and domain. For examples of attributes you can consider, see [Table 2](#).

- Make sure the password credential is in clear text. Some directory servers may encrypt the password. If this happens, Citrix cannot authenticate the user.
- Attributes vary from one directory server to the next. Consult your directory server's documentation for details on which attribute names it supports.

You are not restricted to just using the attributes listed in [Table 2](#). You can also add other attributes to user entries if you require additional details stored in the user entry. However, if you intend to add additional attributes, ensure you create the appropriate object class for those attributes.

Table 2 Directory Attributes You Can Consider

Credential Element	Possible Attribute Names	Example
username	<ul style="list-style-type: none"> • uid • sn • first name 	<ul style="list-style-type: none"> • ksmith • smith • kim
password	<ul style="list-style-type: none"> • password 	<ul style="list-style-type: none"> • abc123
domain	<ul style="list-style-type: none"> • domain 	<ul style="list-style-type: none"> • mycompany

Common Credentials: Creating a Common Windows Account

You can create a single Citrix user ID that is used by Select Access to allow all of your users to access the MPS Web Interface. These users therefore see the same Web Interface display; however, when they select an application, they are subsequently authorized by Citrix with their ICA credentials. This allows the system administrator to determine which user activated an application.

Ask your IT department to create a Windows account that includes a username, password, and domain of your choice. Once set up, you can configure Select Access to:

- Authenticate users
- Forward unique account information
- Allow/deny access to these users according to the policy in the individual user account.

Updating Citrix Files with Select Access-Specific Changes

This integration with Citrix automates user access to MPS' Web Interface. To simplify the integration process and ensure integration requirements are applied correctly, HP has modified specific files so that typical manual edits are not required. You only need to locate and update a few files with the updated ones provided to you by HP.

Files You Need to Replace

HP has modified the following files:

- `<IIS_Web_Root>\Citrix\MetaFrame\Site\include\loginUPD.inc`
- `<IIS_Web_Root>\Citrix\MetaFrame\Site\include\serverscripts\credentials.cs`
- `<IIS_Web_Root>\Citrix\MetaFrame\Site\include\serverscripts\.login.cs`

To use HP-modified files

- 1 Back up all original Citrix files.
- 2 Copy the Select Access-Citrix integration scripts from the following folder on the Select Access installation CD:

`\solutions\Citrix\Web Interface 3.0`

- 3 Overwrite the original files with those updated by HP.

Deploying Select Access

The goal of Select Access's configuration is to set up authentication and authorization so that the correct set of user values is forwarded to Citrix. These values are evaluated by Citrix to determine which content needs to be displayed—whether shared or personalized. [Table 3](#) outlines the tasks you need to consider.

Table 3 Setting up Select Access

Setup Task	Details
<p>Step 1: Install and configure an Enforcer plugin on the Citrix host (which is typically an IIS server).</p> <p>Note: The Select Access Administration server and the Policy Validator must already be running on your network.</p>	<ol style="list-style-type: none"> 1 Run the Select Access installer. 2 Click Next until you reach the Choose Select Access components installation screen. 3 Install the appropriate Enforcer plugin type for host computer. 4 When you are finished installing the Enforcer plugin, the Setup Tool automatically appears. 5 Since this integration doesn't require custom settings, choose a Default configuration for this plugin. 6 When you reach the Finish/Update Configuration setup screen, check the following two boxes: <ul style="list-style-type: none"> — Update Web server configuration to load the Enforcer plugin — Restart Web server 7 Click Finish. <p>For details, refer to the <i>HP OpenView Select Access 6.0 Installation Guide</i>.</p>
<p>Step 2: Since you are only adding one service, you can manually add the Citrix host to the Resources Tree as a service branch.</p> <p>You can use this entry to control access to its resources. However, to provide more granular access, proceed to Step 3. Otherwise, skip to Step 4.</p>	<ol style="list-style-type: none"> 1 Right-click a folder or the root of the Resources Tree. 2 Click New→Service. The New Service dialog box appears. 3 Name the resources and configure the service depending on whether or not the service is specific to a single server. For details see either: <ul style="list-style-type: none"> • Entering Information for a Non-Server-Specific Network Service on page 55 in the <i>HP OpenView Select Access 6.0 Policy Builder Guide</i>. • Entering Information for a Server-Specific Network Service on page 56 in the <i>HP OpenView Select Access 6.0 Policy Builder Guide</i>. 4 Click OK.

Table 3 Setting up Select Access (cont'd)

Setup Task	Details
<p>Step 3: If you want to provide more granular control to Citrix resources, manually add the URLs below the Citrix service.</p>	<ol style="list-style-type: none"> 1 Right-click the service under which you want to add resources. 2 Click New→Resource. The New Resource dialog box appears. 3 In the Name field, type in the URL of the resource you want to protect. 4 Click OK. <p>Note: For details on performing this procedure automatically, refer to the <i>HP OpenView Select Access 6.0 Policy Builder Guide</i>.</p>
<p>Step 4: Populate the Users Tree with known Citrix users.</p>	<ol style="list-style-type: none"> 1 If you have not already done so when initially configuring the Administration server, configure a User Data Location that maps to the directory server you are using. 2 Right-click this branch and click New→User. The New User dialog box appears. 3 Configure this dialog as required for your deployment. 4 Repeat steps 2-3 as often as is required. <p>For details, refer to the <i>HP OpenView Select Access 6.0 Policy Builder Guide</i>.</p>

Table 3 Setting up Select Access (cont'd)

Setup Task	Details
<p>Step 5: Upload the Citrix decision point plugin. Without this plugin, Select Access cannot pass identity information required by the Web Interface.</p>	<ol style="list-style-type: none"> 1 Click Tools→Configure Policy Plugins. The Configure Policy Plugins dialog box appears. 2 Click the Browse button located next to the Decision Point Plugins field and browse to the following folder on the Select Access installation CD: <ul style="list-style-type: none"> /solutions/Citrix/RuleBuilderPlugin <p>The following Citrix files are required for a successful integration:</p> <ul style="list-style-type: none"> — component.jar — component.xml — icon.gif — toolbaricon.gif <p>Warning! Select the folder name and not just any single files in the folder. Otherwise not all parts of the Citrix decision point can upload correctly. An incomplete upload breaks the Citrix-Select Access integration.</p> 3 Click the Upload button. This adds the Citrix decision point's property editor to the Rule Builder interface.

Table 3 Setting up Select Access (cont'd)


Setup Task	Details
<p>Step 6: After uploading the plugin, create a conditional rule that includes this node. Apply this rule to Citrix service you added in Step 2.</p> <p>This rule determines how Select Access passes credentials to MPS. Therefore, you must create a rule using this plugin and ensure you apply it against your Citrix users and the applications you want to protect.</p>	<ol style="list-style-type: none"> 1 From the Rule Builder, click File → New Rule. 2 Enter a name for the rule and click OK. 3 Select  from the toolbar. The Citrix Decision Point dialog appears. 4 To authenticate Citrix users with shared credentials, do the following: <ul style="list-style-type: none"> • Click the Use the following values to log into the Citrix server radio button (common credential configuration) to configure a common username, password, and domain. Citrix uses this data to deliver generic content for all users. • Configure the Credential Options by typing the shared Username, Password, and Domain in the corresponding fields 5 To authenticate users with individual credentials, do the following: <ul style="list-style-type: none"> • Click the Use the values stored in these user attributes to log into the Citrix server radio button (unique credential configuration) to configure the corresponding attributes that hold the unique values. Citrix uses this data to deliver personalized content. • Configure the Credential Options by typing a Username, Password, and Domain Attributes in the corresponding fields. You can use existing attributes or create new ones. <p>Example attribute names are listed in Table 2 on page 15.</p> 6 Save the rule.

Table 3 Setting up Select Access (cont'd)

Setup Task	Details
<p>Step 7: Enable SelectID and configure your authentication server to authenticate the Citrix user(s). Select Access then passes the collected credentials via the Citrix rule you created in Step 6.</p>	<ol style="list-style-type: none"> 1 On the SelectID column, enable SelectID for Citrix MPS service entry. Allow any resources under it to inherit its settings. The Authentication Properties dialog box appears. 2 Click the Authentication tab and configure one or more of the supported authentication servers. <p>Note: For details on authentication restrictions, see Understanding the Key Components of this Integration on page 8.</p> <p>For details on configuring authentication servers, refer to the <i>HP OpenView Select Access 6.0 Policy Builder Guide</i>.</p>
<p>Step 8: Assign access policies to your Citrix users and resources.</p>	<ol style="list-style-type: none"> 1 Set a Deny policy on the Unknown Users column. 2 Set the Citrix rule you created in step 5 against the top-level Citrix resource. 3 Apply other rules as required for your specific deployment. <p>Note: The rules you apply are inherited across multiple resources. Ensure you understand how policies are inherited so the Citrix rule does not get set against the wrong user/resource combinations. For details, refer to the <i>HP OpenView Select Access 6.0 Policy Builder Guide</i>.</p>

Testing your Integration

Testing your integrated deployment is important when integrating any combination of technologies, especially to ensure your configuration is complete and correct.

To test the integration solution

- 1 Request the Citrix MetaFrame Presentation Server homepage in your browser:

```
http://<Citrix_domain>/Citrix/MetaFrame/default/  
default.aspx
```

- 2** Check the message. If you have incorrectly deployed this integration, you will see an error message after logging into Select Access or be presented by another log in screen.

If you have correctly deployed this integration, you will see the main Citrix screen and its available applications.

