HP OpenView Select Access

Integration Paper for VACMAN RADIUS Middleware

Software Version: 6.0

for HP-UX, Linux, Solaris, and Windows operating systems

March 2004

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

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's `<install_path>/3rd_party_license` directory.

Trademark Notices

- Intel® and Pentium® are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- Java™ is a US trademark of Sun Microsystems, Inc.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.
- UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView Select Access web site at:

http://www.openview.hp.com/products/select/index.html

There you will find contact information and details about the products, services, and support that HP OpenView Select Access offers.

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

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

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information
- Security bulletins

Contents

Chapter 1

About this Integration Paper

This Integration Paper describes how to integrate the VACMAN RADIUS middleware with Select Access 6.0.

Select Access 6.0 is the last version HP performed interoperability-testing against. If you have any questions regarding the interoperability of your version of Select Access with the VACMAN RADIUS middleware, contact Global Support Services.

An overview of this document's contents is listed in Table 1.

Table 1: Integration Paper overview

This chapter...	Covers these topics...
Chapter 2, *Technologies overview*	• *Select Access*: what it is, what it does, and how it works. • *VACMAN RADIUS middleware*: what it is and what integration issues exist.
Chapter 3, *Integrating Select Access with VACMAN RADIUS middleware*	Describes what you need to do with VACMAN RADIUS middleware and Select Access to integrate these technologies.

Who is it for?

This Integration Paper is intended to instruct individuals or teams responsible for the following:

- Integrating Select Access with their VACMAN RADIUS middleware and its datasource of RADIUS users.
- Using Select Access to administer access policies to VACMAN RADIUS middleware users.

What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- *Select Access:* Ensures that you understand how integration with VACMAN RADIUS middleware affects Select Access's components.
- *VACMAN RADIUS middleware:* Ensures that you understand how to alter the existing configuration on your network so that transactions between the two systems occur seamlessly.

Related references

Before you begin to integrate Select Access with VACMAN RADIUS middleware, you may want to begin by familiarizing yourself with the contents of the following documents:

- *HP OpenView Select Access 6.0 Installation Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`)
- *HP OpenView Select Access 6.0 Network Integration Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`network_integration_guide.pdf`)
- *HP OpenView Select Access 6.0 Policy Builder Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`policy_builder_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Tutorial Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`dev_tut_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Reference Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`dev_ref_guide.pdf`)
- Hewlett-Packard, Application/portal servers *Integration Papers*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P.

Chapter 2

Technologies overview

This chapter introduces you to Select Access. It gives you an overview of the product, what it does, and what components are installed with this product.

What is Select Access?

Select Access is a centralized access management system that provides you with a unified approach to defining authorization policies and securely managing role-based access to on-line resources. It uses a collection of components that integrate with your network, to give you and your partners the ability to capitalize on the potential of extranets, intranets and portals. These components, along with the access policies you set, offer your Web and wireless users a seamless user experience by connecting them to dispersed resources and applications.

What does Select Access do?

Several features of Select Access extend its functionality beyond that of a simple authorization administration tool. It is a complete access management system, offering you a set of features to support your online relationships with your users and your content partners:

- *Supports single sign-on*
- *Enables user profiling*
- *Provides user password and profile management*
- *Delegates administration*
- *Provides an end-to-end auditing system*
- *Automates the discovery and maintenance of corporate resources*

Together, this extended functionality provides a simplified experience for both the end user and those responsible for managing what the user sees and interacts with.

Supports single sign-on

To improve user satisfaction, Select Access incorporates a Web Single Sign-On (SSO) capability. This means users can sign on once to access

all permitted resources and have their information stored for future access. Select Access supports transparent navigation between:

- Multiple proprietary domains: For organizations with ownership of multiple Web sites.
- Multiple partnering domains: For on-line business partners, so they can securely share authentication and authorization information across corporate boundaries that have separate:
  - user databases
  - authorization policies
  - access management products

Using SSO means that users do not have to remember multiple passwords or PINs, thereby reducing the amount of help desk support.

Enables user profiling

A user is represented as a user entry that is stored in a directory server. When you create a user entry, you can also define a set of attributes that describe that user, which become part of the user's profile. The values contained in the attribute can be used in two ways:

- *To determine level-of-access with roles*: Role-based access allows you to configure and apply policies automatically, according to the attribute values stored in the user's profile.
- *To determine delivery-of-content*: Select Access exports user attributes and their values as environment variables, so that applications can use the profile information to personalize Web pages and to conduct transactions.

A user's profile dynamically changes as a user conducts transactions with your organization. As attributes in the profile change, so too can the role the user belongs to. For example, a customer's profile may contain his current bank balance, date of last transaction, and current credit limit—any of which can change from moment to moment.

This capability of Select Access makes development of Web applications much easier, because programmers do not have to develop (or maintain) complex directory or database access codes to extract entitlement information about each user.

Provides user password and profile management

Select Access's password and profile management feature makes it easy for users to conduct business and minimize the demand on technical resources that can best be employed elsewhere. This feature includes the following principles:

- *Password administration*: Allows you to set the policies and expiration times for user passwords. Select Access automates reminders and messages. Other administration features include:

  - Profile lockout and re-activation
  - Password history lists
- *Self-servicing*: Allows users to initiate:
  - The definition of new or existing passwords, which are controlled by the password policy you create.
  - The modification of profile data, which is predefined by the attributes you select. Typically, these attributes are the same attributes the user provides when they register with your organization. If the user is already known to you (like an employee or a supplier), you can pre-populate the values for them.

By allowing users to self-manage passwords and profile data, you reduce the amount of help desk support.

Delegates administration

Delegated Administration allows for delegation of both user and policy management, providing more control for decentralized administrators. Select Access's delegation is highly efficient: it supports sub-delegation to multiple tiers of administrators, which mimics real-world organization charts. This decentralized approach to administration:

- Reduces administrative bottlenecks and costs.
- Puts the power to manage users in the hands of those who best understand those users.

Provides an end-to-end auditing system

Select Access can record all access and authorization actions, as well as all policy administrative changes to any number of outputs, such as:

- The Baltimore Secure Audit server
- JDBC-compliant databases
- Local files
- Platform-specific log files
- Email

Of all output choices, the Secure Audit server is the most useful: not only does it collect messages from different components on a distributed network, but it also allows you to digitally-sign all audit entries and ultimately create a report from the outputs collected.

Automates the discovery and maintenance of corporate resources

In order to define and enforce authorization, Select Access must be aware of all the resources on your network, as well as the users who want to access them. Select Access uses the directory server as the central repository for policy data, which includes the resource listing. You can deploy special HTTP/HTTPS-specific plugins to automatically scan any given network, thereby enumerating available services and resources. As services and resources are enumerated by the plugin, it adds them hierarchically in the Policy Builder's Policy

Matrix. Unlike other products that require manual data input (where a simple typing error can put the security of resources at risk) Select Access saves administrators' time and improves accuracy.

How does Select Access work?

Select Access delivers the core of its authorization and authentication functionality with the following technical components:

- *Policy Builder*: Allows full or delegated administrators to define the authentication methods and authorization policies with an easy-to-use administration grid.
- *Policy Validator*: Serves the access decision to the Enforcer plugin after it accepts and evaluates the user's access request with the policy information retrieved from the directory server that holds your Policy Store.
- *Enforcer plugin*: Acts as the agent for Select Access on the Web/application server. The Enforcer plugin enforces the outcome of the access request that has been evaluated by the Policy Validator.
- *SAML server*: Handles the logistics of transferring users between your web sites and those of your partners.

These core components form a sophisticated and consistent architecture that easily adapts to any existing network infrastructure. Primarily XML and Java-based, you can readily extend Select Access to meet the needs of future security requirements.

The authentication process

Select Access's authentication and authorization of Web-based or wireless 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 and future applications, whether Web or non-Web based. Select Access's authentication and authorization process follows these steps:

1. A user makes a request to access a resource.
2. The Enforcer plugin passes details of the request to the Policy Validator, including any authentication information provided.
3. The Policy Validator collects user and policy data from the directory and then caches it for future retrieval.
4. Based on this combination of information, the Policy Validator returns a policy decision to the Enforcer plugin, including relevant information to dynamically personalize the user experience.

Other Select Access components

Other Select Access components provide the support system for Select Access's core components:

- *Administration server & Setup Tool*: As a mini Web server, the Administration server is responsible for the configuration of core components and deployment of the Policy Builder applet in a user's browser. The Setup Tool is a client of the Administration server: it is the interface that allows you to quickly set up and deploy Select Access.
- *Secure Audit server*: Collects and manages incoming log messages from Select Access components on a network.

Third-party components Select Access integrates with

Other third-party components that are integral to an effective Select Access solution:

- *Directory server – LDAP v3.0 compliant*: is the foundation of a Select Access-protected system. It acts as the repository of information. Depending on how you have set up your directory system, Select Access can use one or more directory servers to store:
  - A single policy data location
  - One or more user data locations
- *Web/Application/Portal/Provisioning servers*: are third-party technologies that use Select Access as their authorization and access management system. Depending on your server technology, you can use Select Access's native SSO and/or personalization solution rather than use the server's built-in alternative for a more robust solution.

Figure 1 illustrates how Select Access and third-party components interact with each other.

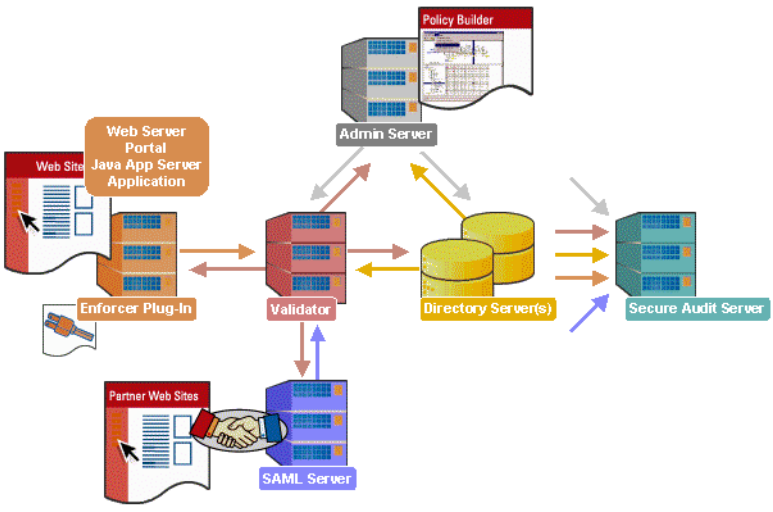

Figure 1: Select Access system architecture

Custom plugins you can customize functionality with

To more efficiently capture your organization's business logic, you can use Select Access's APIs to build custom plugins. Plugins that you can customize functionality with include:

- *Authentication plugins*: A custom Policy Builder authentication plugin allows you to tailor which kinds of authentication methods are available to better meet the needs of your organization. A Policy Builder authentication method plugin allows administrators to use and configure the authentication server for this method via a dialog box. As with the decision point plugin, this dialog box is a property editor that allows security administrators to configure the authentication server.
- *Decision point plugins*: A custom Rule Builder decision point plugin allows you to tailor how rules are built to better meet the needs of your organization. A Rule Builder decision point plugin allows administrators to use and configure the criteria for the decision point via:
  - The icons that represent that decision point on both the toolbar and the rule tree.
  - The dialog box, known as a property editor, that allows security administrators to configure it.
- *Policy Validator decider plugins*: The Validator-specific counterpart of a decision point plugin, the decider plugin allows you to capture the evaluation logic for your custom decision point (described above), so that the Policy Validator can evaluate users based on the information it collects.
- *Resource discovery plugins*: These plugins allow you to customize how resources are scanned on your network.
- *Enforcer plugins*: A new Enforcer plugin allows you to customize the backend application logic by enforcing the decision that the Policy Validator returns to the Enforcer plugin's query.
- *Additional Web/Application/Portal/Provisioning server specific plugins*: These plugins can be included to handle specific integration details between the third-party technology and Select Access. For example, the Domino server requires a `site_data` plugin if you need to transfer site data between Select Access and Domino.

What is VACMAN RADIUS middleware?

VASCO's VACMAN RADIUS middleware (VRM) functions as a back-end authentication server with support for the RADIUS protocol, verifying the Digipass One-Time Passwords (OTP).

VASCO's Digipass enables users to generate OTPs that safeguard access to corporate networks, thereby allowing for more secure transactions. By using Digipass's patented technology, corporations eliminate the weakest link in any security infrastructure: static passwords. These passwords are easily stolen, guessed, reused, or shared.

Corporations who have purchased VASCO's VRM can deploy Digipass as:

- A small hand-held device
- A smart card reader
- Computer software
- PDAs
- Cell phones

Integration point

Via the RADIUS authentication server plugin you configure, Select Access and VACMAN RADIUS middleware provide corporate networks a web-based single sign-on (SSO) solution with strong user authentication. User authentication is a key element of Select Access, which requires a user data source—typically in the form of an LDAP directory server. For Select Access to successfully integrate with the VRM server, it needs to share the same user data source the VRM server uses.

The Policy Validator uses a RADIUS authentication plugin to accomplish this task. The plugin acts as an agent for the VACMAN RADIUS middleware in the Policy Validator itself, which allows the Policy Validator to perform the authentication on users, and thereby ensure that a user is who he or she claims to be. You configure a RADIUS authentication plugin to contact the VRM server. This configuration is needed so that the Policy Validator can:

- Send RADIUS user authentication information to the server.
- Make the correct authentication decision based on the response the Policy Validator receives from the server.

Integration issues for VACMAN RADIUS middleware

Because integration mainly occurs with the Policy Validator's RADIUS authentication plugin, bear the following issues in mind when implementing this solution:

- *Installation and configuration pre-requisites:* You must already have installed the VRM software according to the instructions provided with the product. Additionally, you need to have already entered some tokens into the VRM server's data source.
- *Transient user entry support*: Because VACMAN RADIUS middleware maintains its own user data source, the Policy Validator still needs to authenticate a user, even though there is no entry for that user in the LDAP directory server. Consequently without some kind of user entry, subsequent attempts to reuse authentication information (for example, to load a Java application on a related Web page) would either fail, or require repeated reauthentication because authentication information changes within a short time frame.

  In order to avoid these problems, Policy Validator has a mechanism for handling these special cases: it "synthesizes" user entries by permanently caching data to appear as if it were retrieved from the directory server. This creates a transient user entry on the Users Tree. The Policy Validator does this by concatenating:

  — The user ID that has been authenticated via the VRM server.

  — The DN of the organizational unit (that is, the group or folder you create for this purpose) that is used to specify access policies for synthesized users, without knowing in advance who those users are.

  For more details on transient user entries and how they are created, see Chapter 7, *Setting up authentication servers*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.
- *Access policies*: Because VASCO's VACMAN RADIUS middleware is an authentication mechanism, it does not perform authorization. Therefore, Select Access is not only used to configure the RADIUS plugin for the Policy Validator, but also to create access policies that the Policy Validator uses to authorize asset requests made by users authenticated by the VACMAN RADIUS server. With the transient user mechanism described in the previous bullet, you can now set access policies or conditional rules for VRM users—even though they are not stored as entries in the LDAP directory server.

The benefits of an integrated solution

Integrating Select Access with VACMAN RADIUS middleware offers the following main benefits:

- *Consolidated policy management:* You can set all the policies and resources for your corporate site using only Select Access. Using only one policy management tool makes policy administration easier.
- *Single sign-on (SSO):* SSO is an important feature of Select Access that allows users to authenticate once to any number of third-party SSO-enabled applications—either on single or multiple domains. Once authenticated by Select Access, a user's credentials act like a passport on a network, giving users access to distributed portal content, groupware, workflow and client/server applications.

  For example, a user might authenticate against an IIS Web server, which is protected by an IIS Enforcer plugin. Via the Policy Validator, this user information is shared with the VRM server, so that the user is not required to reauthenticate on a different system as well.

Chapter 3

Integrating Select Access with VACMAN RADIUS middleware

Successfully integrating Select Access with VACMAN RADIUS middleware requires that you configure both systems correctly. To that end, configuration activities take place in two distinct steps:

1. Configure the VRM server so that Select Access is one of its clients and that the VRM server's user data can be shared with the Policy Validator.

   For details, see *Configuring the VACMAN RADIUS middleware server* on page 13.

2. Install and configure Select Access so that authentication data can be correctly exchanged with the Policy Validator. The Policy Validator sends RADIUS authentication information to a VRM server for validation.

   For details, see *Installing and configuring Select Access* on page 16.

Configuring the VACMAN RADIUS middleware server

You need to perform specific configuration steps on the VACMAN RADIUS middleware's Administration interface.

Table 1 describes what you need to do to fully expose user data to Select Access. Once this data is exposed to Select Access, the Policy Validator can authenticate the user on the Select Access system and determine what access privileges the user has for a particular resource.

Table 1: Setting up the VACMAN RADIUS middleware

This step...	Details on how to do it...
Step 1: Configure the VRM server with the VACMAN RADIUS middleware Admin GUI.	1. Log into the VACMAN RADIUS middleware - Admin GUI. 2. Click the **Server Tab** and configure the following: a. Check that the **Server IP** address is correct. b. Set the **Incoming RADIUS Authentication Port** to 1645 and **Incoming RADIUS Accounting Port** to 1646. **Note:** If you have used values other than these defaults, remember the incoming port. You need this port to configure Select Access. c. In the **Authenticator** droplist box, choose `Local Server`. d. If you require debugging, check the **Enable Debug Trace Output** box. 3. Click the **Auto Manage** tab and uncheck the following boxes: — **Autoassign Token on User Create** — **Dynamic User Registration** 4. Click **File>Save** to save these changes.

Table 1: Setting up the VACMAN RADIUS middleware (Continued)

This step...	Details on how to do it...
Step 2: Configure RADIUS settings to allow Select Access as a client.	1. Click the **RADIUS** tab. 2. Click the **Client** tab. 3. Click the **New** button to create a new client definition for Select Access. 4. Configure the following fields: — Enter the IP address of the Policy Validator in the **IP Address** cell. — Type the secret used by Select Access (for example, `VASCO`) in the **Shared Secret** cell. **Note:** Remember the secret you type. You need this secret to configure Select Access. — Check the **Proxy** box. 5. Click the **Save** button.
Step 3: Ensure you have set up your users to use RADIUS authentication in Challenge/Response mode.	1. Select a user name in the left navigation bar and click the **User** tab. 2. Modify the following fields as needed: — In the **Admin Privilege** droplist box, choose `Normal User`. — In the **Authenticator** droplist box, choose `Default`. — Unassign the existing token and instead assign a challenge/response token (for example, type a suitable serial number in the **Serial Number** field like `009700001`; in the **Application** field, identify an application like `appl3`). 3. Click **File>Save** to save these changes. 4. Repeat steps 1-3 for each user that Select Access needs to authenticate.

Installing and configuring Select Access

Once you have set up your VRM server, you can begin to install and configure Select Access. Table 2 describes the steps you need to take to set up Select Access with the VACMAN RADIUS middleware.

These steps assume that all Select Access components are deployed on the same network as your directory server and VRM server.

Table 2: Setting up Select Access

This step...	Details on how to do it...
Step 1: Deploy Select Access on your network according to your specific needs.	See the *HP OpenView Select Access 6.0 Installation Guide* as well as Chapter 4, *Deploying Select Access on your network*, in the *HP OpenView Select Access 6.0 Network Integration Guide*.
Step 2: With your Administration server up and running, launch the Policy Builder and populate the axes of the Users Trees and Resources Tree.	See Chapter 4, *Building your Users and Resources Trees*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.
Step 3: Because the RADIUS server performs user authentication—and not the Policy Validator—HP recommends that you create a group or folder that allows transient VACMAN RADIUS middleware users to be temporarily added to the Users Tree in a single location. This allows you to set a access rules for users authenticated by the VRM server, despite not having a corresponding user entry in the LDAP directory server.	1. Right-click a folder or user location branch in the Users Tree, then click **New>Folder**. The **New Folder** dialog box appears. 2. Configure the fields of the **Folder Information** tab as required. For example, in the **Folder Name** field, name the folder in such a way that you can easily identify it as being used by the Policy Validator to create temporary duplicate entries for those users authenticated by the VRM server (for example, `Authenticated VRM users`). 3. Click **OK** to commit these changes to the directory server for that user location. The folder is added to the Users Tree.

Table 2: Setting up Select Access (Continued)

This step...	Details on how to do it...
Step 4: Create a RADIUS authentication server. **Note:** Before the RADIUS server can challenge the user, the user must be a known user and consequently is required to log into the VRM server first. Only then can the server challenge the known user for the OTP. If the OTP the user supplies matches the OTP on the VRM server, the user is authenticated.	1. Click **Tools>Authentication Servers**. The **Authentication Servers** dialog box appears. 2. Click the **Add** button. The **Authentication Method** dialog box appears. 3. Configure a RADIUS server: a. In the **Server Name** box, enter `VASCORadius` as the name for the server. b. Select **RADIUS** as your authentication method. c. Click **OK**. The **New RADIUS Server** dialog box appears. d. In the **Specify location for user lookups** pull-down list, select the folder you created in Step 3 of this table. Otherwise, the Policy Validator cannot find the transient user entry, and it consequently cannot authorize the VRM user to access a resource. e. In the **Specify policy location for newly authenticated users without user entry** field, choose the location of the Policy Store you configured for Select Access. This is the directory location you configured during the Administration server's setup. For details, see Chapter 5, *Configuring the Administration server*, in the *HP OpenView Select Access 6.0 Installation Guide*. f. Unless you have changed the name of the form templates used by the Enforcer plugin to collect user credentials and the OTP from the user, accept the default filenames shown in the fields of the **RADIUS Forms** group box.
	Step details continued on next page...

Table 2: Setting up Select Access (Continued)

This step...	Details on how to do it...
	g. Click the **Add** button to create a new RADIUS server definition for your VRM server. h. Configure the properties used by the Policy Validator plugin for the VRM server. These properties include a valid domain name or IP address of the server, the VRM server's port number (`1645` by default), the shared secret used by the OTP (for example, `VASCO`), as well as appropriate timeout and retry values. The latter values can vary depending on your security sensitivity. **Note:** Some of these values are the same values you configured in Steps 1 and 2 of Table 1. 4. Click **OK** to commit the authentication server you configured to the Policy Store. **Note:** The Policy Builder checks the validity of the information before it is written to the directory server. If an incorrect value has been entered at any point, an error message directs you to the problem and offers a potential solution.
Step 5: Enable SelectID so that VRM users can be authenticated by the VRM server you configured in the previous step.	1. Where security-sensitive resources and the **SelectID** column intersect, right-click this cell in the Policy Matrix and click **Enable SelectID** from the popup menu. The **Authentication Properties** dialog box appears. 2. Click the **Authentication** tab. This tab allows you to determine which authentication server(s) the Policy Validator will use to authenticate the user. 3. Click the **Add** button. The **Available Authentication Servers** dialog box appears. This dialog box contains the following lists: — The **Available Servers** list contains the authentication servers you have configured. — The **Selected Servers** list contains the authentication servers to be used with SelectID.
	Step details continued on next page...

Table 2: Setting up Select Access (Continued)

This step...	Details on how to do it...
	4. In the **Available Servers** list, select `VASCORadius` and click the **Add** button. This server appears in the **Selected Servers** list. 5. If you want to authenticate the user with any other type of authentication server as well, repeat steps 3-4. 6. If you have configured multiple authentication servers for SelectID, reorder the authentication servers in the **Selected Servers** list. Do this by selecting the corresponding server name and moving it with the corresponding up or down arrow button. **Note:** Reordering the list of selected authentication servers defines in which order these servers authenticate the users. 7. Click **OK** to close the **Available Authentication Servers** dialog box. 8. If you want to personalize the authenticated users experience, click the **Personalization** tab to export data from your directory server into the environment variables required to generate dynamic Web pages. For details, see Chapter 6, *Authentication fundamentals: SelectID and personalization*, in the *HP OpenView Select Access 6.0 Policy Builder Guide* 9. Click **OK** to close the **SelectID Properties** dialog box and commit the changes to the Policy Store
Step 6: Set access policies and conditional access rules as required. You can only set one rule per resource for all users in the folder you created for transient user in Step 3 of this table.	For details, see Chapter 8, *Controlling network access*, and Chapter 9, *Creating policy rules with the Rule Builder*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.