

HP Select Identity Software

Connector for RSA ACE/Server

Connector Version: 1.01

Installation and Configuration Guide

Document Release Date: September 2007
Software Release Date: September 2007



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2006-2007 Hewlett-Packard Development Company, L.P.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>). Portions Copyright © 1999-2003 The Apache Software Foundation. All rights reserved.

Select Identity uses software from the Apache Jakarta Project including:

- Commons-beanutils
- Commons-collections
- Commons-logging
- Commons-digester
- Commons-httpclient
- Element Construction Set (ecs)
- Jakarta-poi
- Jakarta-regexp
- Logging Services (log4j)

Additional third party software used by Select Identity includes:

- JasperReports developed by SourceForge
- iText (for JasperReports) developed by SourceForge
- BeanShell
- Xalan from the Apache XML Project
- Xerces from the Apache XML Project
- Java API for XML Processing from the Apache XML Project
- SOAP developed by the Apache Software Foundation
- JavaMail from SUN Reference Implementation
- Java Secure Socket Extension (JSSE) from SUN Reference Implementation
- Java Cryptography Extension (JCE) from SUN Reference Implementation
- JavaBeans Activation Framework (JAF) from SUN Reference Implementation

- OpenSPML Toolkit from OpenSPML.org
- JGraph developed by JGraph
- Hibernate from Hibernate.org
- BouncyCastle engine for keystore management, bouncycastle.org

This product includes software developed by Teodor Danciu (<http://jasperreports.sourceforge.net>). Portions Copyright © 2001-2004 Teodor Danciu (teodord@users.sourceforge.net). All rights reserved.

Portions Copyright © 1994-2004 Sun Microsystems, Inc. All Rights Reserved.

This product includes software developed by the Waveset Technologies, Inc. (www.waveset.com). Portions Copyright © 2003 Waveset Technologies, Inc. 6034 West Courtyard Drive, Suite 210, Austin, Texas 78730. All rights reserved.

Portions Copyright © 2001-2004, Gaudenz Alder. All rights reserved.

Trademark Notices

AMD and the AMD logo are trademarks of Advanced Micro Devices, Inc.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation in the United States, other countries, or both.

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

Microsoft® and Windows® 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

You can visit the HP software support web site at:

<http://www.hp.com/go/hpsoftwaresupport>

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into 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 sign in. Many also require an active support contract.

To find more information about support access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Contents

1	Documentation Map	7
2	Introduction	9
	About HP Select Identity	9
	About Connectors	9
	About the RSA Connector	9
	Overview of Installation Tasks	10
3	Installing the Connector	11
	RSA Connector Files	11
	System Requirements	11
	Extracting Contents of the Schema File	12
	Installing the Connector RAR	12
4	Installing the Agent	13
	About the Agent	13
	Installing the RSA Connector Agent	13
	Starting the Agent	21
	Configure RSA ACE/Server to Start the Agent for the First Time	21
	Start the Agent	22
	Modifying Configuration Settings	22
	properties.ini	23
	opAttribute.properties	24
	developer_configurations.properties	25
	runAgent.cmd	25
	Updating the Agent with Password Changes	25
	Update the Agent with RSA Password Change	26
	Update the Agent with Select Identity Password Change	26
	Verifying the Agent Operation	26
	Getting Help	27
5	Configuring the Connector with Select Identity	29
	Configuration Procedure	29
	Add a New Connector	29
	Add a New Resource	29
	Map Attributes	32
	Attribute Behavior	35
	Add Service	36

6	Uninstalling the Connector.....	43
	Uninstalling the Agent	43
A	Troubleshooting	45

1 Documentation Map

This chapter describes the organization of HP Select Identity connector documentation and provides necessary information on how to use the documentation set to install and configure the connectors.

[Figure 1](#) illustrates the documentation map for Select Identity connector. For a list of available product documentation, refer to the [Table 1](#).

Figure 1 Documentation Map



Table 1 Connector Documentation

Document Title and Filename	Contents	Location
<i>Release Note</i> RSA Connector v1.01 Release Note.htm	This file contains necessary information on new features of the connector, enhancements, known problems or limitations, and support information.	/Docs/ subdirectory under the connector directory.
<i>Connector Deployment Guide (for Select Identity 4.20)</i> connector_deploy_SI4.20.pdf	Connector deployment guides provide detailed information on: <ul style="list-style-type: none"> • Deploying a connector on an application server. • Configuring a connector with Select Identity. Refer to these guides when you need generic information on connector installation.	/Docs/ root directory on the product's CD media.
<i>Connector Deployment Guide (for Select Identity 4.10-4.13)</i> connector_deploy_SI4.13.pdf		
<i>Connector Deployment Guide (for Select Identity 4.0-4.01)</i> connector_deploy_SI4.pdf		
<i>Connector Installation and Configuration Guide</i> RSA_guide.pdf	Connector installation and configuration guide provides installation instructions for a specific connector. It contains resource specific configuration details.	/Docs/ subdirectory under the connector directory.

2 Introduction

This chapter gives an overview of the HP Select Identity connector for RSA ACE/Server. An HP Select Identity connector for RSA ACE/Server enables you to provision users and manage identities on RSA ACE/Server. At the end of this chapter, you will be able to know about:

- The benefits of HP Select Identity.
- The role of a connector.
- The connector for RSA ACE/Server.

About HP Select Identity

HP Select Identity provides a new approach to identity management. Select Identity helps you automate the process of provisioning and managing user accounts and access privileges across platforms, applications, and corporate boundaries. Select Identity communicates with the enterprise information system through connectors, and automates the tasks of identity management. The enterprise information system, which is also referred to as **resource**, can be a database, a directory service, or an ERP package, among many others.

About Connectors

You can establish a connection between a resource and Select Identity by using a connector. A connector is resource specific. The combination of Select Identity and connector helps you perform a set of tasks on the resource to manage identity. A connector can be **unidirectional** or **bidirectional**. A unidirectional connector helps you manage identities from Select Identity, but if any change takes place in resource, it cannot communicate that back to Select Identity. On the other hand, a bidirectional connector can reflect the changes made on resource back to Select Identity. This property of bidirectional connectors is known as **reverse synchronization**.

About the RSA Connector

The connector for RSA ACE/Server — hereafter referred to as RSA connector — enables Select Identity to perform the following tasks on RSA ACE/Server systems:

- Add, update, and remove users
- Retrieve user attributes
- Enable and disable users

- Verify a user's existence
- Change user passwords
- Reset user passwords
- Retrieve all entitlements
- Grant and revoke entitlements to and from users

It is a bidirectional agent-based connector. The mapping file defines how Select Identity user attributes are mapped to RSA ACE/Server's user attributes.



The RSA connector can be used with Select Identity 4.01-4.20.

Overview of Installation Tasks

Before you start installing the connector, you must ensure that system requirements and all the installation prerequisites are met. Refer to the [Table 2](#) for an overview of installation tasks.

Table 2 Organization of Tasks

Task Number	Task Name	Reference
1	Install the connector on the Select Identity server.	See Installing the Connector on page 11.
	— Meet the system requirements.	See System Requirements on page 11.
	— Extract contents of the Schema file (file that contains the mapping files for the connector) to location on the Select Identity server.	See Extracting Contents of the Schema File on page 12.
	— Install the Resource Adapter Archive (RAR) of the connector on an application server.	See Installing the Connector RAR on page 12.
2	Install the agent on the RSA ACE/Server resource machine.	See Installing the Agent on page 13.
3	Configure the connector with the Select Identity server.	See Configuring the Connector with Select Identity on page 29.

3 Installing the Connector

This chapter elaborates the procedure to install RSA connector on Select Identity server. At the end of this chapter, you will know about

- Software requirements to install the RSA connector.
- Prerequisite conditions to install RSA connector.
- Procedure to install RSA connector.

RSA Connector Files

The RSA connector is packaged in the following files in the RSA directory on the Select Identity Connector CD:

Table 3 RSA Connector Files

Serial Number	File Name	Description
1	<ul style="list-style-type: none">• RSAConnector_420.rar for WebSphere• RSAConnector_420WL9.rar for WebLogic	The Resource Adapter Archive (RAR) file contains the connector binaries.
2	RSASchema.jar	The Schema file contains the XML (RsaConnectorMappingFile.xml) and XSL (RsaConnectorMappingFile.xsl) files that contain the user attribute information of RSA ACE/Server.
3	RSASetup.zip	The ZIP file contains the executable for agent installation.

System Requirements

The RSA connector is supported in the following environment:

Table 4 Platform Matrix for RSA connector

Select Identity Version	Application Server	Database
4.01-4.20	The RSA connector is supported on all the platform configurations of Select Identity 4.01-4.20.	

This connector is supported with RSA ACE/Server, version 5.2, on Windows.

Extracting Contents of the Schema File

The Schema file of the connector contains necessary mapping information to map resource attributes to Select Identity. Extract contents of the `RSASchema.jar` file to a directory that is in the application server `CLASSPATH`. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instruction to extract contents of the Schema file.

Installing the Connector RAR

To install the RAR file of the connector (such as `RSAConnector_420.rar`) on the Select Identity server, you must copy the file to a local subdirectory on the Select Identity server, and then deploy on the application server. Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on deploying a RAR file on an application server.



While deploying the RAR on WebSphere, enter the JNDI Pool Name as `eis/RSAConnector`.

4 Installing the Agent

You must install the agent on the resource system to enable reverse synchronization. This chapter gives you an overview of the agent for RSA connector and the procedure to install the agent on the RSA ACE/Server resource. At the end of the chapter, you will be able to know about:

- The role of an agent.
- The procedure to install an agent.
- The procedure to modify the configuration settings after agent installation.

About the Agent

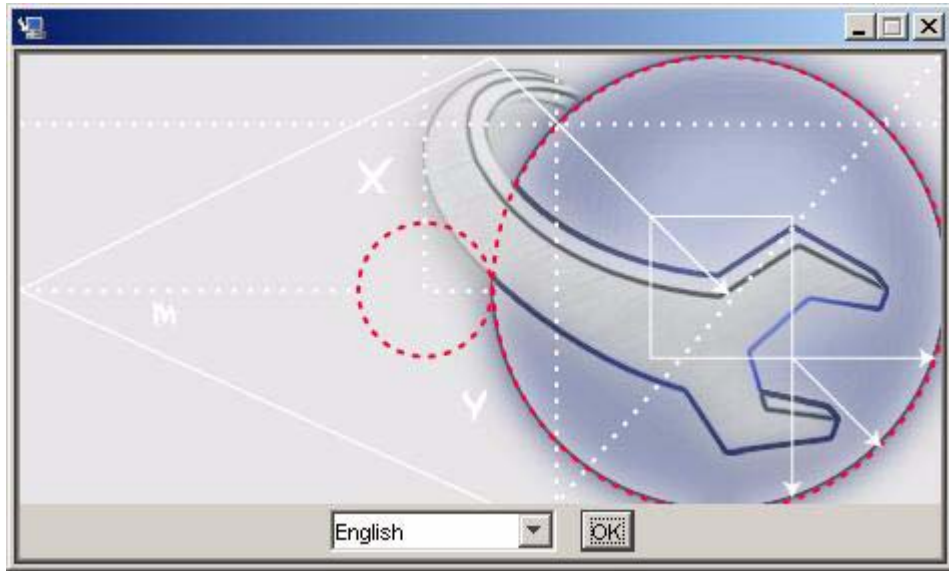
The connector communicates to RSA ACE/Server with the help of an agent. For forward operations (Select Identity to RSA ACE/Server), the connector communicates with the agent and agent performs the provisioning on the resource. Agent sends back any changes made on RSA ACE/Server to Select Identity web service in the form of SPML requests. The agent installer program is packaged with the file `RSASetup.zip`.

Installing the RSA Connector Agent

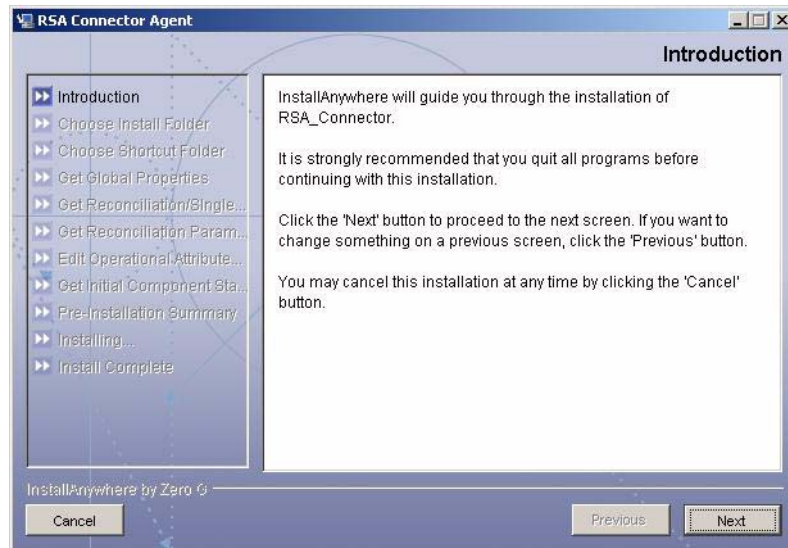
Before you start installing the agent on the RSA ACE/Server machine, make sure that JDK v1.4.2 is installed on the resource system. Perform the following steps to install the agent:

- 1 Extract contents of the `RSASetup.zip` file to a directory (for example, `<Extract_Dir>`) on the RSA ACE/Server system. The directory structure — `Windows/Disk1/InstData/NoVM` — is created under `<Extract_Dir>`.

- 2 Run the `install.exe` file (located in `<Extract_Dir>/Windows/Disk1/InstData/NoVM`). The installation wizard appears.



- 3 Select the language of your choice and click **OK**. The Introduction screen appears.



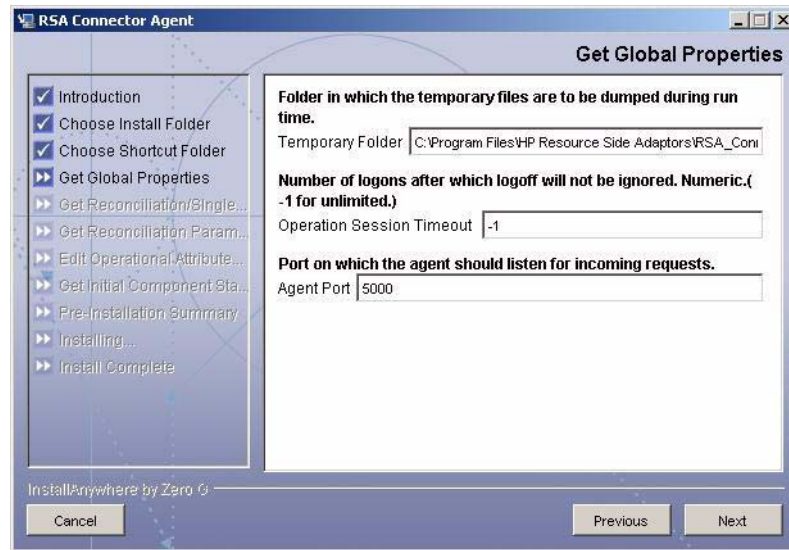
- 4 Click **Next**. The Choose Install Folder screen appears.



- 5 Type the location of the installation and click **Next**. The Choose Shortcut Folder screen appears.



- 6 Select the location where you want to create the shortcut icon, and then click **Next**. The Get Global Properties screen appears.



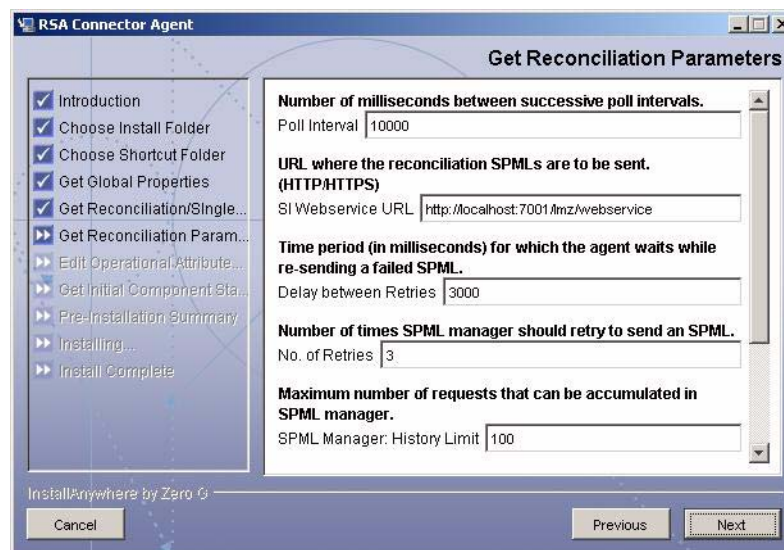
- 7 Type the appropriate global properties in the text boxes. Refer to the table below for description of each property.

Serial Number	Property	Default Value	Description
1	Temporary Folder	C:\Program Files\HP Resource Side Adaptors\RSA_Connector\temp\	The location where the agent places the temporary files created during the operation. These files are needed by the agent to perform queries on the RSA database. The default temp folder is located under the installation folder. It is recommended to keep the default location so that all the temporary files are removed automatically during uninstallation.
2	Operation Session Timeout	-1	The Operation Session Timeout gives the number of logoff requests, after which the agent will terminate the connection with the RSA server. Value -1 indicates the connection should never be disconnected.
3	Port Number	5000	The port on which the agent listens for the incoming requests.

After typing in the global properties, click **Next**. The Get Reconciliation/ Single Sign-on Credentials screen appears.



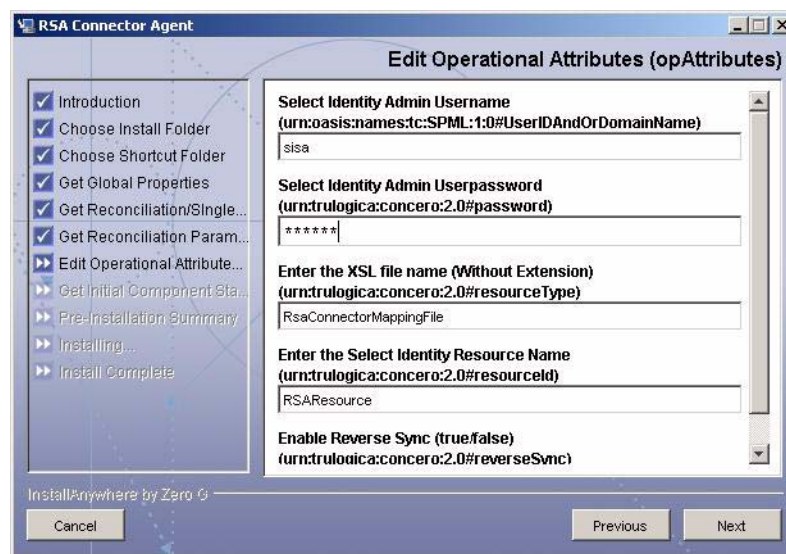
- 8 Type the connection credentials for reconciliation (reverse synchronization) and click **Next**. The Get Reconciliation Parameters screen appears.



- 9 Refer to the table below to type the parameters.

Serial Number	Parameter	Default Value	Description
1	Poll Interval	10000	The time interval (in milliseconds) between successive polling operations. on RSA server by agent.
2	Select Identity Webservice URL	http://localhost:7001/lmz/webservice	URL of Select Identity web service.
3	Delay between Retries	3000	The time period (in milliseconds) for which the agent waits before re-sending a failed SPML.
4	No. of Retries	3	The number of times the SPML manager must retry to send an SPML to Select Identity web service.
5	SPML Manager: History Limit	100	The maximum number of requests that can be accumulated in the SPML manager.
6	SPML Manager: Delay before sending SPML	5000	The time interval (in milliseconds) for which the SPML manager must wait before sending an SPML request.
7	SPML Manager: Polling Interval	10000	The time interval (in milliseconds) after which the SPML manager tries to send the accumulated requests.

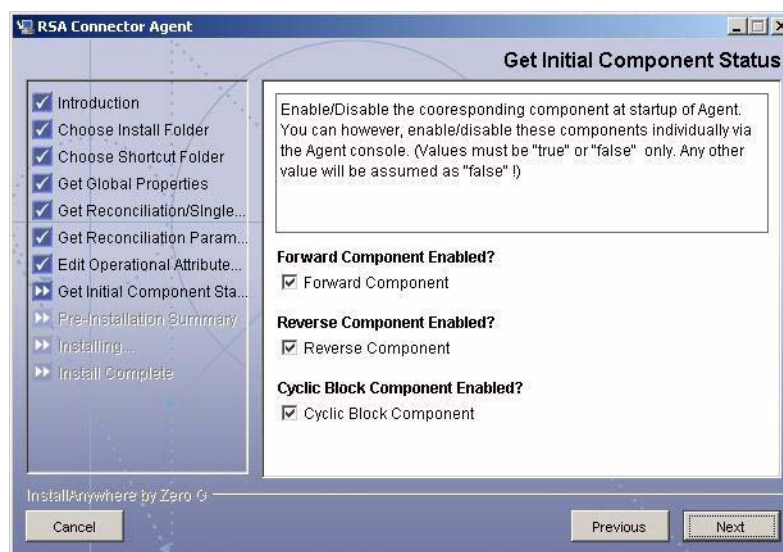
After typing all the parameters, click **Next**. The Edit Operational Attributes (opAttributes) screen appears.



- 10 Refer to the table below to type the parameters.

Serial Number	Text Box Label	Default Value	Description
1	Select Identity Admin Username (sis	Type the Select Identity user name with administrative privilege.
2	Select Identity Admin Userpassword	*****	Type the password for the above mentioned user.
3	Enter the XSL Filename (Without Extension)	RsaConnectorMappingFile	Type the name of the XSL file extracted from the schema file (without the extension .xsl).
4	Enter the Select Identity Resource Name	RSAResource	Type the name of the resource for RSA connector that will be added in Select Identity. (You must provide an identical resource name while creating a resource in Select Identity)

Select the ReverseSync check box to enable reverse synchronization and click **Next**. The Get Initial Component Status screen appears.

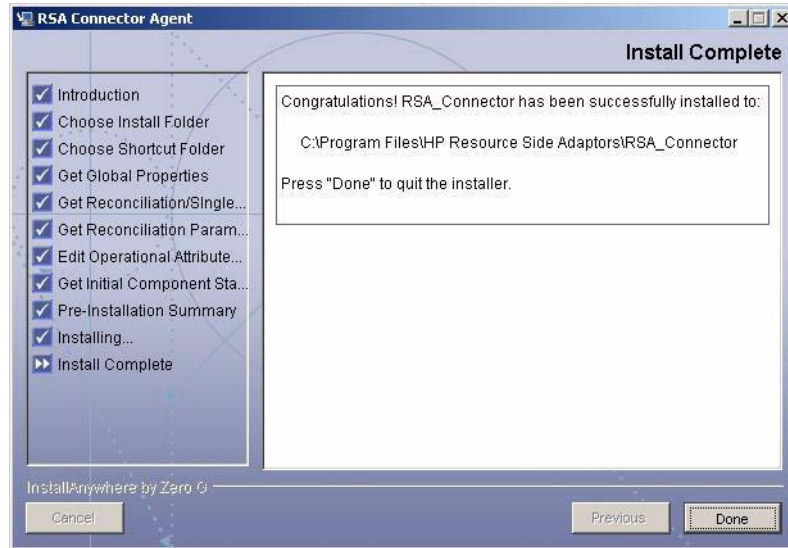


- 11 Enable an agent component by selecting the respective check box.
 - Select the Forward Component check box to enable forward connector operations.
 - Select the Reverse Component check box to enable reverse connector operations.
 - Select the Cyclic Block component to enable cyclic block.

After setting the component status, click **Next**. The Pre-Installation Summary screen appears.



12 Click **Install** to begin installation. After installation is complete, the Install Complete screen appears.



13 Click **Done**.

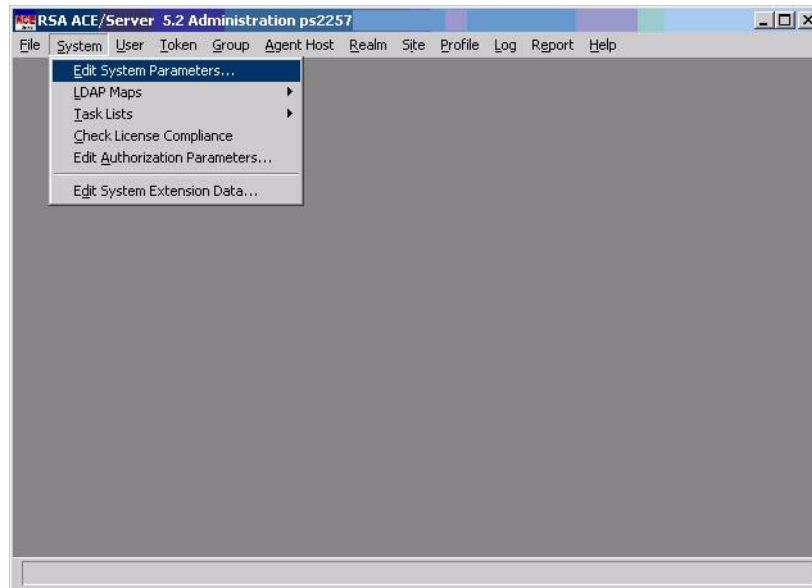
Starting the Agent

The RSA connector agent runs as a console application on the RSA ACE/Server machine. You must perform some additional steps on RSA while starting the agent for the first time.

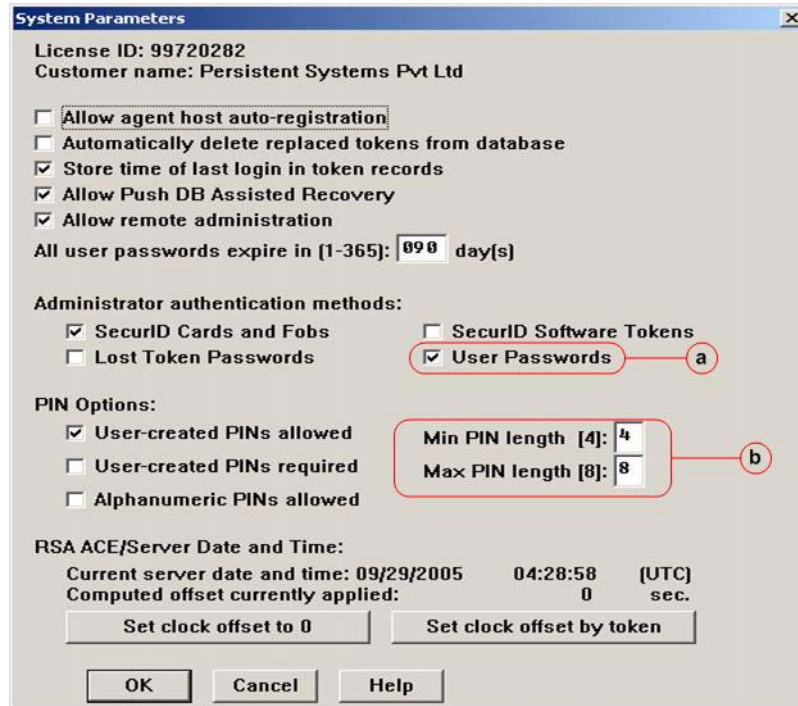
Configure RSA ACE/Server to Start the Agent for the First Time

Perform the following steps to configure RSA ACE/Server to run the agent for the first time:

- 1 Open RSA Database Administration - Host Mode.



- 2 On the menu bar, click **System** → **Edit System Parameters**. The System Parameters dialog box appears.



Perform the following in this dialog box:

- a Select the User Passwords check box.
- b Set the values for Min PIN Length and Max PIN Length according to your requirement. By default, Min PIN Length is set to 4 and Max PIN Length is set to 8.

Start the Agent

To run the agent as a console application, perform the following:

- 1 Go to the installation directory of the agent.
- 2 Double-click the `runAgent.cmd` file.

Modifying Configuration Settings

Most of the configuration properties of the agent are set at the time of agent installation. After installing the agent, you can change these configuration settings by editing the following files:

- `properties.ini`
- `opAttributes.properties`
- `developer_configurations.properties`
- `runAgent.cmd`

properties.ini

The `properties.ini` file is available in the `<Install_Dir>/conf/` folder where `<Install_Dir>` is the agent installation location mentioned in [step 5](#) on page 15. All the configurable properties of this file are listed in the table below.

Serial Number	Configuration Property	Description	Sample Value
1	<code>spml_manager_interval</code>	The time interval (in milliseconds) after which the SPML manager must try to send the accumulated requests.	5000
2	<code>spml_delay</code>	The time interval (in milliseconds) for which the SPML manager must wait before sending an SPML request.	5000
3	<code>session_timeout</code>	Number of logons after which logoff will not be ignored.	100
4	<code>recon_user</code>	The user name in RSA that is to be used while connecting to RSA. The user must be an administrator.	user1
5	<code>recon_user_password</code>	The PIN to be used with <code>recon_user</code> by reconciliation.	1000
6	<code>history_limit</code>	The maximum number of requests that can be accumulated in the SPML manager.	100
7	<code>spml_retries</code>	The number of times the SPML manager must retry to send an SPML.	3
8	<code>resend_delay</code>	The time interval (in milliseconds) for which the agent waits while re-sending a failed SPML.	3000
9	<code>initially_reconciliation_running</code>	Whether to start reconciliation module at start up	True
10	<code>initially_forward_running</code>	Whether to start forward module at start up.	True
11	<code>initially_cyclic_block_running</code>	Whether to start cyclic blocking at start up.	True
12	<code>temporary_folder</code>	The location where the agent places the temporary files created during the operation.	C:/temp/

Serial Number	Configuration Property	Description	Sample Value
13	concero_server_url	The URL where the reconciliation SPMLs are sent.	http://SIServer:7001/lmz/webservice
14	poll_interval	The time interval (in milliseconds) between successive polling operations on RSA server by agent.	10000
15	AGENT_PORT	The port on which the agent listens for the incoming requests.	5000

opAttribute.properties

The `opAttribute.properties` file is available under `<Install_Dir>/conf/`. This file contains the attributes that are included in the reconciliation SPML requests. The following table lists all the operational attributes:

Serial Number	Configuration Property	Description	Sample Value
1	urn:trulogica:concero:2.0#reverseSync	This property determines whether reconciliation is enabled or not. It is set to <code>true</code> if reconciliation is enabled.	true
2	urn:trulogica:concero:2.0#resourceId	Name of the resource on Select Identity.	RSAResource
3	urn:oasis:names:tc:SPML:1:0#UserIDAndOrDomainName	Select Identity user name with administrative privilege.	sis
4	urn:trulogica:concero:2.0#resourceType	Reverse mapping file (XSL transformation file) name without any extension.	RsaConnectorMappingFile
5	urn:trulogica:concero:2.0#password	Select Identity password for the user with administrative privilege.	abc123

developer_configurations.properties

The `developer_configurations.properties` file is available under `<Install_Dir>/conf/`. This file contains advanced configuration properties. The following table lists all the properties:

Serial Number	Configuration Property	Description	Sample Value
1	<code>last_log_entry_num</code>	Number of the last log entry in RSA logs. Agent starts reading logs from this position	300000
2	<code>SUPPORTED_ENTITIES_STRING</code>	Comma separated list of entities that are to be monitored by the reconciliation module. If an entity is removed from the list (for example, group), its add, modify, and delete requests will not be sent. However link of that entity with other enabled entities (for example, User) are still monitored.	User,group,site,agent_host. Entities from the following set are supported and the values are case sensitive: {User,group,site,agent_host}

runAgent.cmd

You can edit this file to modify the connection timeout setting. This setting decides how long the agent must wait after sending an SPML request to Select Identity. Perform the following to edit this setting:

- 1 Open the `runAgent.cmd` file with the help of a text editor.
- 2 Look for the line beginning with `set CONCERO_URL_TIMEOUT=`.
- 3 Set this property (`CONCERO_URL_TIMEOUT`) to desired value (in milliseconds). By default, it is set to -1.

Updating the Agent with Password Changes

While installing the agent, you must provide the following passwords:

- Password of Select Identity user with administrative privilege
- Password (PIN) of RSA user with administrative privilege

If one of these passwords are changed after agent installation, you must update the agent with the change information. The password encrypt utility provided with the agent helps you update the agent with the change information.

Update the Agent with RSA Password Change

Perform the following steps to update the agent with RSA password change:

- 1 Open command prompt.
- 2 Go to the `<agent_install_directory>` (the location where the agent was installed).
- 3 Run the following command:

```
passwordEncrypt.cmd -p <new_password>
```

where `<new_password>` is the new RSA password (PIN).

The password encrypt utility updates the `properties.ini` file with the new RSA password (PIN) in encrypted format.

Update the Agent with Select Identity Password Change

Perform the following steps to update the agent with RSA password change:

- 1 Open command prompt.
- 2 Go to the `<agent_install_directory>` (the location where the agent was installed).
- 3 Run the following command:

```
passwordEncrypt.cmd -s <new_password>
```

where `<new_password>` is the new Select Identity password.

The password encrypt utility updates the `opAttributes.properties` file with the new Select Identity password in encrypted format.

Verifying the Agent Operation

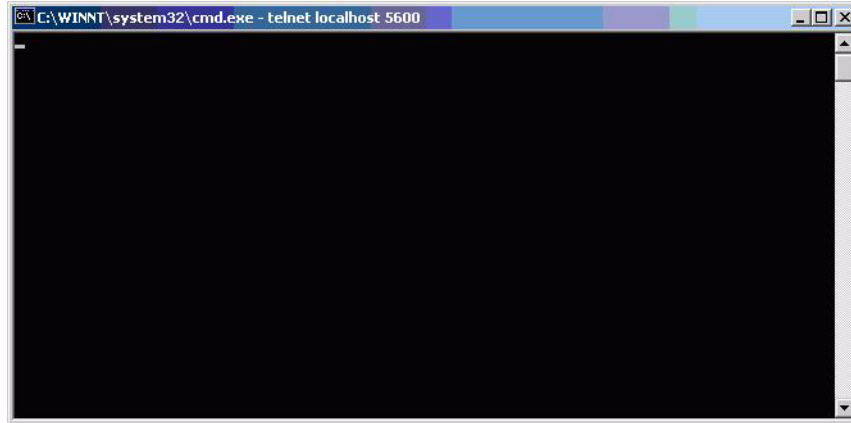
After you start the agent, it listens to the specified port. To verify whether the agent is listening to the specified port or not, perform the following steps:

- 1 Open the command prompt.
- 2 Run the following command:

```
telnet localhost <port_number>
```

where `<port_number>` is the port assigned to the agent.

If the agent is listening to the port, a clear screen appears as shown below.

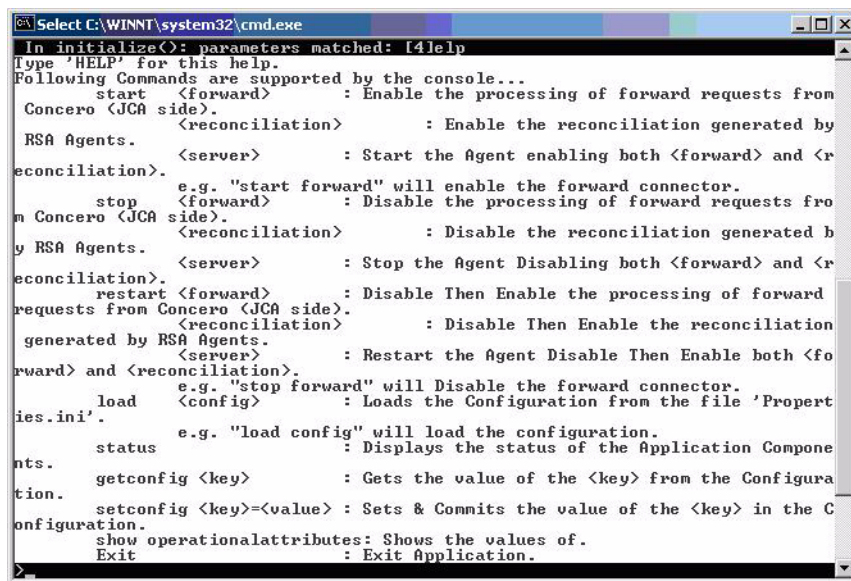


If the agent is not listening to that port, the following error appears:

```
Connecting to localhost...Could not open a connection to host on port
<port_number>: Connect failed
```

Getting Help

The agent runs as a console application on the command prompt. To view the command line help options, type **help** in the agent console. It displays a list of all the commands supported by the agent.



5 Configuring the Connector with Select Identity

This chapter describes the procedure to configure the RSA connector with Select Identity. At the end of this chapter, you will know the procedure to configure the RSA connector with Select Identity.

Configuration Procedure

After you deploy the connector RAR on application server, you must configure the connector with Select Identity. Perform the following steps to configure the RSA connector with Select Identity.

- 1 Add a New Connector
- 2 Add a New Resource
- 3 Map Attributes

Add a New Connector

Add a new connector in Select Identity by using the user interface. While adding the connector, do the following:

- In the Connector Name text box, specify a name for the connector.
- In the Pool Name text box, enter `eis/RSAConnector`.
- Select No for the Mapper Available section.

Figure 2 Manage Connectors Page

Current Resource Connectors		
Connector Name:	Pool Name:	Mapper Available:
<input type="text" value="RSAConnector"/>	<input type="text" value="eis/RSAConnector"/>	<input type="radio"/> Yes <input checked="" type="radio"/> No
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Refer to the *HP Select Identity Connector Deployment Guide* for detailed information on adding a new connector in Select Identity.

Add a New Resource

Add a new resource in Select Identity that uses the newly added connector. Refer to the *HP Select Identity Connector Deployment Guide* for detailed instructions on adding a resource in Select Identity.

Refer to the following table while entering the parameters in the Basic Information and the Access Information pages:

Table 5 Resource Configuration Parameters

Field Name	Sample Values	Description	Comment
Resource Name	RSAResource	Name given to the resource.	The resource name must be same as the resource name mentioned in step 10 on page 18.
Connector Name	RSA	The newly deployed connector.	
Authoritative Source	Yes	Whether this resource is a system that is considered to be the authoritative source for user data in your environment. You must specify Yes because the connector can synchronize account data with the Select Identity server.	
Mapping File	RsaConnectorMappingFile.xml	The attribute mapping XML file.	
Username	Administrator	The administrative user name of RSA ACE/Server.	
Machine name of agent	sint4	The hostname of the machine where the agent is installed (resource machine).	
Password	P4SSW0rd	The administrative password of RSA ACE/Server.	
Database file of RSA log	C:/RSA_Setup/ace/data/sdlog.db	The location on resource system where the log of RSA Server is located.	
Agent port	5000	The port on the resource machine allocated for the agent. The agent listens to this port.	The port number must be same as the port number mentioned in step 7 on page 16.
Database file of RSA server	C:/RSA_Setup/ace/data/sdserv.db	The location on resource system where the database files of RSA Server is located.	

Figure 3 Resource Basic Information Page

Add New Resource : Basic Information

Step 1 of 2: Set up basic information.

Use the page to create a resource profile.

*Required Field **

Resource Name:*

Resource Description:

Connector Name:*

Authoritative: Yes No

OVS! Password Authority: Yes No
Select a single Resource for OVS! password verification.

Delete User: Yes No

Resource Owner:

A Resource Owner is required when User Reconciliation polling is enabled.

Next **Cancel**

Figure 4 Resource Access Information Page

RSAResource: Resource Access Information

Step 2 of 2: Set up access information.

Define Resource parameters using the fields listed below.

*Required Field **

Mapping file: * [View](#)

User Name: *

Machine name of agent: *

password: *

Database file of RSA log: *

Agent port: *

Database file of RSA server: *

Previous **Finish** **Cancel**

After typing in the resource access information, perform the following:

- 1 Click **Finish**.

- 2 Click The **User Reconciliation Policy** link in the left pane. The User Reconciliation Policy page appears..

Basic Information
Resource Access Information
User Reconciliation Policy
Resource Attribute Mapping
Caching Policy

RSAResource: User Reconciliation Policy

Review and edit the reconciliation policy set for the selected resource.

Resource named RSAResource1 successfully saved.

Recon Filter

Recon Filter:

User Polling

Polling Enabled:

Add

Report Policy: Audit Enabled: Yes No

Resource Action: User Action:

Reconciliation Workflow: Rule Name:

Serial Process: Yes No

Modify

Report Policy: Audit Enabled: Yes No

Resource Action: User Action:

- 3 Set Recon Filter to **ExtendedSpmlRequestFilter**, keep all other default settings, and then click **OK**.

Map Attributes

After successfully adding a resource for the RSA connector, you must map the resource attributes to Select Identity attributes. You can create appropriate attributes in Select Identity to be mapped with RSA ACE/Server user attributes. Refer to the *HP Select Identity Connector Deployment Guide* for information on mapping and the *HP Select Identity Administration Online Help* for information on creating attributes. While mapping attributes, refer to the following table for resource specific mapping information. [Table 6](#) lists all the RSA

connector attributes and the corresponding Select Identity attributes to which the attributes must be mapped. The table also describes the possible values of each attribute that can be set while creating a new user by using this connector.

Table 6 RSA Mapping Information

RSA ACE/Server Attribute	Select Identity Attribute	Description	Sample Value
bCreatePin	bCreatePin	This attribute indicates whether the user is allowed to create pin or not. Possible values are Yes/No (case insensitive). All values other than Yes are treated as No. <i>This is an optional attribute.</i>	Yes
bMustCreatePIN	bMustCreatePin	This attribute indicates whether the user is required to create a PIN or not. Possible values are Yes/No (case insensitive). All values other than Yes are treated as No. <i>This is an optional attribute.</i>	Yes
bTempUser	bTempUser	This attribute indicates whether the user is a temporary user or not. Possible values are Yes/No (case insensitive). All values other than Yes are treated as No. <i>This is an optional attribute.</i>	No
EndDate	EndDate	Specifies the date when a temporary user expires. Valid only if bTempUser is Yes. [Format — mm/dd/yyyy]. <i>This is an optional attribute.</i>	08/23/2006
EndTime	EndTime	Specifies the time of day (in number of hours from mid night) when a temporary user expires. Valid only if bTempUser is set to Yes. Only integer values are allowed (0-23). [Format — hh:mm]. Minutes are rounded off to the nearest hour. For example, 10:13 is rounded off to 10:00 and 02:45 is rounded off to 03:00. <i>This is an optional attribute.</i>	04:00

Table 6 RSA Mapping Information (cont'd)

RSA ACE/Server Attribute	Select Identity Attribute	Description	Sample Value
StartDate	StartDate	Specifies the date when a temporary user becomes enabled to authenticate. Valid only if bTempUser is Yes. [Format — mm/dd/yyyy]. <i>This is an optional attribute.</i>	06/21/2006
StartTime	StartTime	Specifies the time of day (in number of hours from mid night) when a temporary user becomes enabled to authenticate. Valid only if bTempUser is Yes. Only integer values are allowed (0-23). [Format — hh:mm]. Minutes are rounded off to the nearest hour. For example, 10:13 is rounded off to 10:00 and 02:45 is rounded off to 03:00. <i>This is an optional attribute.</i>	21:00
FirstName	FirstName	String of user's first name, must be limited to 24 characters. <i>This is an optional attribute.</i>	John
LastName	LastName	String of user's Last name, must be limited to 24 characters. <i>This is a mandatory attribute.</i>	Smith
password	Password	PIN associated with password token of the user (must be a numeric value). <i>This is an optional attribute.</i>	1111
rsa_password	rsa_password	Password token of the user (must be a numeric value). <i>This is an optional attribute.</i>	4444
RSAResource_ENTITLEMENTS	RSAResource_ENTITLEMENTS	RSA groups are treated as entitlements. <i>This is an optional attribute.</i>	Employee

Table 6 RSA Mapping Information (cont'd)

RSA ACE/Server Attribute	Select Identity Attribute	Description	Sample Value
RSAResource_KEY	RSAResource_KEY	<i>This is an optional attribute.</i>	
Shell	Shell	Default shell of the user, relevant for RSA installed on UNIX based platforms. It must be limited to 256 character long string. <i>This is an optional attribute.</i>	ksh
UserName	UserName	String of user's default login in RSA, must be limited to 48 characters. <i>This is a mandatory attribute.</i>	username

You can create new attributes in Select Identity to map the connector attributes.

Figure 5 Resource Attribute Mapping

RSAResource: Resource Attribute Mapping				
Modify the mapping the applicable resource attributes to the associated HP OpenView Select Identity attributes and determine how each will be updated.				
Resource Attribute	Attribute	Sync In	Sync Out	
bCreatePin	bCreatePin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
bMustCreatePIN	bMustCreatePIN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
bTempUser	bTempUser	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
EndDate	EndDate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
EndTime	EndTime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
FirstName	FirstName	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
LastName	LastName	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
password	Password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
rsa_password	rsa_password	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Shell	Shell	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
StartDate	StartDate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
StartTime	StartTime	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
UserName	UserName	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RSAResource_ENTITLEMENTS	RSAResource_ENTITLEMENTS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RSAResource_KEY	RSAResource_KEY	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Refer to *Service Studio* chapter of *HP Select Identity Administration Online Help* for information adding a new attribute to Select Identity.

Attribute Behavior

The set of RSA attributes can be broadly classified into three categories:

Class 1: password and rsa_password

The `password` attribute represents the PIN on RSA resource and the `rsa_password` represents the Password Token on RSA resource. When you mention the `password` attribute during user creation, you must also provide the `rsa_password` attribute. These two attributes cannot be modified from Select Identity during modify user operation. Do not include these attributes in Modify View form. use reset password for changing the password.

Class 2: Temporary User Attributes

This category consists of the following attributes:

- `bTempUser`
- `StartDate`
- `StartTime`
- `EndDate`
- `EndTime`

These attributes control the status of a temporary user. If `bTempUser` is set to Yes, other four attributes must be mentioned while creating a user. If `bTempUser` is set to No, other four attributes are ignored.



`StartTime` and `EndTime` attributes are specified as per local time while creating the user from Select Identity, but stored in RSA database as per GMT.

Class 3: `bCreatePin` and `bMustCreatePIN`

These attributes decide whether the user is allowed to and required to create a PIN. These can be set to Yes or No. However, if you set `bCreatePin` to No and `bMustCreatePIN` to Yes, Select Identity throws an error as this is an invalid input.

Add Service

After mapping the attributes, you must add a service to which you can associate the newly created resource. Perform the following steps to add a service:

- 1 Click **Service Studio** → **Services**. The Service List page appears.
- 2 Click **Add Service**. The Add New Service: Basic Information page appears.

- 3 Select the settings as shown in the image below.

Add New Service : Basic Information

Use this page to define the new service.

Service Information

*Required Field **

Service Name:*

Service Type:*

Service Description:

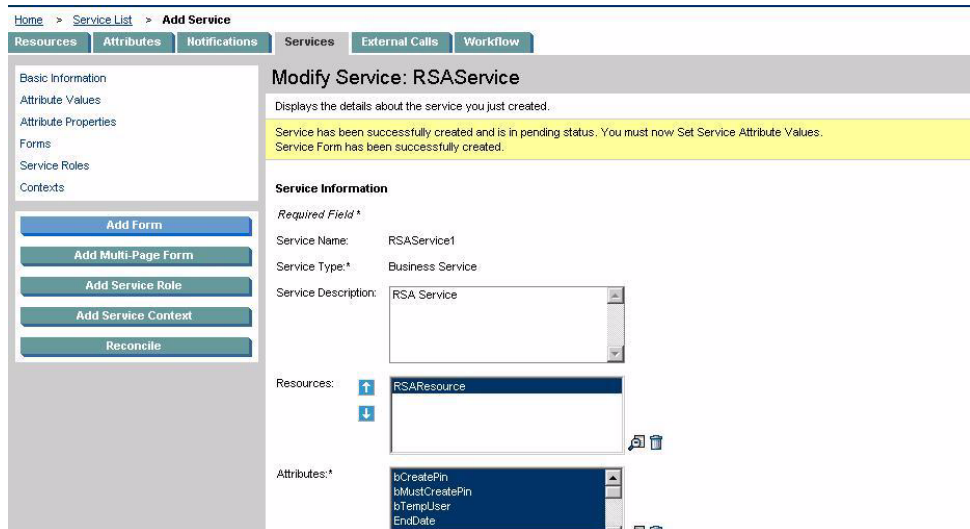
Resources:

Attributes:*

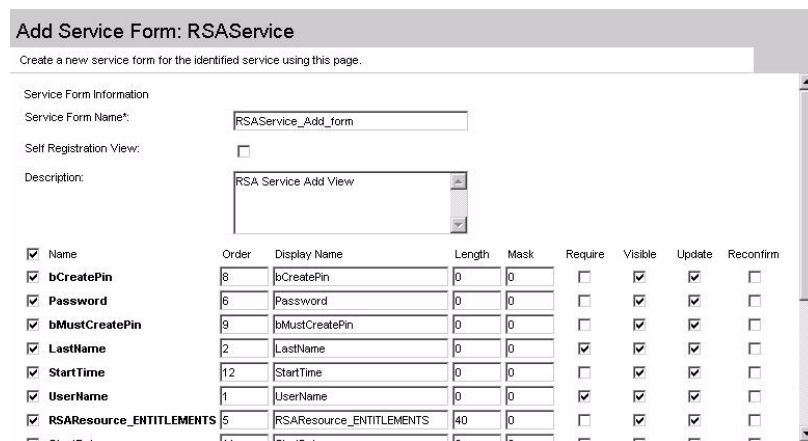
Context Attribute:*

Primary User Key:*

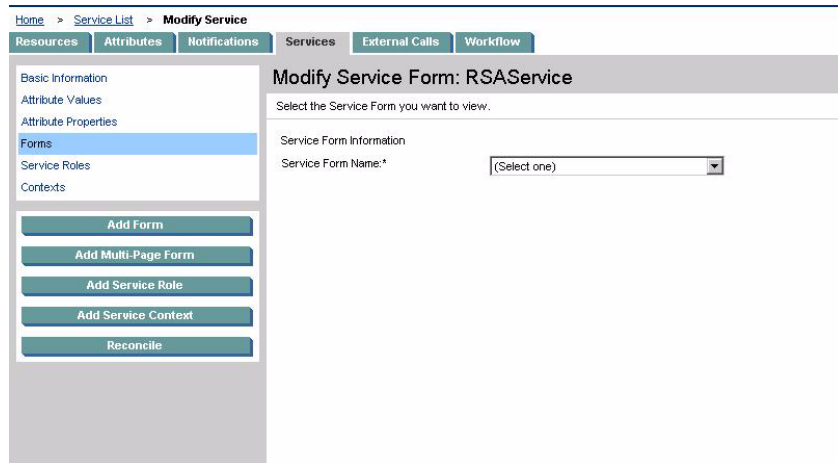
- 4 In this page, perform the following:
 - a Type a name in the Service Name text box.
 - b Select Business Service from the Service Type drop down list.
 - c Select the newly crated RSA resource in the Resources list.
 - d In the Attribute list, select all the Select Identity user attributes that have been mapped to RSA user attributes.
 - e In the Context Attribute drop down list, select LastName.
 - f In the Primary User Key drop down list, select UserName.
- 5 Click **Create**. A new service is created.



- 6 Click **Add Form**. The Add Service Form page appears.



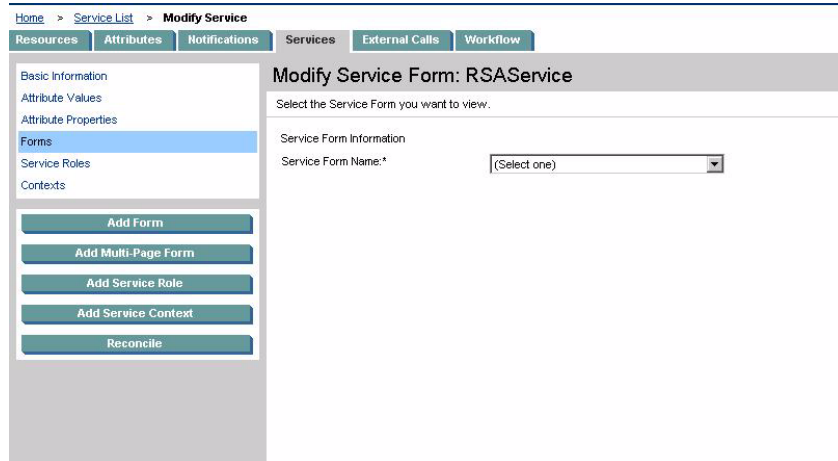
- 7 Perform the following steps in this page to create an Add form:
 - a Type a name in the Service Form Name text box.
 - b Select all the listed attributes other than the following attributes:
 - GUID
 - RSAResource_KEY
 - c Clear the Require check boxes for all the listed attributes other than the following attributes:
 - UserName
 - LastName
- 8 Click **Create**. The Modify Service Form page appears.



- 9 Click **Add Form**. The Add Service Form page appears.

<input checked="" type="checkbox"/> Name	Order	Display Name	Length	Mask	Require	Visible	Update	Reconfirm
<input checked="" type="checkbox"/> bCreatePin	4	bCreatePin	0	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Password		Password	0	0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> bMustCreatePin	5	bMustCreatePin	0	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> LastName	2	LastName	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> StartTime	10	StartTime	0	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> UserName	1	UserName	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> RSAResource_ENTITLEMENTS	7	RSAResource_ENTITLEMENTS	40	0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- 10 Perform the following steps in this page to create a Modify form:
 - a Type the form name in the Service Form Name text box.
 - b Select all the listed attributes other than the following attributes:
 - Password
 - RSA_Password
 - GUID
 - RSAResource_KEY
 - c Clear all the Require check boxes other than the following attributes:
 - UserName
 - LastName
 - d Clear the Update check boxes only for the following attributes:
 - UserName
 - LastName
- 11 Click **Create**. The Modify Service Form page appears.



- 12 Select Default View from the Service Form Name drop down box. The Modify Service Page for the Default View appears.

Modify Service Form: RSAService

Use this page to modify the selected form.

Service Form Information

Service Form Name:*

Self Registration View:

Description:

<input type="checkbox"/> Name	Order	Display Name	Length	Mask	Require	Visible	Update	Reconfirm
<input checked="" type="checkbox"/> bCreatePin	1	bCreatePin	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> bMustCreatePin	2	bMustCreatePin	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> bTempUser	3	bTempUser	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> EndDate	4	EndDate	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> EndTime	5	EndTime	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> FirstName	6	FirstName	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> LastName	7	LastName	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Password	8	Password	0	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- 13 Clear all the Require check boxes other than the following attributes:

- UserName
- LastName

- 14 Click **Apply**. The Modify Service Form page appears.
- 15 Click **Add Service Role**. The Add Service Role screen appears.

- 16 Perform the following steps in this page:
 - a Type a name in the Service Role Name text box.
 - b For forward add operation (Add event), set Workflow template as Select Identity Provisioning only and Default Form to the newly created Add form (step 7 on page 38).
 - c For Reconciliation event, keep the default setting.
 - d For any other operation set workflow template as Select Identity Provisioning only and Default Form to the newly created Modify form (step 10 on page 39).
 - e Click **Create**. The Modify Service Form page appears.


- 17 Click **Add Service Context**. The Add Service Context page appears.


Add Service Context: RSAService

Use this page to create a new Context user group for the identified service.



Service Context Information

Service Context Name:*

Service Role:* 



LastName:* 

Notification Event Handlers

Notification Events  

Notifications

Event Handlers

Request Events  

Workflow Template

- 18 Perform the following in this page:
 - a Type the Service Context name.
 - b Select the newly created Service Role ([step 15](#) on page 40).
 - c Type * in LastName text box.
- 19 Click **Create**.

6 Uninstalling the Connector

If you want to uninstall a connector from Select Identity, perform the following steps:

- Remove all resource dependencies.
- Delete the connector from Select Identity.
- Delete the connector from application server.

See *HP Select Identity Connector Deployment Guide* for more information on deleting the connector from application server and Select Identity.

Uninstalling the Agent

Perform the following steps to uninstall the agent from the RSA ACE/Server machine:

- 1 Invoke the uninstallation wizard from the shortcut. For example, if you chose shortcut location as
C:\Program Files\HP Resource Side Adaptors during installation, click **Start** → **Programs** → **HP Resource Side Adaptors** → **RSA_Connector** → **Uninstall RSA_Connector**. The uninstallation wizard appears.
- 2 Follow the instruction on the wizard. In the Uninstall Option screen, select Complete Uninstall.

Alternatively, if you have not selected any shortcut location for the agent, perform the following steps to uninstall:

- 1 From Start menu, click **Settings** → **Control Panel**. The Control Panel window appears.
- 2 In the Control Panel, double-click **Add or Remove Programs**. The Add or Remove Programs window appears.
- 3 In the Add or Remove Programs window, double-click on **RSA_Connector**. The uninstallation wizard appears.
- 4 Follow the instruction on the wizard. In the Uninstall Option screen, select Complete Uninstall.

A Troubleshooting

- **Problem:** While creating the RSA resource on Select Identity, an error message appears displaying `Test Failed! Unable to connect to the resource: ConnectorTestFailedException, [Managed Connection reference is null. Unable to connect to the underlying EIS resource.]`:

Possible Causes:

- a RSA services are not running.
- b The value of agent port entered in Select Identity while creating the resource does not match with `AGENT_PORT` value in `properties.ini` file.
- c The username entered in Select Identity during resource creation does not exist in RSA or does not have administrative privilege.

Solutions:

- a On the resource machine, open RSA's Database Administration — Host Mode. This starts all the necessary RSA services.
 - b Provide the correct agent port information in Select Identity.
 - c Enter an existing RSA username with administrative privilege while creating the resource on Select Identity.
- **Problem:** While associating a user to a group or groups, the `get` operation fails.

Possible Cause: The Temporary Folder mentioned during agent installation ([step 6](#) on page 16) is not a valid location, or you do not have write access to this folder.

Solution: Make sure you mention a valid location with appropriate privilege at the time of typing the Temporary Folder during agent installation. Otherwise, you can edit this location information from `properties.ini` file. Refer to [Modifying Configuration Settings](#) on page 22 for more information on modifying agent configuration parameters and settings.

- **Problem:** Reset Password or Add User operations fail with one of the following error messages:

- `Sd_AssignPassword Error Alpha characters not allowed: TACConnectorException, [Sd_AssignPassword Error Alpha characters not allowed`
- `Sd_AssignPassword Error Invalid Password: TACConnectorException, [Sd_AssignPassword Error Invalid Password]`:

Possible Cause: The password entered does not match with the constraints imposed by RSA settings.

Solution: Enter a password that matches with RSA settings. Otherwise, you must change the settings in RSA.

- **Problem:** During user creation, an error message appears displaying `Function disabled due to license violation.: TACConnectorException, [Function is disabled due to license violation.]`:

Possible Cause: This error appears when the number of users exceed the number of active users in RSA database allowed by your RSA license.

Solution: The number of active users in RSA can be reduced by removing all tokens from users.

- *Problem:* An error message appears displaying `Sd_AdmLogin Error User not found.:TAConnectorException, [Sd_AdmLogin Error User not found.]`:

Possible Cause: The RSA administrative user you used to connect to RSA does not exist on RSA anymore.

Solution: Make sure to provide a valid username with administrative privilege while creating the resource on Select Identity.

- *Problem:* While linking a token to a user from Select Identity, an error message appears displaying `Sd_AssignAnotherToken Error Token is already assigned:TAConnectorException, [Sd_AssignAnotherToken Error Token is already assigned]`:

Possible Cause: The token you are trying to link is already linked to some other user. RSA does not allow you to link one token to more than one user.

Solution: Unlink the token or use another token that has not been linked to any user.

- *Problem:* An error message appears displaying `com.trulogica.truaccess.connector.exceptions.ConnectorSysException:Unable to get Connector from pool:eis/RSACConnector:Failed in getConnection (TAConnectorParamValueBean) of com.trulogica.truaccess.connector.rsa.impl.cci.EISConnectionFactory`

Possible Cause: Agent may not be running or there is a problem with the port.

Solution: Verify and make sure the agent is running. Refer to [Verifying the Agent Operation](#) on page 26 for more information to check if the agent is running.

- *Problem:* Suddenly the agent stops working.

Possible Cause: This happens if the agent is stopped accidentally (by pressing **Ctrl +C** in the agent console).

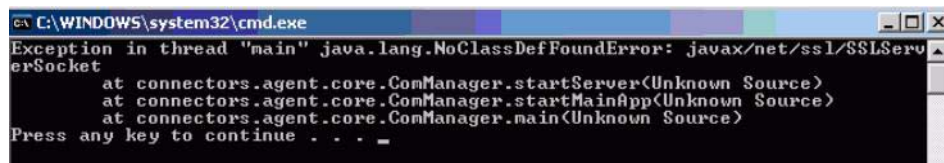
Solution: Type **Exit** in the agent console to exit the console and restart the agent.

- *Problem:* Reconciliation stops working.

Possible Cause: At least one group in the RSA system has @ as part of its name. RSA uses @ character to separate group name from the name of a site that the group is linked with. For example, if group g1 is linked with site s1, RSA identifies it as g1@s1.

Solution: Do not include @ character in group name.

- *Problem:* An error occurs similar to one of the following:



```
C:\WINDOWS\system32\cmd.exe
Exception in thread "main" java.lang.NoClassDefFoundError: javax/net/ssl/SSLServerSocket
    at connectors.agent.core.ConManager.startServer(Unknown Source)
    at connectors.agent.core.ConManager.startMainApp(Unknown Source)
    at connectors.agent.core.ConManager.main(Unknown Source)
Press any key to continue . . .
```

or

```
ex C:\WINDOWS\system32\cmd.exe
> java.lang.UnsupportedClassVersionError: in/co/persistent/enconnect/ucf/mware/ex
ceptions/HostNotRespondingException (Unsupported major.minor version 48.0)
  at java.lang.ClassLoader.defineClass0(Native Method)
  at java.lang.ClassLoader.defineClass(ClassLoader.java:488)
  at java.security.SecureClassLoader.defineClass(SecureClassLoader.java:10
6)
  at java.net.URLClassLoader.defineClass(URLClassLoader.java:243)
  at java.net.URLClassLoader.access$100(URLClassLoader.java:51)
  at java.net.URLClassLoader$1.run(URLClassLoader.java:190)
  at java.security.AccessController.doPrivileged(Native Method)
  at java.net.URLClassLoader.findClass(URLClassLoader.java:183)
  at java.lang.ClassLoader.loadClass(ClassLoader.java:294)
  at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:281)
  at java.lang.ClassLoader.loadClass(ClassLoader.java:250)
  at java.lang.ClassLoader.loadClassInternal(ClassLoader.java:310)
  at connectors.agent.core.ComServer.startReconciliation(Unknown Source)
  at connectors.agent.core.ComServer.run(Unknown Source)
```

Possible Cause: The Java version is 1.3.

Solution: You must use Java 1.4.2 or above.

