Oracle® COREid Federation

COREid Federation V1.0 to V2.0 Upgrade Guide

10*g* Release 2 (10.1.2)
Part No. B19019-01

May 2005

ORACLE

Copyright © 1996-2005 by Oracle. All rights reserved. US Patent Numbers 6,539,379; 6,675,261; 6,782,379; 6,816,871.

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

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle COREid Access and Identity products includes RSA BSAFE™ cryptographic or security protocol software from RSA Security. Copyright © 2003 RSA Security Inc. All rights reserved.

This program contains third-party code from Apache. Under the terms of the Apache Software License, Oracle is required to provide the following notices. Note, however, that the Oracle program license that accompanied this product determines your right to use the Oracle program, including the Apache software, and the terms contained in the following notices do not change those rights. Notwithstanding anything to the contrary in the Oracle program license, the Apache software is provided by Oracle "AS IS" and without warranty or support of any kind from Oracle or Apache.

```
* The Apache Software License, Version 1.1
 *
 * Copyright (c) 2000 The Apache Software Foundation.  All rights
 * reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. The end-user documentation included with the redistribution,
 *    if any, must include the following acknowledgment:
 *       "This product includes software developed by the
 *        Apache Software Foundation (http://www.apache.org/)."
 *    Alternately, this acknowledgment may appear in the software itself,
 *    if and wherever such third-party acknowledgments normally appear.
 *
```

* 4. The names "Apache" and "Apache Software Foundation" must
*   not be used to endorse or promote products derived from this
*   software without prior written permission. For written
*   permission, please contact apache@apache.org.
*
* 5. Products derived from this software may not be called "Apache",
*   nor may "Apache" appear in their name, without prior written
*   permission of the Apache Software Foundation.
*
* THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED
* WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES
* OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
* DISCLAIMED. IN NO EVENT SHALL THE APACHE SOFTWARE FOUNDATION OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
* LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND
* ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY,
* OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT
* OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
* ==
*
* This software consists of voluntary contributions made by many
* individuals on behalf of the Apache Software Foundation. For more
* information on the Apache Software Foundation, please see
* <http://www.apache.org/>.
*
* Portions of this software are based upon public domain software
* originally written at the National Center for Supercomputing Applications,
* University of Illinois, Urbana-Champaign.
*/

Bouncy Castle License
Copyright (c) 2000 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This program contains third-party code from Jason Hunter & Brett McLaughlin for JDOM. Under the terms of the JDOM license, Oracle is required to provide the following notices. Note, however, that the Oracle program license that accompanied this product determines your right to use the Oracle program, including the JDOM software, and the terms contained in the following notices do not change those rights. Notwithstanding anything to the contrary in the Oracle program license, the JDOM software is provided by Oracle "AS IS" and without warranty or support of any kind from Oracle, Jason Hunter, or Brett McLaughlin."

JDOM License
Copyright (C) 2000-2003 Jason Hunter & Brett McLaughlin.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact <license AT jdom DOT org>.

4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management <pm AT jdom DOT org>.

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following:
"This product includes software developed by the JDOM Project (http://www.jdom.org/)."
Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Jason Hunter <jhunter AT jdom DOT org> and Brett McLaughlin <brett AT jdom DOT org>. For more information on the JDOM Project, please see <http://www.jdom.org/>.

This program contains third-party code from the OpenSSL Project. Under the terms of the OpenSSL Project license, Oracle is required to provide the following notices. Note, however, that the Oracle program license that accompanied this product determines your right to use the Oracle program, including the OpenSSL software, and the terms contained in the following notices do not change those rights. Notwithstanding anything to the contrary in the Oracle program license, the OpenSSL software is provided by Oracle "AS IS" and without warranty or support of any kind from Oracle or the OpenSSL Project"

OpenSSL License

```
/* ====================================================================
 * Copyright (c) 1998-2003 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
```

* 5. Products derived from this software may not be called "OpenSSL"
*   nor may "OpenSSL" appear in their names without prior written
*   permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
*   acknowledgment:
*   "This product includes software developed by the OpenSSL Project
*   for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ==
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Contents

Preface

The *COREid Federation 1.0 to COREid Federation 2.0 Upgrade Guide* provides information about migrating COREid Federation 1.0 to COREid Federation 2.0.

Note: Oracle *COREid Federation* was previously known as Oblix *SHAREid* and Oracle *COREid Federation* V1.0 was also previously referred to as NetPoint (COREid) SAML Services. All legacy references to Oblix and SHAREid should be understood to refer to Oracle and COREid Federation, respectively. All legacy reference to NetPoint (COREid) SAML should be understood to refer to COREid Federation 1.0 specifically.

This Preface covers the following topics:

Intended Audience

This guide is intended for administrators who are responsible for migrating COREid Federation 1.0 (NetPoint SAML Services) to COREid Federation 2.0.

This document assumes that you are familiar with your LDAP directory and Web servers, COREid (NetPoint) and COREid Federation products.

Documentation

The manuals that are available for this release include:

COREid Federation Guide—Provides COREid Federation concepts and considerations, product installation and configuration, to help you create a Federated identity management system that provides cross-domain SSO to connect your partners and customers to your systems while reducing compliance risks.

COREid Release Notes—Provides up-to-the minute details about the latest COREid release.

COREid Installation Guide—Explains how to install and configure the COREid components.

COREid Upgrade Guide—Explains how to upgrade earlier versions of COREid to the latest release.

COREid Administration Guide—Explains how to configure COREid applications to display information stored in the directory, how to assign view and modify permissions for data displayed on the COREid applications, and how to assign access controls to users.

COREid Deployment Guide—Provides information for people who plan and manage the environment in which COREid will run. This guide covers capacity planning, system tuning, failover, load balancing, caching, and migration planning.

COREid Customization Guide—Explains how to change the appearance of COREid applications and how to control COREid by making changes to operating systems, Web servers, directory servers, directory content, or by connecting CGI files or JavaScripts to COREid screens.This guide also describes the Access Server API and the Authorization and Authentication Plug-in APIs.

COREidDeveloper Guide—Explains how to create AccessGates and how to develop plug-ins. This guide also provides information to be aware of when creating CGI files or JavaScripts for COREid.

COREid ntegration Guide—Explains how to set up COREid to run with third-party products such as BEA WebLogic, the Plumtree portal, and IBM Websphere.

COREid Schema Description—Provides details about the COREid schema.

Online Help is available from each screen.

Typographical Conventions

COREid manuals use the following typographical conventions:

- When you are instructed to select elements sequentially, the actions are separated with angle brackets, as shown below:

  Click System Admin > System Configuration > View Server Settings

- Paths to a file are shown using syntax for either the Unix or Windows platform:

  /COREid_install_dir/identity/oblix/logs/debugfile.lst
  COREid_install_dir\identity\oblix\logs\debugfile.lst

  where *COREid_install_dir* refers to the directory where the component, in this case, the COREid Server, is installed.

Contact Information

For a list of contacts including corporate offices world wide, sales, and other details, visit the Oracle Web site at:

`http://www.oracle.com`

You can contact Oracle with questions or comments as follows:

Customer Care—http://www.oracle.com/support/contact.html

Corporate Headquarters

Oracle maintains offices world wide. Oracle corporate headquarters is located at:

500 Oracle Parkway
Redwood Shores, CA 94065
Phone: (650) 506-7000

Before Contacting Customer Care

Before contacting Customer Care, please have available the following:

- Oracle product name and version number
- Type of computer and operating system you are using

Accessing the Customer Care Knowledge Base

For more information about using COREid Federation, see the Oracle Customer Care Knowledge Base. To access the Knowledge Base, you need a login name and password, which you can obtain from your Oracle sales representative.

To access the Knowledge Base:

1. Enter the following URL in your browser and press Return.

   `http://www.oracle.com/support/contact.html`

2. Click the phrase, Login to the Oracle PremiumCare Online Portal.
3. Enter your user name and password in the box that appears, then click Login.
4. Under Oracle Support Tools, click Case Manager.
5. In the next screen, click Find Answers to gain access to the Knowledge Base.

Migrating NetPoint SAML Services to SHAREid

This chapter describes how to use the NetPoint SAML to SHAREid migration tool to migrate NetPoint SAML Services to Oblix SHAREid. Included are the following topics:

Note: The NetPoint name is changing to COREid. However, you will see NetPoint in the product itself and in some documentation.

About Migrating NetPoint SAML to SHAREid

The NetPoint SAML to SHAREid migration tool imports configuration data for an existing NetPoint SAML (also known as SHAREid 1.0) installation into a new SHAREid 2.0 installation. This includes local (MyDomain) and partner domain URLs, keys, passwords, and certificates.

Note: The migration tool performs only migration for SHAREid servers; it does *not* migrate NetPoint SAML proxy servers to SHAREid proxy servers.

About NetPoint and SAML Services

In NetPoint 6.x, SAML Services configuration data is held in three places:

- NetPoint authorization rule actions in the SAML policy domain, managed by the Access Manager SAML Services function
- Properties in the file below, edited manually:

  NetPointSAML_install_dir/NetPointSAML.properties
- NetPoint authentication schemes for assertion mappings, defined using the Access Manager SAML Services function.

Configuration items in actions and properties can be considered to be in the form below:

[*domain*.]*name*=*value*

where:

- *domain* is MyDomain or the configured partner domain. If omitted, the domain is assumed to be MyDomain. For actions in the SAML policy domain, *domain* is derived from the name of the authorization rule holding the action.
- *name* is the name of the configuration item
- *value* is the value of the configuration item

For example: Partner1. ReceiverURL=https://saml.partner1.com/saml/ObSAMLReceiverURL.

If you choose to migrate keys from NetPoint SAML to SHAREid, the keys are imported. The migration tool changes the password of the imported keystore alias to match the SHAREid keystore password.

Note: SHAREid 2.0 requires NetPoint 6.5.2 or later. NetPoint 6.1.x policy data, including the SAML policy domain and associated authentication schemes, can be upgraded to NetPoint 7.0. After upgrading to NetPoint 7 you can run the NetPoint SAML to SHAREid migration tool using the upgraded policy domain and schemes. For details, see "Upgrading to NetPoint 7.0" on page 15.

About SHAREid Configurations

SHAREid 2.0 configuration data is held in the XML file below:

SHAREid_install_dir/oblix/config/shareid-config.xml

This file has elements for MyDomain and each partner domain, as well as elements for the local login and IdMBridge configurations, signer keystores and keys, artifact store, assertion profiles, and assertion mappings.

Preparing for Migration

If you do not complete the procedures below, the migration may not be successful.

Task overview: Preparing for the migration

1. Ensure that your NetPoint SAML Services are configured and operating properly, as described in the *NetPoint 6.x Administration Guide*.
2. Upgrade NetPoint components, as described in "Upgrading to NetPoint 7.0" on page 15.

3. Ensure that your SHAREid v2 installation is installed and operating properly, as described in the Oblix *SHAREid 2 Administration Guide*.

   Failure to complete step 4 results in an error during the migration indicating that the AccessGate cannot contact any Access Servers.

4. Set up a COREid back end to use the same NetPoint configuration as the NetPoint SAML Services, as described in the *SHAREid 2 Administration Guide.*

   For example:

   Enter the info on the IdMBridge configuration pages (both COREId configuration and Server configuration pages).

5. Proceed with migration, as described in "Migrating SAML Services to SHAREid" on page 16.

Upgrading to NetPoint 7.0

There are two upgrade paths to NetPoint 7.0 when SAML Services are involved:

- "Upgrading from NetPoint 6.1.1" on page 15
- "Upgrading from NetPoint 6.5" on page 15

Upgrading from NetPoint 6.1.1

Upgrading from NetPoint 6.1.1 with SAML Services to NetPoint 7.0 is a two step task.

Task overview: Upgrading NetPoint 6.1 with SAML Services

1. Upgrade NetPoint 6.1.1 components to NetPoint 7.0 using instructions in the *NetPoint 7.0 Upgrade Guide*.
2. Use the instructions in "Migrating SAML Services to SHAREid" on page 16 of this guide to complete the migration from NetPoint SAML to SHAREid.

Upgrading from NetPoint 6.5

Upgrading from NetPoint 6.5 with SAML Services to NetPoint 7.0 is a three step task.

Task overview: Upgrading NetPoint 6.5 with SAML Services

1. Patch your NetPoint 6.5 installation up to 6.5.2, if needed, as described in the *NetPoint 6.5.2 Release Notes*.
2. Use the instructions in "Migrating SAML Services to SHAREid" on page 16 to complete the migration from NetPoint SAML to SHAREid.

3. Upgrade NetPoint 6.5.2 components to NetPoint 7.0 using instructions in the *NetPoint 7.0 Upgrade Guide*.

Migrating SAML Services to SHAREid

Migrating NetPoint SAML Services to SHAREid v2 includes the procedures below:

- "Installing the Migration Tool" on page 16
- "Starting the Migration" on page 16
- "Evaluating Messages" on page 18
- "Completing the Migration" on page 19

Installing the Migration Tool

The migration tool is a Java Server Page file, migrate.jsp, that contains all of the code and the user interface for the migration.

To install the migration tool

1. Locate the migration tool you received from Oblix.
2. On the SHAREid v2 host, copy migrate.jsp to the directory below:

   SHAREid_install_dir/webapps/shareid/admin

   where *SHAREid_install_dir* is the directory where you installed SHAREid v2.

Starting the Migration

When you use migrate.jsp, the SHAREid Server automatically compiles the JSP into a Java source file, then compiles the Java source into a class file. You do not need to restart the SHAREid Server after copying the JSP to the correct location.

You use the migration tool through any browser and are prompted for SHAREid Admin credentials to prevent unauthorized users from running the tool. The tool provides two main options: Migrate and Revert.

The Migrate option instructs the tool to read the SAML configuration from the following locations and import it into SHAREid:

- NetPoint SAML policy domain
- NetPoint SAML properties file in:

  NetPointSAML_install_dir/NetPointSAML.properties
- NetPoint SAML authentication schemes

The imported configuration is immediately available and SHAREid writes an updated shareid-config.xml file.

To start the migration

1. Enter the URL for the tool.

   For example:

   http(s)://*host*:*port*/shareid/admin/migrate.jsp

   where *host* is the SHAREid Server host and port is either the open or the SSL port configured for SHAREid.

   This URL is part of the SHAREid Admin Web application.

2. Enter your SHAREid Admin username and password when asked.

   The migration tool displays a form with two major options: Migrate and Revert.

3. Choose the Migrate option to continue.

   A form appears with fields and checkboxes for migration parameters.

4. Ensure the parameters are accurate for your environment:

   - **Directory holding NetPointSAML.properties**—A text field:
     - If the NetPoint SAML installation is on the same host as the SHAREid Server, this is NetPoint SAML installation directory.
     - If the NetPoint SAML installation is *not* on the same host, the NetPointSAML.properties file must be copied from the NetPoint SAML host to the SHAREid host, and this is the directory to which it is copied.
   - **Directory holding NetPointSAML keystore**—A text field:
     - If the NetPoint SAML installation is on the same host as the SHAREid Server, this can be left blank and the migration tool will determine the location of the NetPoint SAML keystore from Keystore property in the properties file.
     - If the NetPoint SAML installation is not on the same host, the keystore file must be copied from the NetPoint SAML host to the SHAREid host, and this is the directory to which it is copied.
   - **Assertion profile name**—The name of SHAREid assertion profile can be specified here. The default profile name is “Default”.

     The assertion properties configured for NetPoint SAML Services are migrated to a newly created SHAREid assertion profile that is used by each migrated domain.

- **Preserve NetPointSAML URLs?**—A checkbox. This setting effects local (MyDomain) URLs. SHAREid uses fixed local URL paths for these:

  http(s)://*host*:*port*/shareid/saml/ObSAML*name*Service

  where *name* is either Transfer, Receiver, Responder, or Error.

  These will differ from the MyDomain URLs used by your NetPoint SAML installation. As a result, migration to SHAREid requires that your partners change their URLs for your domain.

  Note: If you are using the SHAREid Proxy, you may preserve the NetPoint SAML URLs for MyDomain by checking this box and by modifying the SHAREid Proxy configuration file to map the existing URLs used by your NetPoint SAML installation to the URLs expected by the SHAREid Server. To do this, you edit the ProxyPass and ProxyPassReverse directives in the *SHAREid_Proxy_install_dir*/conf/http.conf and ssl.conf. For example, ProxyPass /saml http://*host*:*port*/shareid/saml.

- **Preserve NetPointSAML key/certificate?**—A checkbox. This setting replaces the SHAREid signing key and its self-signed or CA-issued certificate with the signing key and certificate from the NetPoint SAML keystore.

  Your partner domains can continue to use the existing NetPoint SAML certificate to verify signatures from your SHAREid Server. If you elect to use the new SHAREid signing key, your partner domains must then import the corresponding certificate.

  Note: This migration tool does *not* migrate any keys or certificates from proxy servers you might have used with NetPoint SAML to the SHAREid Proxy Server. You must either migrate these manually or generate new proxy keys and certificates.

Evaluating Messages

It is a good idea to read and evaluate migration tool messages.

The migration tool reports its actions in an HTML response to the form submittal. The report lists each NetPoint SAML configuration item that was processed, from the NetPointSAML.properties file, an SAML policy domain authorization rule, or an authentication scheme, with the following messages:

- *domain.property=value*

  The corresponding SHAREid configuration item for the domain and the property was set to the value. MyDomain assertion profile items, for example NotOnOrAfter, are set for the assertion profile specified in the migration form. Key-related items are set in the Signer configuration element.

- *domain.property=value* **has been changed** to new-value

  The corresponding SHAREid configuration item had an existing value that could not be changed, for example, MyDomain URLs when Preserve NetPoint SAML URLs is not checked.

- *domain.property=value* **is not supported by SHAREid. It was ignored.**

  The feature corresponding to the configuration item is not supported by SHAREid, for example, MyDomain.MyAudiences.

- *domain.property=value* **is no longer used. It was ignored.**

  SHAREid does not require that this configuration item, for example, MyDomain.Domains. No functionality is lost.

- *domain.property=value* **is invalid. It was ignored.**

  The configuration property name or value is invalid.

- *keystore-alias*

  The key or certificate was copied from the NetPoint SAML keystore to the SHAREid keystore.

Completing the Migration

There are several things you need to do to complete the migration. For example, if you chose to preserve the NetPoint SAML keystore, the keys are imported and the migration tool changes the password of the signing key to match the SHAREid keystore password. In this case, you need to take a specific action before you restart the SHAREid server; otherwise you need to take a different action.

To complete the migration

1. Take the appropriate action below depending upon your choice during migration:

   a) If you chose to preserve the NetPoint SAML keystore, change the password of the migrated certificate to match the SHAREid keystore password before restarting SHAREid.

   b) If you did not preserve the NetPoint SAML keystore or URLs during migration, notify your partners to update their information about your domain.

2. Restart the SHAREid server.

3. To use the existing NetPoint SAML URLs, edit the httpd.conf and ssl.conf files in your Apache Proxy server using instructions in Apache documentation as a guide.

4. For Smartmarks, change the policy on the protected resource from using a Transfer Form authentication scheme to using the SHAREid SmartMarks authentication scheme.

Note: The migration tool does not populate the fields for the Transfer and Error URLs in a migrated domain unless these URLs were specified in the NetPoint SAML properties file.

---

5. Check the destination Domain entry for the domain that was migrated, and manually enter URLs for the servlets ObSAMLError and ObSAMLTransferService if needed.

   For example, if the destination domain in NetPoint SAML has the URL:

   https://*domain.company*.com:*port*/shareid/saml/ObSAMLReceiverService

   the transfer URL for the domain in SHAREid should be set to:

   https://*domain.company*.com:*port*/shareid/saml/ObSAMLTransferService

In a Migrated Domain

No error URL is defined unless an error URL for that domain was specified in the NetPoint SAML properties file. If no error URL is present in the migrated domain, SHAREid uses the default error URL.

SAML 1.1 support is not selected. If the domain also supports SAML 1.1, you will need to select SAML 1.1 support in the GUI.

The option “responds to authorization queries” is not selected unless this option was explicitly set in the NetPoint SAML properties file. In SHAREid, domains do not have this option selected by default.

No Subject DN or Issuer DN is defined unless these DNs are present in the NetPoint SAML properties file. Otherwise, you will need to enter these DNs manually.

Reverting a Migrated Environment

The migration tool makes a backup copy of the shareid-config.xml and keystore files before importing the NetPoint SAML configuration. The backup files are located in the same directories as the original files and named as follows:

shareid-config.xml.bak
keystore.bak

Previous backup files are numbered .bak.1, .bak.2, etc., with higher numbers for older backups.

The Revert option copies the shareid-config.xml.bak file to shareid-config.xml, and moves up any previous backup files. For example, .bak.1 becomes .bak, .bak.2 becomes .bak.1, and so on.

Because the keystore file is kept open by SHAREid 2.0, the keystore.bak cannot be copied to keystore, so you must perform that copy manually after stopping the SHAREid Server.

After reverting a migrated environment, certain migrated entries (migration Domain, Assertion Profile, and Mapping entries) still exist in SHAREid. In addition, all authentication-scheme entries exist in the NetPoint System Console. When you restart the SHAREid Server, the entries disappear in the SHAREid Admin Console. However, authentication-scheme entries in NetPoint should be removed manually if needed.

To revert a migrated environment

1. Start the migration by entering the URL for the migration tool.

   For example:

   http(s)://*host*:*port*/shareid/admin/migrate.jsp

   where *host* is the SHAREid Server host and *port* is either the open or the SSL port configured for SHAREid.

2. Enter your SHAREid Admin username and password when asked.

   The migration tool displays a form with two major options: Migrate and Revert.

3. Choose the Revert option.
4. Restart the SHAREid Server after reverting to have changes take affect.
5. Check the SHAREId Admin Console to ensure the migration Domain, Assertion Profile, and Mapping entries are removed; remove them manually if needed.
6. Check the NetPoint System Console for authentication-scheme entries and remove these manually, if needed.

Index