

**OPNET Authentication Service™**

## **Installation and Administrator Guide**

---

Release 1.1  
November 12, 2013

---

Riverbed Technology  
199 Fremont St.  
San Francisco, CA 94105 USA

---



## Copyright and Contacts

---

### Document Copyright

Title: OPNET Authentication Service User Guide  
Version: 1.1  
Revised: 11/12/13

© 2013 Riverbed Technology. All rights reserved.

Riverbed®, OPNET® and any Riverbed product or service name or logo used herein are trademarks or registered trademarks of Riverbed Technology, Inc. in the United States and other countries. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein cannot be used without the prior written consent of Riverbed Technology or their respective owners.

### Software Copyright

Product Name: OPNET Authentication Service  
Product Release: 1.1  
© 2013 Riverbed Technology  
All Rights Reserved.

### Contacts

Riverbed Technology  
199 Fremont St.  
San Francisco CA, 94105 USA

#### General

Telephone: 415.247.8800  
E-mail: [info@riverbed.com](mailto:info@riverbed.com)  
Web: <http://www.riverbed.com>

#### Technical Support

Telephone: 240.497.1200  
Fax: 240.497.1064  
E-mail: [support@riverbed.com](mailto:support@riverbed.com)

### This Documentation and Riverbed

This document and the accompanying product documentation describes the functions of the Riverbed software product(s) ("SOFTWARE") identified above (this document and the product documentation are collectively referred to as "DOCUMENTATION"). Riverbed Technology, 199 Fremont St., San Francisco, California 94105 is the sole owner of all rights, title, and interest to the DOCUMENTATION and SOFTWARE. Nothing herein shall grant or imply a license to the DOCUMENTATION or SOFTWARE. The right to use the DOCUMENTATION and SOFTWARE shall result only from entering into a Master Software License Agreement and a Software Usage Agreement, and paying the applicable license fees.

---

## Terms and Conditions of Use

### Eligible Users

This document is subject to restrictions on use and distribution is intended solely for persons who are subject to the terms and conditions of Riverbed's Software Master License Agreement or persons authorized by Riverbed ("Eligible Users"). As a condition of being granted access to and use of this document, each User represents that: i) the User is an Eligible User of a Licensee under a valid Riverbed Software Master License Agreement or the User is authorized by Riverbed and ii) the User accepts the terms and conditions of Riverbed's Software Master License Agreement and the terms and conditions governing the use of this document.

### Confidential Information

The User agrees that the DOCUMENTATION, including this document, are the proprietary property of Riverbed and constitutes a trade secret of Riverbed. The User agrees that access to and use of this document does not grant any title or rights of ownership. The User shall not copy or reproduce, in whole or in part, disclose or permit third parties access to this document without the prior written consent of Riverbed. This document may not be stored, in whole or in part, in any media without the prior written consent of Riverbed. Any unauthorized use of this document will be subject to legal action that may result in criminal and/or civil penalties against the User.

### Intellectual Property and Proprietary Notices

© 2013 Riverbed Technology. All rights reserved.

Riverbed and any Riverbed product or service name or logo used herein are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed Technology or their respective owners.

The absence of a patent or mark from the above notices does not constitute a waiver of intellectual property rights that OPNET Technologies, Inc. has established in any of its products, service names or marks in use. Alteration, removal, obscuring, or destruction of any proprietary legend, copyright, trademark, patent, or intellectual property notice contained in this document is prohibited.

### Restricted Rights Legend

The DOCUMENTATION and SOFTWARE are subject to the restrictions on use and distribution in the Riverbed Software Master License Agreement (for Agencies of the U.S. Government). Any use of the DOCUMENTATION or any SOFTWARE by an agency of the U.S. Government or a direct contractor of an agency of the U.S. Government requires a valid Riverbed Software Master License Agreement and Riverbed Software Usage Agreement.

For all users, this Software and Documentation are subject to the restrictions (including those on use and distribution) in Riverbed's Master License Agreement. Use of this Software or Documentation requires a current Riverbed license and shall be governed solely by the terms of that license. All other use is prohibited. For the U.S. Government and its contractors, the Software is restricted computer software in accordance with Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. The Software and Documentation qualify as "commercial items," "commercial computer software," and "commercial computer software documentation."

### No Warranty and Limitation of Liability

ALL INFORMATION PROVIDED IN THIS USER MANUAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND EITHER EXPRESS OR IMPLIED INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. No representations by Riverbed, such as statements of capability, suitability for use, accuracy or performance, shall be a warranty by Riverbed, or bind Riverbed or vary any term or condition of any Software Master License Agreement, unless contained in written agreement and signed by Riverbed and any other party or parties to such Software Master License Agreement.

In no event shall Riverbed be liable for any incidental, indirect, special, or consequential damages whatsoever (including but not limited to lost profits arising out of or relating to this document or the information contained herein) even if Riverbed has been advised, knew, or should have known of the possibility of such damages.

THE USER UNDERSTANDS AND ACCEPTS THAT RIVERBED SHALL NOT BE LIABLE FOR DAMAGES WHICH ARE: (i) INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR CONSEQUENTIAL, OR (ii) THE RESULT FROM LOSS OF USE, DATA, OR PROFITS, OR (iii) FROM THE USE OF THE SOFTWARE AND DOCUMENTATION, WHETHER BROUGHT IN AN ACTION OF CONTRACT, TORT, OR OTHERWISE, EVEN IF RIVERBED WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

### **Export Controls**

Any User of the DOCUMENTATION including this document shall comply with the laws of the United States, including the provisions of the U.S. Department of Commerce, Bureau of Industry Security ("BIS"), *Export Administration Regulations (EAR)*, the U.S. Department of State, International Traffic in Arms Regulations, and the U.S. Department of Treasury, Office of Foreign Assets Control, regarding the export, re-export and disclosure of the DOCUMENTATION or the SOFTWARE. Any export, re-export or disclosure of the DOCUMENTATION or the SOFTWARE shall be subject to the prior written consent of Riverbed. Users shall not remove any Destination Control Notices provided by Riverbed from the DOCUMENTATION or the SOFTWARE.

### **Destination Control Statement**

The DOCUMENTATION and the SOFTWARE were manufactured in the United States by Riverbed. The initial export of the DOCUMENTATION and the SOFTWARE from the United States, and any subsequent relocation or re-export to another country shall comply with the laws of the United States relating to the export of technical data, equipment, software, and know-how. Any diversion contrary to the laws of the United States is prohibited.

# Contents

---

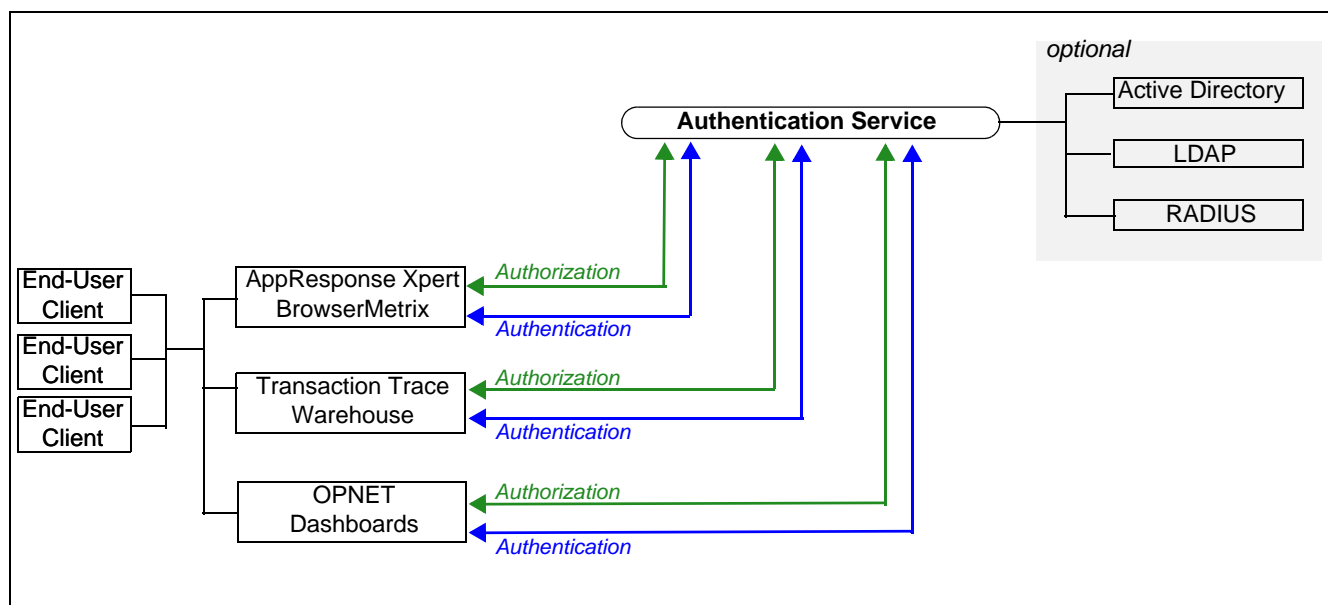
<b>1</b>	<b>Introduction</b>	<b>6</b>
	Implementing Authentication Service with Compatible OPNET Components . . . . .	8
	Migration Considerations . . . . .	11
	Migration Sequence . . . . .	11
	Migration of Transaction Trace Warehouse Users and Roles . . . . .	12
	Understanding the Authentication Service User Interface . . . . .	13
<b>2</b>	<b>Installation and Configuration</b>	<b>14</b>
	Step 1: Prepare for the Installation . . . . .	15
	Environment and Configuration Considerations . . . . .	16
	Step 2: Install Authentication Service . . . . .	23
	Upgrade Authentication Service . . . . .	24
	Step 3: Configure Authentication . . . . .	26
	Configure Authentication Modules & Fetch Users/Groups (Active Directory/LDAP) . . . . .	26
	Configure Authentication Module (RADIUS Server) . . . . .	30
	Configure Local Users . . . . .	40
	Step 4: Configure Authorization . . . . .	41
	Certificate Management . . . . .	43
<b>3</b>	<b>AAM to OAS Migration Utility</b>	<b>45</b>
	Requested Information . . . . .	46
	Running the Utility . . . . .	49
<b>4</b>	<b>Backups: Create and Restore</b>	<b>50</b>
	Create a Backup . . . . .	52
	Restore a Backup . . . . .	53
<b>5</b>	<b>Useful How-To's and FAQs/Troubleshooting</b>	<b>54</b>
	Authentication Service Configuration . . . . .	55
	Start/Stop Authentication Service . . . . .	57
	Access Control Management . . . . .	58
	Uninstall Authentication Service . . . . .	72
	Frequently Asked Questions/Troubleshooting . . . . .	72
<b>App A</b>	<b>Active Directory: A Brief Introduction</b>	<b>80</b>
	Active Directory: The Basics . . . . .	80
	Active Directory: Browsing Utilities . . . . .	83
	Active Directory: Glossary . . . . .	84
<b>App B</b>	<b>Active Directory: Configuration Fields</b>	<b>86</b>
	<b>System Requirements</b>	<b>89</b>
	<b>Index</b>	<b>90</b>

# 1 Introduction

OPNET Authentication Service provides authentication (including single sign-on) and authorization (account access privileges) to other OPNET components deployed in the environment. And since authentication and authorization are specified on a single server, the information can be quickly defined and easily maintained.

The following figure shows a typical deployment of Authentication Service with other supported OPNET components.

**Figure 1-1 Typical Deployment of OPNET Authentication Service**



## Getting Started...

To install and configure Authentication Service, review the following sections:

- [Implementing Authentication Service with Compatible OPNET Components](#)
- [Migration Considerations](#)
- [Installation and Configuration](#)

For additional information, see:

- Component Installation Instructions (available on the Support website)
  - BrowserMetrix
  - Transaction Trace Warehouse
  - OPNET Dashboards
- [Understanding the Authentication Service User Interface](#)
- [Useful How-To's and FAQs/Troubleshooting](#)

If you require assistance, contact Technical Support.

## Implementing Authentication Service with Compatible OPNET Components

OPNET Authentication Service is bundled and installed with other OPNET components that leverage its authentication and authorization capabilities. In fact, the installer will prompt for the components that you want to install.

The following table lists the OPNET components that are compatible with OPNET Authentication Service. For each component, the table indicates the compatible releases and whether an install of OPNET Authentication Service is required to implement the component.

**Table 1-1 Compatible OPNET Components**

Component	Release	Required
<b>BrowserMetrix</b> —delivers end-user experience (EUE) monitoring for web applications	2.2+	Yes
<b>Transaction Trace Warehouse</b> —stores continuous transaction data harvested from application tiers monitored by AppInternals Xpert.	2.2+	Yes
<b>OPNET Dashboards</b> —provide a 24x7 picture of network and application health, aggregated from multiple existing management systems and integrated with OPNET's planning solutions.	2.2+	Yes

When Authentication Service is required, the software can be installed on the same computer as one or more of the compatible component(s) or on a different computer. If installed on different computers, the computers must be accessible to one another.

**Important**—Currently, the installers are packaged as follows:

- Authentication Service + OPNET Dashboards
- Authentication Service + BrowserMetrix + Transaction Trace Warehouse

Note that the same Authentication Service is available with both installers. Unless you want multiple installs of Authentication Service, you should install Authentication Service only once. For the installation sequence, see [Migration Considerations](#).



The following table lists the recommended sequence for installing/upgrading Authentication Service and other OPNET components.

**Table 1-2 Sequence for Installing/Upgrading Multiple Components with OPNET Authentication Service**

	<b>Local Server</b> <i>(OAS installed on the same server as the application software)</i>	<b>Remote Server</b> <i>(OAS installed on a different server than the application software)</i>
<b>Initial Install</b>	<ol style="list-style-type: none"> <li>1. Run the OAS+BMX+TTW installer.</li> <li>2. Run the OAS+ODS installer. (OAS is auto-detected)</li> </ol>	<ol style="list-style-type: none"> <li>1. Run the OAS+BMX+TTW installer.</li> <li>2. Run the OAS+ODS installer. (Specify the server name of the OAS install.)</li> </ol>
<b>Upgrade</b>	<b>If upgrading ODS only:</b> <ol style="list-style-type: none"> <li>1. Run OAS+ODS installer (If upgrading from ODS 1.0, migrate the AAM settings.)</li> <li>2. Run the OAS+BMX+TTW installer.</li> </ol>	<b>If upgrading ODS only:</b> <ol style="list-style-type: none"> <li>1. Upgrade OAS (If upgrading from ODS 1.0, migrate the AAM settings.)</li> <li>2. Upgrade ODS</li> <li>3. Install BMX</li> <li>4. Install TTW</li> </ol>
	<b>If upgrading TTW only:</b> <ol style="list-style-type: none"> <li>1. Run the OAS+BMX+TTW installer (If upgrading from TTW 1.0/2.0, migrate the AAM setting.)</li> <li>2. Run the OAS+ODS installer</li> </ol>	<b>If upgrading TTW only:</b> <ol style="list-style-type: none"> <li>1. Upgrade OAS (If upgrading from TTW 1.0/2.0, migrate the AAM settings)</li> <li>2. Upgrade TTW</li> <li>3. Upgrade BMX</li> <li>4. Install ODS</li> </ol>
	<b>If upgrading ODS and TTW:</b> <ol style="list-style-type: none"> <li>1. Run the OAS+ ODS installer (If upgrading from ODS 1.0, migrate the AAM settings.)</li> <li>2. Run the OAS+BMX+TTW installer (If upgrading from TTW 1.0/2.0, do <i>not</i> migrate the AAM settings.)</li> <li>3. If upgrading TTW 1.0/2.0, run the “AAM to OAS Migration” utility to migrate TTW settings from AAM to OAS</li> </ol>	<b>If upgrading ODS and TTW:</b> <ol style="list-style-type: none"> <li>1. Upgrade OAS (If upgrading from ODS 1.0, migrate the AAM settings.)</li> <li>2. Upgrade ODS</li> <li>3. Upgrade BMX</li> <li>4. Upgrade and TTW (If upgrading from TTW 1.0/2.0, do <i>not</i> migrate the AAM settings.)</li> <li>5. If upgrading TTW 1.0/2.0, run the “AAM to OAS Migration” utility to migrate TTW settings from AAM to OAS</li> </ol>
<b>Legend:</b> OAS = OPNET Authentication Service BMX = BrowserMetrix TTW = Transaction Trace Warehouse ODS = OPNET Dashboards AAM = OPNET AAM Server		

**Note**—For important installation information, see [Migration Considerations](#).

The general installation workflow is as follows:

- 1) Download the software installers and installation documentation from the Riverbed Technical Support website.
- 2) Double-click the installer to start the installation
- 3) The installer prompts for the components to install.

**Note**—If Authentication Service is already installed on another server, unselect the Authentication Service option. The installer will prompt for the hostname of the Authentication Service server.

- 4) Follow the instructions on the screen.

## Migration Considerations

OPNET Authentication Service replaces OPNET AAM, used by earlier versions of OPNET components, such as OPNET Dashboards 1.0 and Transaction Trace Warehouse 1.0/2.0.

If you are upgrading either OPNET Dashboards 1.0 or Transaction Trace Warehouse 1.0/2.0, those upgrades must also migrate AAM to Authentication Service.

### Migration Sequence

Note the following migration considerations:

- **Upgrade an Earlier Version of Dashboards *and* Transaction Trace Warehouse**

If earlier versions of multiple components are installed, always upgrade OPNET Dashboards first. The OPNET Dashboards upgrade performs an internal migration to Authentication Service that must occur before any other upgrade.

Use the component installer to install the Authentication Service and upgrade OPNET Dashboards on the same system. The installer prompts for the location of the AAM files and migrates them to the Authentication Service. This upgrade and migration does not require manual steps or assistance from Riverbed Technical Support.

The migration for the other components (e.g., upgrading an existing install of Transaction Trace Warehouse and AAM) requires the [AAM to OAS Migration Utility](#).

- **Upgrade an Earlier Version of Transaction Trace Warehouse *Only***

If an earlier version of Transaction Trace Warehouse is installed, use the component installer to install Authentication Service on the same system and upgrade Transaction Trace Warehouse. The installer prompts for the location of the AAM files and migrates them to Authentication Service. This upgrade and migration does not require manual steps or assistance from Riverbed Technical Support.

- **Migrate AAM on One Server to Authentication Service on Another Server**

Installed components (e.g., BrowserMetrix, Transaction Trace Warehouse, OPNET Dashboards) can access an Authentication Service installed on a remote server. In this case, migrating earlier versions of components requires manual steps. Contact Technical Support for assistance.

## Migration of Transaction Trace Warehouse Users and Roles

Note the following information regarding role assignment when upgrading Transaction Trace Warehouse from 1.0/2.0:

- Active Transaction Trace Warehouse users with admin privileges will get the TTWAdmin role, but not the RootAdmin role.
- Active Transaction Trace Warehouse users without admin privileges will only get the TTWAccess role.
- Inactive Transaction Trace Warehouse users will be migrated, but will not get any role in OPNET Authentication Service.
- The “admin” user (the default user one uses to first log into the system) will always get the RootAdmin role.
  - If the “admin” user was active in Transaction Trace Warehouse before the upgrade, then that user will also get the TTWAdmin role.
  - If the “admin” user was inactive in Transaction Trace Warehouse before the upgrade, then that user will *not* get the TTWAdmin role, but the user will be made active. And, since the user has the RootAdmin role, he could easily log into OPNET Authentication Service and give himself the TTWAdmin role. Therefore, if the “admin” user was inactive before the upgrade, then you need to reconfigure the “admin” user after the upgrade.

### Upgrading from Transaction Trace Warehouse 2.1 Build 1812

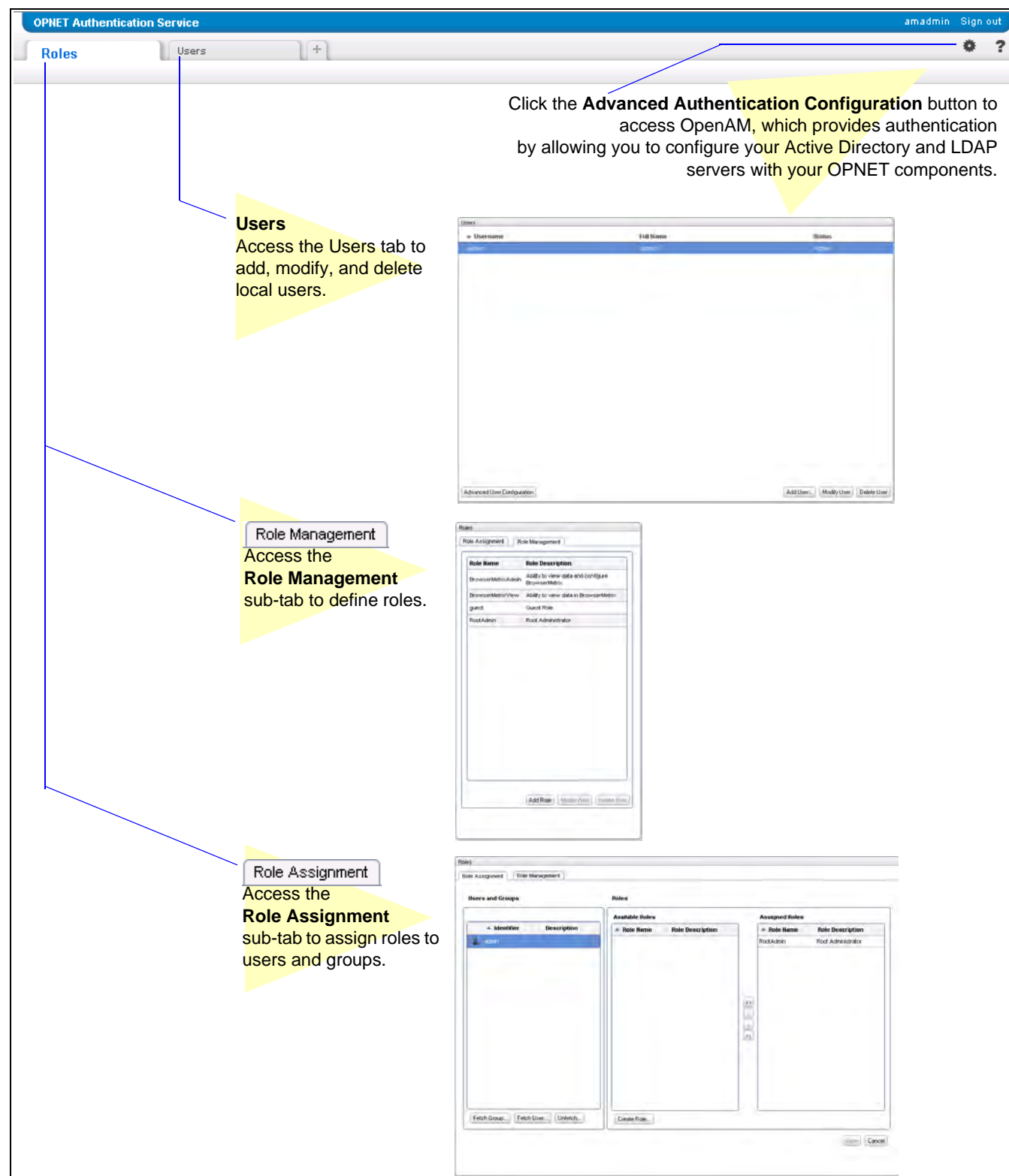
If upgrading from Transaction Trace Warehouse 2.1 build 1812 (from the AppInternals Xpert 8.5 Advanced Technology Release), then you must manually add the TTWAdmin role and then assign the role to the “admin” user.

- 1) To add a role, see [How to add a role](#).  
When prompted for the role name, enter: TTWAdmin  
(Be sure to enter the role name exactly as shown.)
- 2) To assign a role, see [How to assign a role](#).
  - a. In the first column, select the “admin” user.
  - b. In the second column, select the newly added “TTWAdmin” role.
  - c. Click the “>” button between the second and third columns.
  - d. Click Save.

## Understanding the Authentication Service User Interface

OPNET Authentication Service has a simple interface for defining roles and users. The following figure shows a high-level overview of the interface.

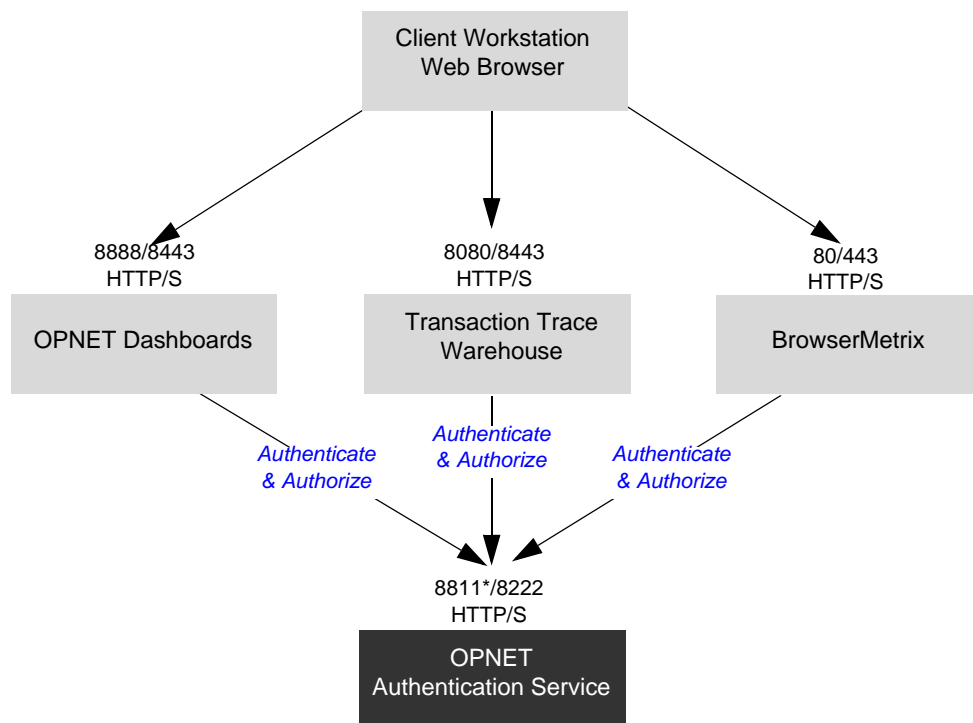
**Figure 1-2 User Interface at a Glance**



## 2 Installation and Configuration

OPNET Authentication Service is installed as part of a software solution with other OPNET components. The following figure shows the architecture of the software solution.

**Figure 2-1 Solution Architecture**



\* If upgraded from Authentication Service 1.0, the HTTP port remains 8111.

The installation and configuration process will differ slightly depending on the environment. However, for a smooth installation, perform the steps listed in the following table.

**Table 2-1 General Installation Workflow**

Step / Description	
<input type="checkbox"/>	<a href="#">Step 1: Prepare for the Installation</a>
<input type="checkbox"/>	<a href="#">Step 2: Install Authentication Service</a>
<input type="checkbox"/>	<a href="#">Step 3: Configure Authentication</a> (Includes configuring authentication modules and fetching external users and groups)
<input type="checkbox"/>	<a href="#">Step 4: Configure Authorization</a>

For information about configuring secure communication (SSL) between Authentication Service and Active Directory/LDAP servers, see [Certificate Management](#).

For information about upgrading from a previous version of Authentication Service, see [Upgrade Authentication Service](#).

## Step 1: Prepare for the Installation

For a smooth installation carefully review the following sections:

- [Environment and Configuration Considerations](#)
- [Required Installation Information](#)

## Environment and Configuration Considerations

Before installing the software, it is a good idea to think about and plan how you want to configure the software for your environment. Due to the various environments and the built-in flexibility, it is impossible to document the exact configuration that is right for your implementation. To help, consider the information in the following table.

Prepare for Installation	
Authentication: Define External and/or Local Users	
<input type="checkbox"/> External Users	<p>If you have existing authentication modules (e.g., Active Directory, LDAP) that you want to use, then you must configure Authentication Service.</p> <p>To configure Authentication Service, you need the following information:</p> <ul style="list-style-type: none"> <li>• The server and Bind DN information for each module</li> <li>• If you have multiple authentication modules, consider the order that the modules should be accessed for authentication</li> </ul> <p>For more information, see <a href="#">Step 3: Configure Authentication</a>.</p>
<input type="checkbox"/> Local Users	<p>If you plan to use “local” users (that is users that are defined in Authentication Service), then prepare to define each user in Authentication Service. For each user, you need to specify an ID, first name, last name, and a password.</p> <p>For more information, see <a href="#">Step 3: Configure Authentication</a>.</p>
Authorization: Define Roles and Assign Roles to Users	
<input type="checkbox"/> OPNET Components	<p>Which OPNET components will be accessed using Authentication Service:</p> <ul style="list-style-type: none"> <li>• BrowserMetrix</li> <li>• Transaction Trace Warehouse</li> <li>• OPNET Dashboards</li> </ul>
<input type="checkbox"/> Roles	<p>For each OPNET component, consider the end-user roles. For example: read-only, administrator.</p> <p>Note that Authentication Service includes default roles for BrowserMetrix and Transaction Trace Warehouse. See <a href="#">Table 2-4 Default Roles</a>.</p>
<input type="checkbox"/> Role Assignments	<p>For each user or group of users, which role(s) are best. (Users and groups can be assigned multiple roles.)</p>



## Accounts

The following table lists the accounts created by the Authentication Service installer.

**Table 2-2 Authentication Service Accounts**

Account	Description
Directory Manager (Datastore user)	Used by Authentication Service to connect to the built-in datastore. Additionally, the password specified during installation is required when performing a manual migration.  <b>Note</b> —Unless instructed by technical support, you should not login as this user.
admin (Admin user)	Used to login to Authentication Service as the administrator. Additionally, this user/password is required when upgrading from a previous release.  The default username is <i>admin</i> . The default password is <i>opnet</i> .  For related information, see: <ul style="list-style-type: none"> <li>• <a href="#">How to change/reset a user password (local user only)</a></li> <li>• <a href="#">How to change the specially-designated administrator</a></li> </ul>

---

**Note**—When configuring Authentication Service, you may see the account/group *service-account*. This is an account/group used by the Authentication Service software. Be sure not to delete or alter the account in any way. Otherwise, Authentication Service will not function.

---



---

**Note**—During installation, you are prompted for account passwords that are used by Authentication Service to run without user intervention. The passwords are encrypted and stored in configuration files on the server. Also, the information required to decrypt the passwords is available on the server. Therefore, for security reasons, it is important to restrict access to the server to protect the passwords.

---

## Required Installation Information

The following table lists the information requested during the installation process. Fill-out the table with the requested information. Then be sure to retain the information for future reference.

**Important**—Be sure to retain the values that you entered for the requested information. This information is necessary for future migrations and troubleshooting.

**Table 2-3 Information Requested during Installation**

Install Parameter	Description / Your Setting
<b>Install location</b>	
<input type="checkbox"/> Install Location	Specify the destination (home) directory for the installation.  <i>Default: C:\OPNET</i>
	<b>Your Setting:</b> <ul style="list-style-type: none"> <li>• Destination/home directory:</li> </ul>
<b>AAM Migration</b>	
<input type="checkbox"/> Import users and roles from existing OPNET AAM Server (optional)	If you have an existing install of OPNET AAM from which you want to import users and roles to Authentication Service, you must specify the location of the AAM Folder.  <b>Important</b> —If you need to migrate users/roles from multiple AAM Servers and/or from multiple components, use <a href="#">AAM to OAS Migration Utility</a> after installation.
	<b>Your Setting:</b> <ul style="list-style-type: none"> <li>• Location of the AAM folder:</li> </ul>

**Table 2-3 Information Requested during Installation (Continued)**

Install Parameter	Description / Your Setting
<b>Configuration Information</b>	
<input type="checkbox"/> Directory Manager Password	<p>Specify a password for the Directory Manager account, which is a service account used by the software.</p> <p>For more information about the Directory Manager, see <a href="#">Accounts</a>.</p> <p>Note the following information regarding the password:</p> <ul style="list-style-type: none"> <li>• The password must have a minimum of 8 characters.</li> <li>• By default, the initial password specified for <i>Directory Manager</i> is also assigned to the OpenAM administrative user, <i>amadmin</i>. However, after the initial password is set, changing the password for one of these users does not change the password for the other user.</li> </ul> <p>(Don't confuse the <i>amadmin</i> user with the <i>admin</i> user. The <i>admin</i> user is the default administrator user, with the default password of <i>opnet</i>.)</p> <ul style="list-style-type: none"> <li>• Use letters, numbers, and the following special characters: ! (exclamation), @ (at sign), * (asterisk), ( ) (open and close parentheses), _ (underscore), - (hyphen), . (period), { } (open and close curly brackets). Do not use spaces.</li> </ul> <hr/> <p><b>Your Setting:</b></p> <ul style="list-style-type: none"> <li>• Directory Manager Password:</li> </ul>
<input type="checkbox"/> Hostname (Fully-Qualified Domain Name) or IP Address	<p>Confirm the hostname of the Authentication Service server.</p> <p>If incorrect, the hostname can be a Fully Qualified Domain Name (recommended), an IP address or a Short Name. (See <a href="#">Important Notes</a>.)</p> <p><b>Note</b>—If the server has multiple interfaces, specify the interface that you intend to use to access Authentication Service. The generated security certificate is based on the specified hostname.</p> <hr/> <p><b>Your Settings:</b></p> <ul style="list-style-type: none"> <li>• Hostname:</li> </ul>

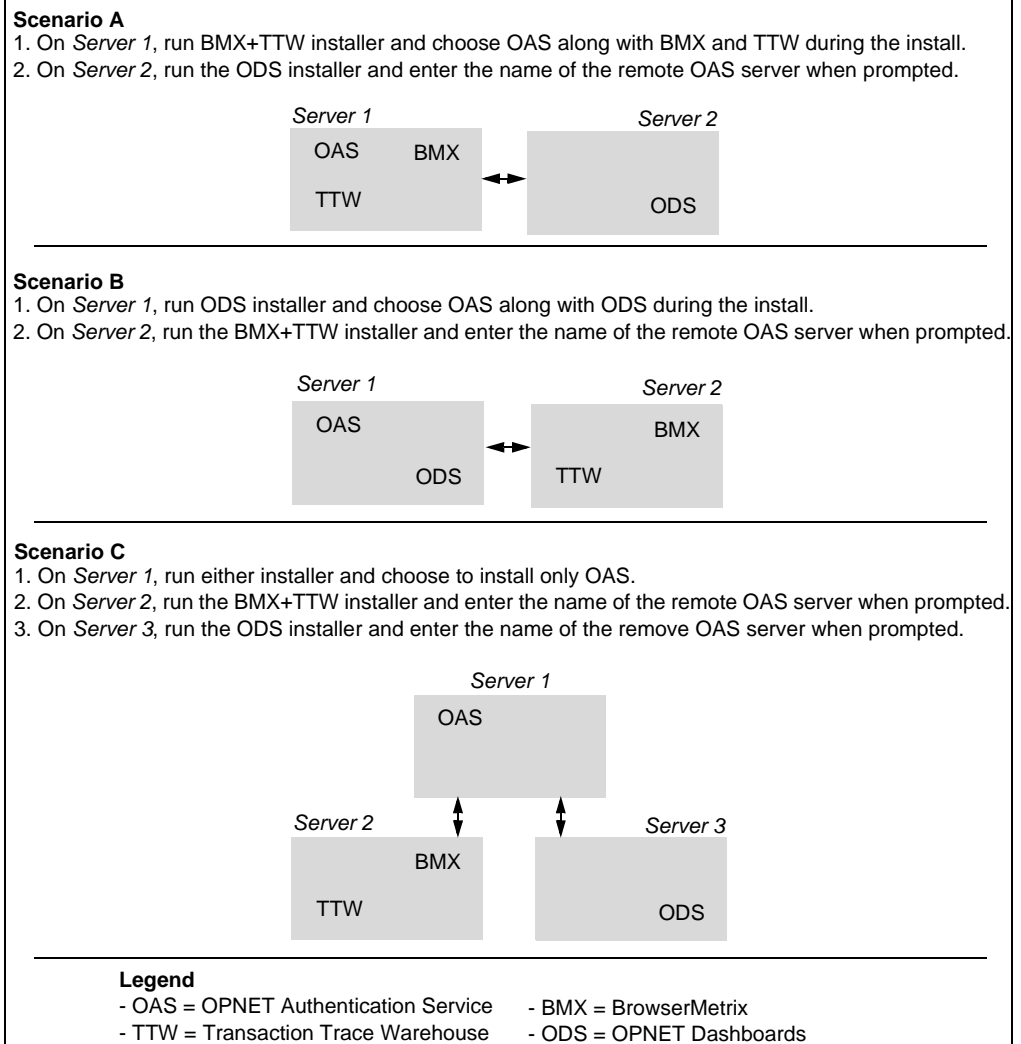
**Table 2-3 Information Requested during Installation (Continued)**

Install Parameter	Description / Your Setting
<b>Application Server Information</b>	
<input type="checkbox"/> Ports	<p>Specify the ports used for communication with Authentication Service:</p> <p><i>Default:</i></p> <ul style="list-style-type: none"> <li>• HTTP Port (unsecure): 8811</li> <li>• HTTPS Port (secure): 8222</li> </ul> <hr/> <p><b>Your Setting:</b></p> <ul style="list-style-type: none"> <li>• HTTP Port (unsecure):</li> <li>• HTTPS Port (secure):</li> </ul>
<input type="checkbox"/> Keystore Password	<p>Specify the password used to protect the keystore file, which contains the HTTPS certificate and keys. This password is needed when importing security certificate(s) for secure communication with LDAP/Active Directory servers.</p> <p>The keystore password must satisfy the following requirements:</p> <ul style="list-style-type: none"> <li>• The password must have a minimum of 6 characters.</li> <li>• The password must begin with an alphabetic character.</li> <li>• The password must <i>not</i> contain spaces or special characters, except underscores. Underscores are acceptable.</li> </ul> <hr/> <p><b>Your Setting:</b></p> <ul style="list-style-type: none"> <li>• Keystore Password:</li> </ul>
<input type="checkbox"/> Self-signed certificate	<p>Specify the organization information used to create a self-signed and/or third-party certificate.</p> <hr/> <p><b>Your Settings:</b></p> <ul style="list-style-type: none"> <li>• Organizational Unit:</li> <li>• Organization:</li> <li>• City:</li> <li>• State/Province:</li> <li>• Country Code:</li> </ul> <p><b>Note</b>—Only enter letters (A-Z, a-z), numbers (0-9), and spaces. Do not enter special characters.</p>

## Important Notes

- Authentication Service must be installed/upgraded first. During the installation of other components, you must specify the location of Authentication Service. (For additional upgrade information, see [Migration Considerations](#).)
- Authentication Service must be accessible to all other components that will use Authentication Service. Therefore, the server where Authentication Service is installed must be accessible to the server(s) where the other components of the solution are installed. The following figure shows example component installs on one or more servers.

**Figure 2-2 Example Component Installs**



- The Authentication Service server's actual hostname or Windows domain name does not necessarily have to change or be set. But DNS must recognize or set the correct domain name for the server that Authentication Service is installed on.

- For single-sign on to work, the following items must be true:
  - All components must be installed on the same server or the Authentication Service server must share a common domain name with the servers on which the other components are installed.

For example:

- oas.**opnet.com**, bmx.**opnet.com**, ttw.**opnet.com** would work
- oas.**opnet.com**, bmx.**riverbed.com**, ttw.**acme.com** would *not* work
- The cookie domain, which is determined during installation, must end in .com, .edu, .net, .org, .gov, .mil, .int or contain three components (e.g., .example.co.uk).

## Step 2: Install Authentication Service

The following procedure describes how to install Authentication Service.

---

### Procedure 2-1 Installing OPNET Authentication Service

- 1 Log into the designated Authentication Service host computer as Administrator.

**Important**—Be sure to login as administrator. Do not use the “Run as Administrator” option, which may cause issues later in the installation/configuration process.

- 2 Disable any virus scan applications running on the server.

Virus scan applications can corrupt component installations and it is highly recommended that you turn those applications off before running the installer.

- 3 Access the Authentication Service software installer:

- If installing from a DVD, insert the DVD into the optical drive and double-click on the icon that represents the DVD.
- If not installing from DVD, download the install program and copy it to the host computer.

- 4 Verify that the 8dot3 Windows property is enabled:  
If the 8dot3 Windows property is not enabled, then the installer may hang during installation.

To determine the setting:

- 4.1 Open a Command Prompt.

- 4.2 Enter the following command:

```
fsutil behavior query disable8dot3
```

If the response shows `disable8dot3 = 0`, then the property is already enabled. Skip to the [step 5](#).

If the response shows `disable8dot3 = 1`, then the property is disabled and you must change setting.

To change the setting:

- 4.3 In the Command Prompt, enter the following command

```
fsutil behavior set disabled8dot3 0
```

- 4.4 To verify the change, close the Command prompt, open a new command prompt, and enter the command shown in [step 4.2](#).

For more information about the 8dot3 property and settings, see <http://support.microsoft.com/kb/121007>.

- 5 Double-click on the install program to run the installer.

- 6 When prompted, enter the requested information. See [Table 2-3 Information Requested during Installation](#).
- 7 When the installation completes, click Done.
- 8 Enable any virus scanning software that was disabled in [step 2](#).

---

#### End of Procedure 2-1

---

## Upgrade Authentication Service

The following procedure describes the installation process when upgrading from a previous version of Authentication Service. When complete, the Authentication Service retains all of the settings that were configured for the previous installation.

**Important**—During the upgrade, Authentication Service will be shut down. Therefore, components that depend on Authentication Service for authentication/authorization will not be accessible during the upgrade. Plan the upgrade accordingly.

---

### Procedure 2-2 Upgrading OPNET Authentication Service

- 1 Run the Authentication Service installer on the same server where the older version of Authentication Service is installed.
- 2 The installer prompts for the Authentication Service administrative username/password. The default is admin/opnet.
  - ➔ During the upgrade process, the previous Authentication Service configuration is backed up to the user's home directory. For example:  
C:\Users\OPNET\OPNET Authentication Service Backup.
- 3 If you upgrade Authentication Service *without* upgrading the components that access Authentication Service for authentication/authorization (e.g., BrowserMetrix, Transaction Trace Warehouse, OPNET Dashboards), then you must re-import the security certificate into each of these components.

**Note**—Skip this step if all components have/will be upgraded.

The following sub-steps describe how to import the certificate. Perform the sub-steps for each component.

- 3.1 If the component (BrowserMetrix, Transaction Trace Warehouse, OPNET Dashboards) is on a different server than Authentication Server, then copy the certificate to the server.
- 3.2 Open a command prompt.



- 3.3** Use the keytool command to import the security certificate. For more information about the keytool command, see [Certificate Management](#).

The syntax of the keytool command is as follows:

```
keytool -import -alias <AliasName> -file
<PathOfCertificate> -keystore <KeystoreLocation>
```

Examples:

- The following command imports a self-signed certificate into BrowserMetrix. The command assumes that BrowserMetrix and Authentication Service are installed on the same server. If the two components are on different servers, you must change the location of the certificate file.

```
"C:\OPNET\Authentication Service\Jre7\bin\keytool.exe"
-import -alias oas.keystore -file
"C:\OPNET\Authentication
Service\Secure\openam-keystore.cer" -keystore
C:\OPNET\JBoss\5.1.0\Jre6_x64\lib\security\cacerts
```

- The following command imports a self-signed certificate into Transaction Trace Warehouse. The command assumes that Transaction Trace Warehouse and Authentication Service are installed on the same server. If the two components are on different servers, you must change the location of the certificate file.:

```
"C:\OPNET\Authentication Service\Jre\bin\keytool.exe"
-import -alias oas.keystore -file
"C:\OPNET\Authentication
Service\Secure\openam-keystore.cer" -keystore
C:\OPNET\JBoss\5.1.0\Jre\lib\security\cacerts
```

- 3.4** Respond to the prompts:

- Enter keystore password: <password>
- Trust the certificate (y): yes

- 3.5** Restart the component using the component's Stop and Start shortcut option on the Start menu.

**Reminder**—Repeat [step 3](#) for each component that you did not upgrade. Failure to perform these steps will result in an error when you attempt to access that component.

## End of Procedure 2-2

---

## Step 3: Configure Authentication

This step includes the following sub-tasks:

- [Configure Authentication Modules & Fetch Users/Groups \(Active Directory/LDAP\)](#)

**Note**—Skip this sub-task if you do not intend to authenticate users with your existing Active Directory and/or LDAP servers.

- [Configure Authentication Module \(RADIUS Server\)](#)

**Note**—Skip this sub-task if you do not intend to authenticate users with your existing RADIUS server.

- [Configure Local Users](#)

**Note**—Skip this sub-task if you do not intend to have local users. Instead, all of the users will be defined in existing authentication modules.

### Configure Authentication Modules & Fetch Users/Groups (Active Directory/LDAP)

---

#### Procedure 2-3 Configuring Authentication Modules & Fetching Users/Groups

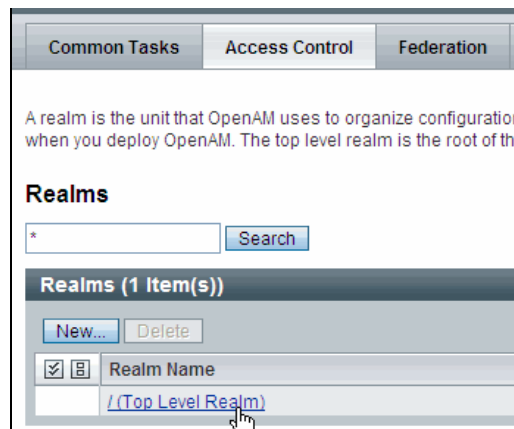
- 1 Log in to OPNET Authentication Service as the administrator:
  - 1.1 From the Start menu, choose Start > All Programs > OPNET Authentication Service > Launch OPNET Authentication Service.  
➡The Login page appears.
  - 1.2 In the Login page, enter the default administrative user name (admin) and the password (opnet).  
➡OPNET Authentication Service appears.
- 2 Click the “Advanced Configuration” option to access OpenAM.

The “Advanced Configuration” option is the gear icon in the upper-right.



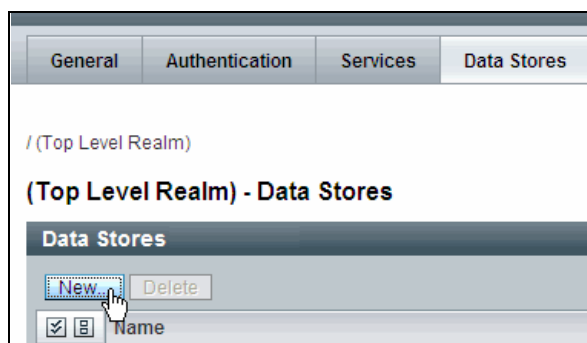
- 3 Configure authentication modules:
  - 3.1 Click the “Access Control” tab.
  - 3.2 Click the “/(Top Level Realm)” hyperlink

## 3.3



3.4 Click the “Data Stores” tab.

3.5 Click “New...”.



➡ The “Step 1 of 2: Select Type of Data Store” page appears.

The screenshot shows the 'Step 1 of 2: Select Type of Data Store' page. It contains a form with the following fields:

- Name:** A text input field.
- Type:** A radio button selection menu with the following options:
  - ☒ Active Directory
  - ☐ Active Directory Application Mode (ADAM)
  - ☐ Database Repository (Early Access)
  - ☐ OpenDJ
  - ☐ Sun DS with OpenAM schema
  - ☐ Tivoli Directory Server

3.6 Specify the following information and click **Next**:

- **Name**—Enter a name that describes authentication server. This name is used to identify the server in the user interface.
- **Type**—Select the authentication server type which most closely corresponds to your authentication sever. The selected corresponding type determines the default options.

## 3.7 The “Step 2 of 2: Select Type of Data Store” page appears.

**Step 2 of 2: New Data Store - Active Directory**

\* Name:

Load schema when finished: ☐

---

**Server Settings**

\* LDAP Server

Current Values:

New Value:

Format: LDAP server host name:port | server\_ID | site\_ID

LDAP Bind DN:   
A user or admin with sufficient access rights to perform the supported operations.

LDAP Bind Password:

LDAP Bind Password (confirm):

\* LDAP Organization DN:

3.8 Under **LDAP Server**, in the **New Value** field, enter the LDAP server host name (using the format *server:port*) and click **Add**.

**Note**—Only specify a single server. If necessary, remove any servers that don’t belong (such as the default server). To remove a server, click the server value in the **Current Values** field and then click **Remove**.

➡ The server name appears in the list of Current Values.

## 3.9 Specify other configuration settings, as needed.

See [Table B-1 New Data Store - Active Directory](#).

3.10 Click **Finish/Save**.3.11 If editing an existing module, click the **Back to Data Stores** button.3.12 To verify, click the **Subjects** tab. Verify that the user names shown are the expected names.

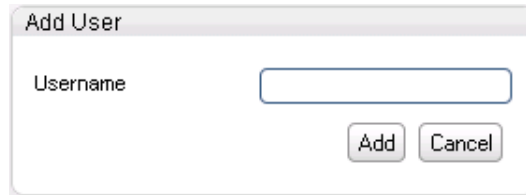
**Important**—Only a partial list (e.g., approximately the first 150 users/groups) is shown. If a particular user/group is not shown, try using the search feature to filter the list.

## 4 Fetch external users/groups:

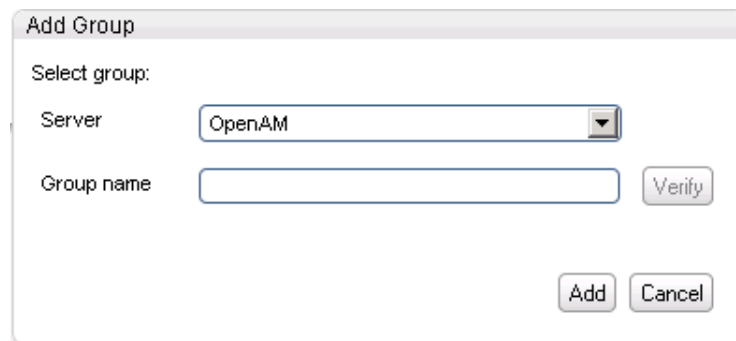
Perform this step to fetch external users/groups from authentication modules. After a user/group has been fetched (added to the OPNET Authentication Service interface), you can assign roles to the users/groups.

**4.1** Click the **Roles** tab and the **Role Assignment** sub-tab.

**4.2** To fetch a user, click the **Fetch User...** button. In the **Add User** dialog box, enter the username and click **Add**. The external user is added to the list of users and groups.

The 'Add User' dialog box has a title bar 'Add User'. Inside, there is a label 'Username' followed by a text input field. Below the input field are two buttons: 'Add' and 'Cancel'.

**4.3** To fetch a group, click the **Fetch Group...** name. In the **Add Group** dialog box, select the server (authentication module) and the group name, then click **Add**. The external group is added to the list of users and groups. Optionally, before clicking Add, click the **Verify** button to confirm the existence of the specified group.

The 'Add Group' dialog box has a title bar 'Add Group'. Inside, there is a label 'Select group:' followed by a 'Server' dropdown menu showing 'OpenAM'. Below that is a 'Group name' text input field. To the right of the 'Group name' field is a 'Verify' button. At the bottom right are 'Add' and 'Cancel' buttons.

End of Procedure 2-3

### Notes—

- **Restrict Permissions of Admin User**—Be sure to verify the permission granted to the “LDAP Bind DN” (admin) user, especially after migrating users from AAM. For more information, see [How do I restrict the permissions for the LDAP Bind DN \(admin\) user?](#).
- Never delete the embedded datastore, which contains more than users. If the datastore is deleted, there is no way to access Authentication Service.

## Configure Authentication Module (RADIUS Server)

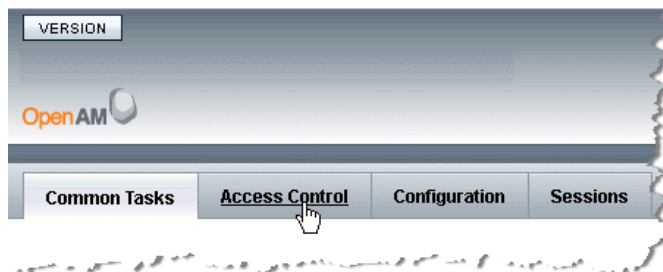
### Procedure 2-4 Configuring Authentication Module (RADIUS Server)

- 1 Log in to OPNET Authentication Service as the administrator:
  - 1.1 From the Start menu, choose Start > All Programs > OPNET Authentication Service> Launch OPNET Authentication Service.  
➡The Login page appears.
  - 1.2 In the Login page, enter the default administrative user name (admin) and the password (opnet).  
➡OPNET Authentication Service appears.
- 2 Click the “Advanced Configuration” option to access OpenAM.

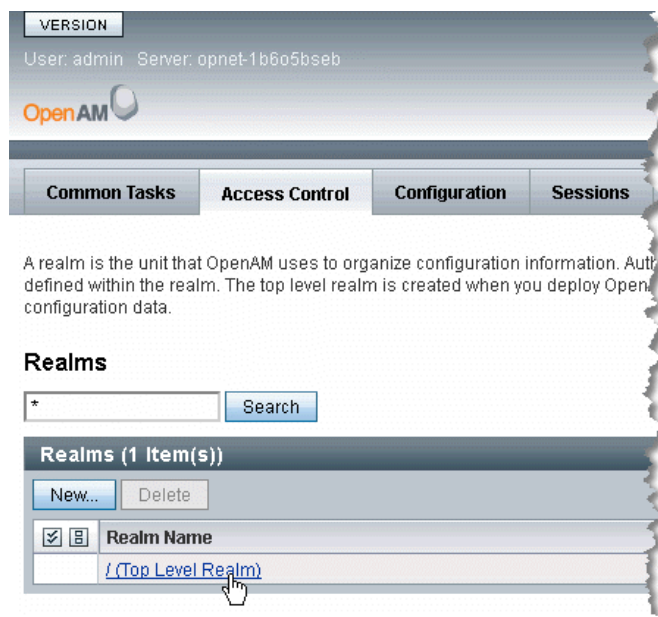
The “Advanced Configuration” option is the gear icon in the upper-right.



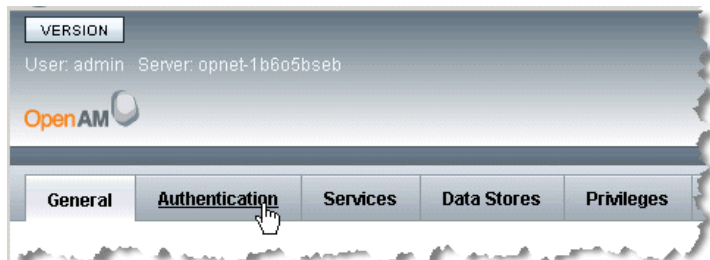
- 3 Configure authentication module:
  - 3.1 Click the “Access Control” tab.



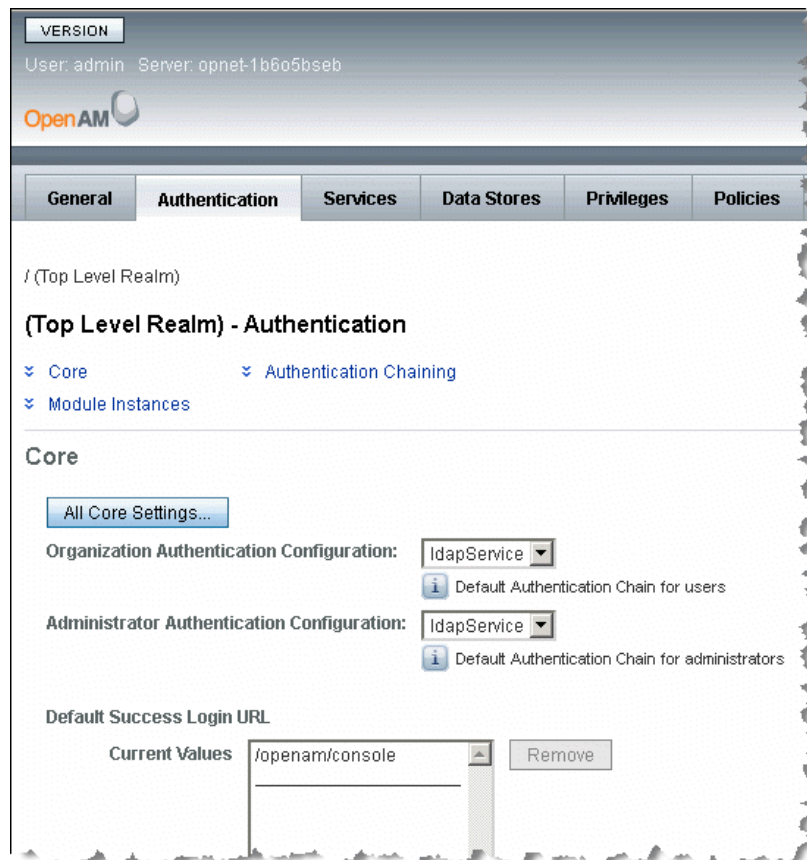
### 3.2 In the Realms table, click the “/(Top Level Realm)” hyperlink.



### 3.3 Click the Authentication tab.

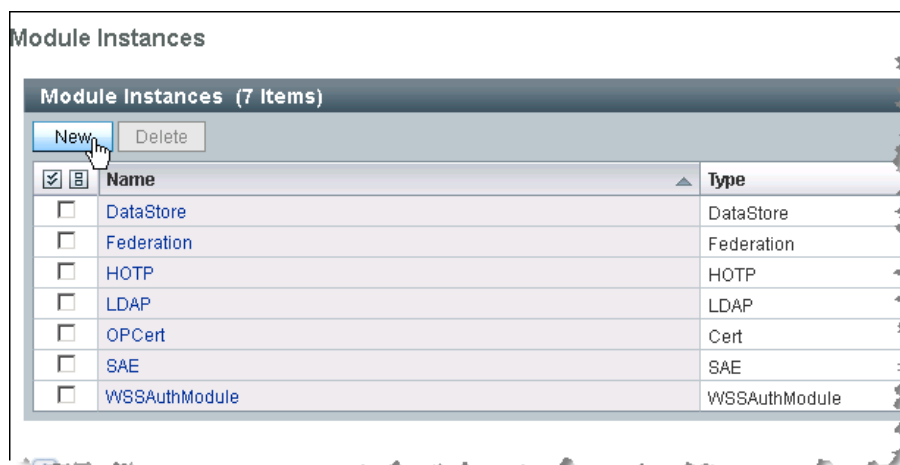


➔The “(Top Level Realm) - Authentication” page appears.



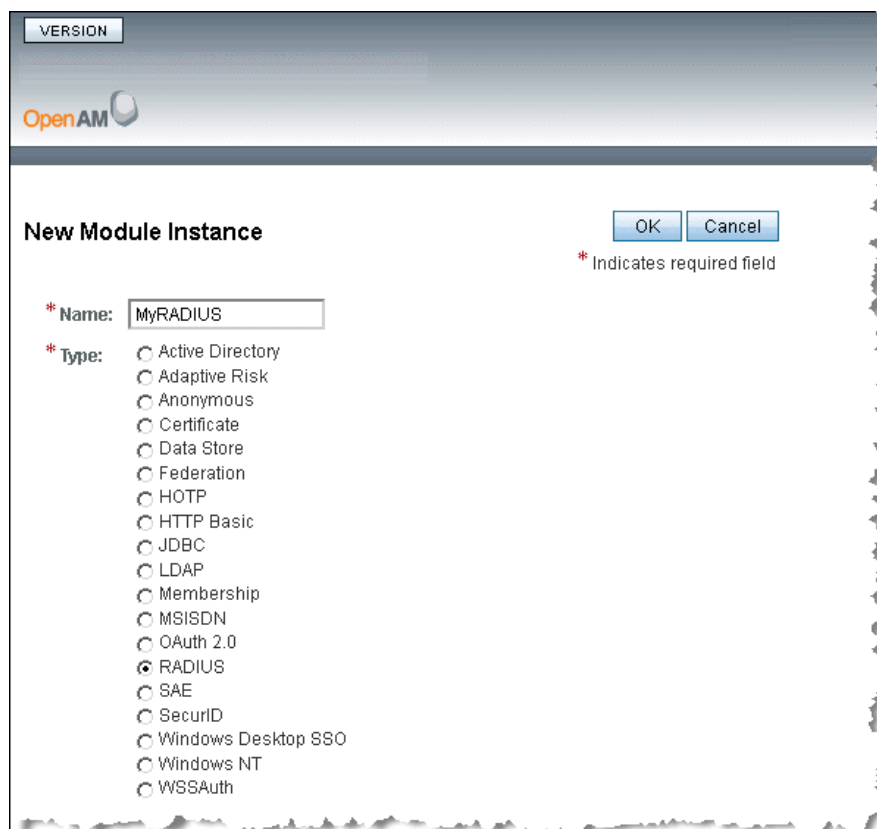


### 3.4 Scroll down to the “Module Instances” table and click New.



### 3.5 In the “New Module Instance” screen, do the following:

- Name—Enter a name for the RADIUS module.
- Type—Select “RADIUS”.



### 3.6 Click the OK button.

➡The “(Top Level Realm) - Authentication” page appears again.

- 3.7** Scroll down to the “Module Instances” table to verify that the RADIUS module was added.

Module Instances

Module Instances (8 Items)		
<input type="button" value="New"/> <input type="button" value="Delete"/>		
<input checked="" type="checkbox"/> <input type="checkbox"/>	Name	Type
<input type="checkbox"/>	DataStore	DataStore
<input type="checkbox"/>	Federation	Federation
<input type="checkbox"/>	HOTP	HOTP
<input type="checkbox"/>	LDAP	LDAP
<input type="checkbox"/>	MyRADIUS	RADIUS
<input type="checkbox"/>	OPCert	Cert
<input type="checkbox"/>	SAE	SAE
<input type="checkbox"/>	WSSAuthModule	WSSAuthModule

**Important**—Depending on your browser, you may have to refresh the page or click on another tab and return to the Authentication tab before the RADIUS module is listed in the “Module Instances” table.

- 3.8** In the “Module Instances” table, click the name of the RADIUS module that you just added.

➡ The Radius configuration screen appears.

**RADIUS**
Save
Reset
Back to Service Configuration

**Realm Attributes**

**Primary Radius Servers**

Current Values

127.0.0.1

Remove

New Value

Add

i A list of primary Radius servers that will be used for authentication

**Secondary Radius Servers**

Current Values

Remove

New Value

Add

i A list of secondary Radius servers that will be used for authentication, in case the primary servers are unavailable.

**Shared Secret:** ●●●●●●  
The secret shared between the RADIUS server and the authentication module.

**Shared Secret (confirm):** ●●●●●●

**Port Number:** 1812  
Port number on which the RADIUS server is listening.

**Timeout:** 3  
i Amount of time in seconds to wait for the RADIUS server response.

**Health check interval:** 5  
i The interval between checks to unavailable RADIUS servers, in minutes.

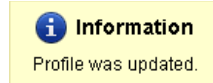
**Authentication Level:** 0

- 3.9** In the RADIUS configuration screen, do the following:

- Primary RADIUS Servers:
  - Remove the default server address
  - Enter the IP address of the RADIUS server
- Secondary RADIUS Servers:
  - Remove the default server address
- Shared Secret / Shared Secret (confirm):
  - Enter the shared secret.
  - (Be sure to enter the same string specified on the RADIUS server.)
- Port Number:
  - Enter the port number on which the RADIUS server is listening.
- Other Fields
  - Enter values in the other fields, as appropriate.

**3.10** Click the Save button.

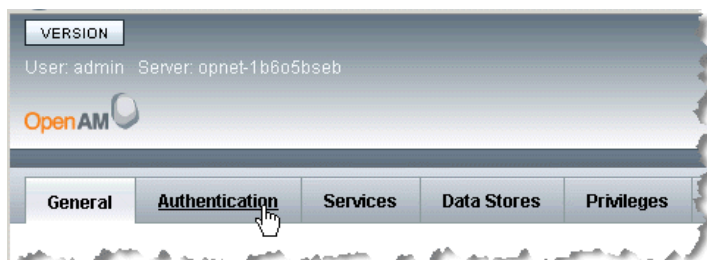
➡ A confirmation message appears at the top of the screen.



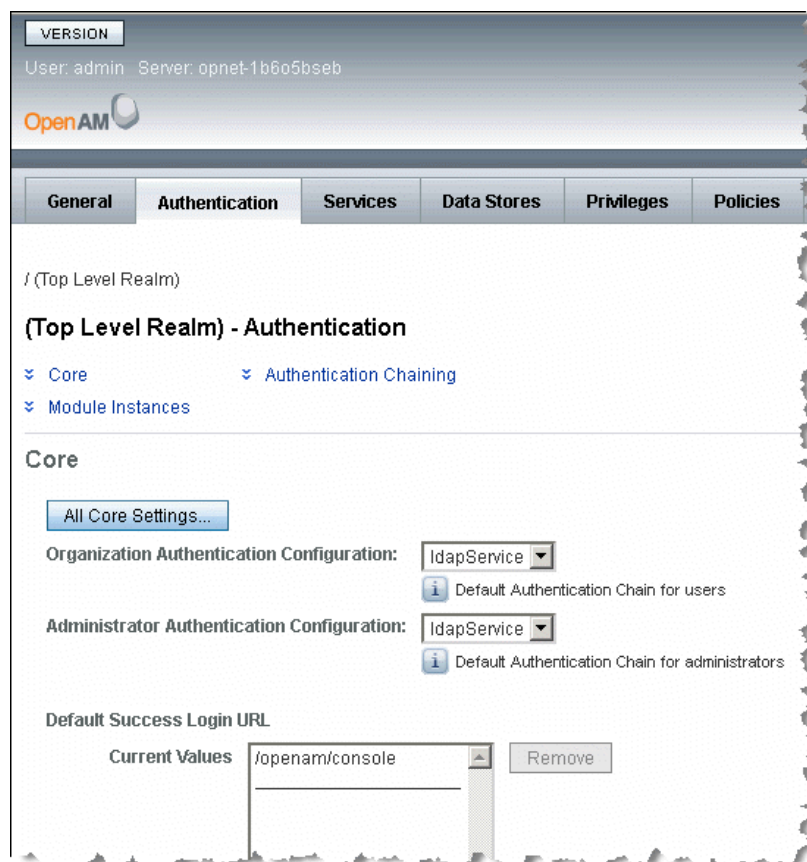
**Important**—Be sure to look for the confirmation message before performing the next step. Users commonly forget to save the configuration information before continuing with the next step.

**3.11** Click the “Back to Authentication” button.**3.12** Click the “Back to Access Control” button.**4** Add the RADIUS module to the existing LDAP authentication chain:**4.1** In the Realms table on the “Access Control” tab, click the “/(Top Level Realm)” hyperlink.

#### 4.2 Click the Authentication tab.

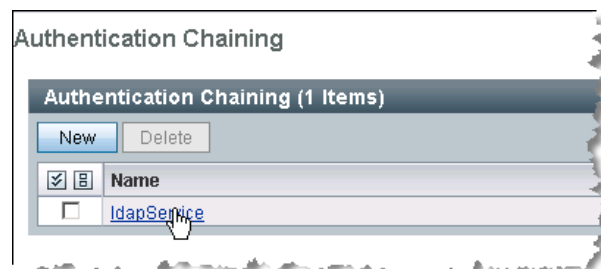


➔The “(Top Level Realm) - Authentication” page appears.



#### 4.3 Scroll down to the “Authentication Chaining” table and click the “IdapService” hyperlink.

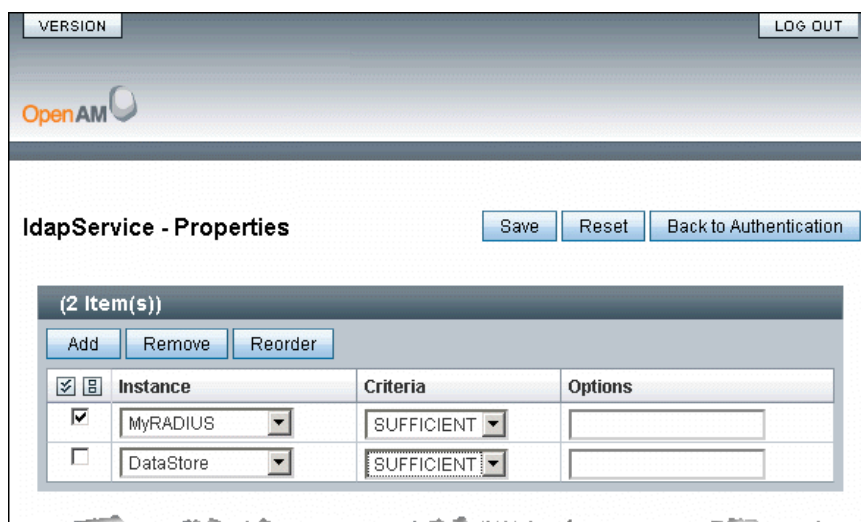
**Important**—*Don’t click New*, which adds a new chain. You want to click the “IdapService” hyperlink and add to the existing chain.



**4.4** In the table under the “IdapService - Properties” heading, click the Add button.



➡ A new line is added to the table.

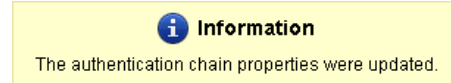


**4.5** For the new line in the table, do the following:

- Instance—From the pull-down menu, select the RADIUS module.
- Criteria—From the pull-down menu select SUFFICIENT.
  - If necessary, update the Criteria fields for other items in the chain.
- If necessary, set the order of the modules in the chain.
  - The primary module should be first.
- Optionally, in the Options field, specify shared state options. See [Best Practice: Enable Shared State with Authentication Modules](#).

**4.6** Click the Save button.

➡ A confirmation message appears at the top of the screen.



**Important**—Be sure to look for the confirmation message before performing the next step. Users commonly forget to save the chaining information before continuing with the next step.

**4.7** Click the “Back to Authentication” button.**4.8** Click the “Back to Access Control” button.

The configuration is complete.

**End of Procedure 2-4****Best Practice: Enable Shared State with Authentication Modules**

Share login credentials between authentication modules to pass the username and password. Sharing credentials provides a smoother login experience.

For example, in the “ldapService - Properties” table shown in [step 4.4](#), consider entering the following options:

- For MyRADIUS use the option  
“iplanet-am-auth-shared-state-enabled=true”
- For DataStore use the option  
“iplanet-am-auth-shared-state-enabled=true  
iplanet-am-auth-shared-state-behavior-pattern=useFirstPass”

For more information, see  
<http://docs.oracle.com/cd/E19575-01/820-3885/gbarg/index.html>.

## Configure Local Users

Perform the following procedure if you plan to use either of the following:

- local users in addition to or instead of external users
- users defined in and fetched from authentication modules

---

### Procedure 2-5 Configuring Local Users

**1** Log in to OPNET Authentication Service as the administrator:

**1.1** From the Start menu, choose Start > All Programs > OPNET Authentication Service > Launch OPNET Authentication Service.

➡ The Login page appears.

**1.2** In the Login page, enter the default administrative user name (admin) and the password (opnet).

➡ OPNET Authentication Service appears.

**2** Define local users:

Click the Users tab, and then:

- Add a User—Click the “Add User” button, specify the requested information, and click Save.
- Edit a User—Select the user from the list, click the “Modify User” button, edit the user in the new browser tab, and click Save. (Close the browser tab to return to the Users tab.)
- Delete a User—Select the user from the list, click the “Delete User” button, then click OK to confirm.

### End of Procedure 2-5

---

Optionally, you can change the administrative user. There is always a local specially-designated administrative user. The default administrator is created during installation with the credentials admin/opnet. To change the administrator, see [How to change the specially-designated administrator](#).



## Step 4: Configure Authorization

The following table lists the default roles created during installation. All roles are automatically assigned to the default Authentication Service administrative user, admin.

**Note**—For security reasons, it is a good idea to change the password of the default administrative user. For more information, see [How to change/reset a user password \(local user only\)](#).

**Table 2-4 Default Roles**

Component	Role Description
<b>OPNET Authentication Service</b>	
	<b>RootAdmin</b> —Provides the ability to administer users in Authentication Service
<b>BrowserMetrix</b>	
	<b>BrowserMetrixAdmin</b> —Provides the ability to configure and view data in BrowserMetrix
	<b>BrowserMetrixView</b> —Provides the ability to view data in BrowserMetrix
<b>Transaction Trace Warehouse</b>	
	<b>TTWAdmin</b> —Provides the ability to view data and configure Transaction Trace Warehouse
	<b>TTWAccess</b> —Provides the ability to view data in Transaction Trace Warehouse

The following procedure describes how to assign roles to users.

---

### Procedure 2-6 Configuring Authorization

- 1 Log in to OPNET Authentication Service as the administrator:
    - 1.1 From the Start menu, choose Start > All Programs > OPNET Authentication Service > Launch OPNET Authentication Service.  
➡The Login page appears.
    - 1.2 In the Login page, enter the default administrative user name (admin) and the password (opnet).  
➡OPNET Authentication Service appears.
  - 2 Assign Roles to Users/Groups:
    - 2.1 On the Roles tab, select the Role Assignment sub-tab.
    - 2.2 In the first column, select the user/group to which you want to assign roles.  
  
To add an external user/group to the list (that is, users/groups that are defined in Active Directory or LDAP), click the “Fetch Group...” or “Fetch User...” button and specify the group/user name.
    - 2.3 Using the buttons between the second and third column, move the roles that you want to assign to the user to the third column.
    - 2.4 Click Save.
- Important**—After the RootAdmin role is assigned to one or more users, you must perform the following tasks before the new administrative users have complete administrative access:
1. Run the sync command. Choose Start > All Programs > OPNET Authentication Service > Sync Admin Users.
  2. When prompted, enter the password for the default administrative user, *admin*. The default password is *opnet*.
  3. When prompted, respond with *Yes* to restart the service. (Note that restarting the service may disrupt users currently logged in and/or in the process of logging in. To restart the service at a later time, respond with *No*.)

End of Procedure 2-6

---

## Certificate Management

If Authentication Service connects to other servers (e.g., LDAP/Active Directory) using secure SSL communication, you must import the public certificates from the other servers into the keystore file on the Authentication Service server.

---

**Note**—HTTPS is the default setting for OPNET Authentication Service.

---

The following procedure describes how to import a public certificate for secure communication between a server and Authentication Service. Before running the procedure, note the following requirements:

- The public certificate must be in PEM format.
- The public certificate must be in a location accessible from the Authentication Service server.
- You need to know the keystore password specified during the installation of Authentication Service.

---

### Procedure 2-7 Importing Certificates

- 1 Open a Command Prompt window.
- 2 Navigate to the following directory:  
`<install_dir>/Authentication Service/Jre/bin.`
- 3 Use the keytool command to import the certificate.

The syntax of the keytool command is as follows:

```
keytool -importcert -trustcacerts -alias <AliasName> -file <PathOfCertificate>
-keystore <Keystorelocation> -storepass <KeystorePassword>
```

where:

`-importcert` = Specifies to import the certificate to the keystore.

`-trustcacerts` = Considers additional certificates included in the chain of trust, namely those certificates in the file named “cacerts.” Use this option for adding self-signed certificates to the keystore.

`-alias <AliasName>` = Specifies a unique, user-defined alias name that you need to access the keystore entries, which are the key and trusted certificates. Although optional, this command field is highly recommended.

`-file <PathOfCertificate>` = User-supplied path of the file to the server certificate that you want to add as the trusted certificate.

`-keystore <Keystorelocation>` = Specifies the name and location of the

persistent keystore file. By default, this file is located at  
C:\OPNET\Authentication Service\Secure\openam-keystore.jks.

`-storepass <KeystorePassword>` = The keystore password. This password was specified during the installation of Authentication Service. Optionally, for security reasons, you can omit this argument from the command. However, if you do omit the password, you will be prompted for the password.

For more information, see the Java documentation or type “keytool” for usage.

- 4 If you omitted the keystore password from the command, you are prompted for the keystore password. (The keystore password was specified during installation of Authentication Service.)

The following information displays:

```
Owner: CN=DEMO, OU=ABC, O=YOURCOMPANY, L=Bethesda, ST=MD, C=US
```

```
Issuer: CN=DEMO, OU=ABC, O=YOURCOMPANY, L=Bethesda, ST=MD, C=US
```

```
Serial number: 4c2a2c5c
```

```
Valid from: Tue Jun 29 13:24:44 EDT 2012 until: Wed Jun 29 13:24:44 EDT 2015
```

```
Certificate fingerprints:
```

```
MD5: A2:D0:84:FA:82:76:36:0B:C9:5D:F2:50:5A:5D:0B:A3
```

```
SHA1: 59:05:11:DF:23:05:A3:90:66:20:92:D2:64:85:01:E5:19:0C:34:D0
```

```
Signature algorithm name: SHA1withRSA
```

```
Version: 3
```

```
Trust this certificate? [no]: yes
```

- 5 Enter “yes” to the question, “Trust this certificate?” (as shown in the line above).

➡ The following confirmation message appears:

```
Certificate was added to keystore.
```

- 6 Restart OPNET Authentication Service:

- 6.1 Choose Start > All Programs > OPNET Authentication Service > Stop Authentication Service.

- 6.2 Choose Start > All Programs > OPNET Authentication Service > Start Authentication Service.

**End of Procedure 2-7**

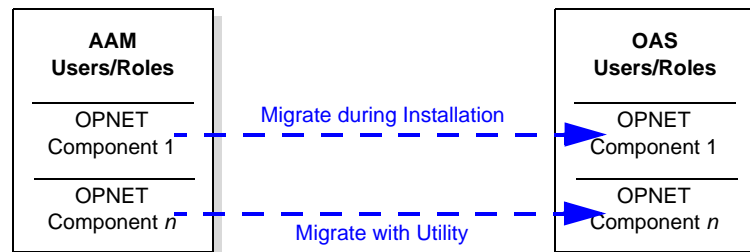
---

### 3 AAM to OAS Migration Utility

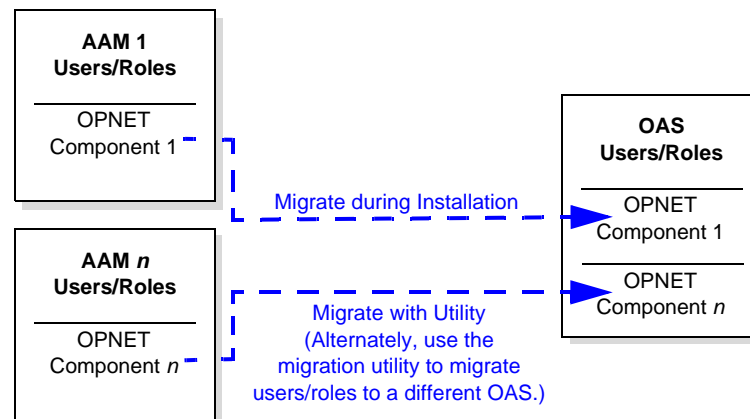
Use the “AAM to OAS Migration” utility to perform a post-installation migration of users and their associated roles from OPNET AAM Server(s) (AAM) to OPNET Authentication Service (OAS).

Run the “AAM to OAS Migration” utility when either of the following is true:

- When users/roles for an upgraded component were not migrated from OPNET AAM Server to OPNET Authentication Service during the installation process



- When there are multiple OPNET AAM Servers from which you want to migrate users/roles to OPNET Authentication Service



**Note**—The “AAM to OAS Migration” utility works whether the OPNET components are installed on the same server or different servers. However, all servers and files must be accessible from the server on which OPNET Authentication Service is installed.

For more information, see the following sections:

- [Requested Information](#)
- [Running the Utility](#)

## Requested Information

The following table lists the information requested by the migration utility. For a smooth migration, review the requested information before running the utility.

**Table 3-1 Information Requested by AAM to OAS Migration Utility**

Field	Description
<b>Source</b>	
AAM Directory	<p>The full path to the OPNET AAM Server installation directory.</p> <p>This field is required.</p> <p>If for some reason the AAM install is not accessible from the OPNET Authentication Service server, see <a href="#">Required AAM Files for Migration</a>.</p>
<b>Target</b>	
OAS Installation Directory	<p>The path to the OPNET Authentication Service install directory.</p> <p>This field is automatically detected.</p>
OAS Directory Manager Password	<p>The “Directory Manager” password. This password is specified during the install of OPNET Authentication Service.</p> <p>This field is required.</p>
Password for OAS User	<p>The local administrator user of OPNET Authentication Service. (The specially-designated administrator user name is shown.)</p> <p>This field is required.</p>

**Table 3-1 Information Requested by AAM to OAS Migration Utility (Continued)**

Field	Description
<b>Optional Fields</b>	
User-Role Mapping File	<p>The full path to the user-role mapping file. The user-role mapping file explicitly specifies the roles assigned to users. This field is optional.</p> <p><b>When to Use the Mapping File</b> Use the mapping file to change a role for a group of users. For example, in AAM, Transaction Trace Warehouse users with administrative privilege are assigned the “admin” role. However, in OAM, Transaction Trace Warehouse users with administrative privilege are assigned the “TTWAdmin” role. To easily make the conversion, you can edit the generated user-role mapping file, changing “admin” to “TTWAdmin”.</p> <p>The user-role mapping file is in XML format and lists the users assigned to each role. When editing the mapping file, be aware that role names are case-sensitive.</p> <p><b>Where to Find the Mapping File</b> The mapping file, DerbyUsers.xml, is created during an upgrade of Transaction Trace Warehouse. During the upgrade, a backup folder is created in the user’s home directory, something like C:\Users\OPNET\AppData\Local\TransactionTraceWarehouse Backup.</p>
Users with the AAM role “admin” will get the OAS role “RootAdmin”	<p>If selected, migrated users with the AAM administrator role are assigned the OPNET Authentication Service administrator (RootAdmin) role.</p> <p>If not selected, no migrated AAM users are assigned the OPNET Authentication Service administrator (RootAdmin) role.</p> <p>By default, this option is not selected.</p>

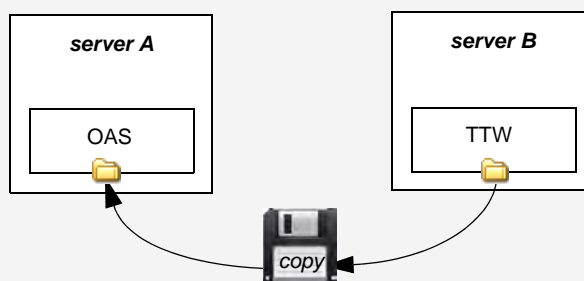
**Required AAM Files for Migration**

If for some reason the AAM install is not accessible from the OPNET Authentication Service server, you can copy the required files from the AAM install to the OPNET Authentication Service server. Then when you perform the migration, you can use the copied files as the AAM source.

- To migrate users/roles from Transaction Trace Warehouse 1.0, copy the following directory:  
`C:\OPNET\AppInternals Xpert Transaction Trace Warehouse 1.0\JBoss\server\op_webapps\deploy\aam.war`
- To migrate users/roles from Transaction Trace Warehouse 2.0, copy the following directory:  
`C:\Program Files\OPNET\AppInternals Xpert Transaction Trace Warehouse 2.0\JBoss\server\op_webapps\deploy\aam.war`
- To migrate users/roles from OPNET Dashboards 1.0, copy the following directory:  
`C:\OPNET\1.0.W\sys\utilities\netcop\webserver\tomcat\webapps\aam`

**Note**—The migration process obtains user and role data from the \*.dtd and \*.res files within the required directories and imports the data into OPNET Authentication Service.

For example, suppose OPNET Authentication Service (OAS) is installed on *server A*, which cannot access *server B*, where Transaction Trace Warehouse (TTW) 1.0 is installed.



In this case, perform the following steps to migrate TTW 1.0 users and roles:

1. On *server B*, navigate to the **aam.war** directory, as specified above.
2. Copy the directory and its contents to *server A*.
3. Run the *AAM to OAS Migration* utility.  
 (Choose Start > All Programs > OPNET Authentication Service > Migrate OPNET AAM.)
4. For the **AAM Directory** field, specify the **aam.war** directory on *server A* (that you just copied from *server B*).
5. Specify the remaining fields described in [Requested Information](#).
6. Click **Migrate Users/Roles**.

The TTW users/roles are migrated to OAS.



## Running the Utility

**Note**—If OPNET AAM Server(s) and OPNET Authentication Service are not installed on the same server, then the OPNET AAM Server(s) files must be accessible from the OPNET Authentication Service server. If for some reason the AAM install is not accessible from the OPNET Authentication Service server, see [Required AAM Files for Migration](#).

### Procedure 3-1 Migrating AAM to OAS (Post-Install)

- 1 Review and gather the [Requested Information](#).
- 2 Login as a user with administrative privileges on the computer where OPNET Authentication Service is installed.
- 3 Choose Start > All Programs > OPNET Authentication Service > Migrate OPNET AAM.

➔The “AAM to OAS Migration Utility” dialog box appears.

- 4 Enter the requested information.
- 5 Click the “Migrate Users/Roles” button.

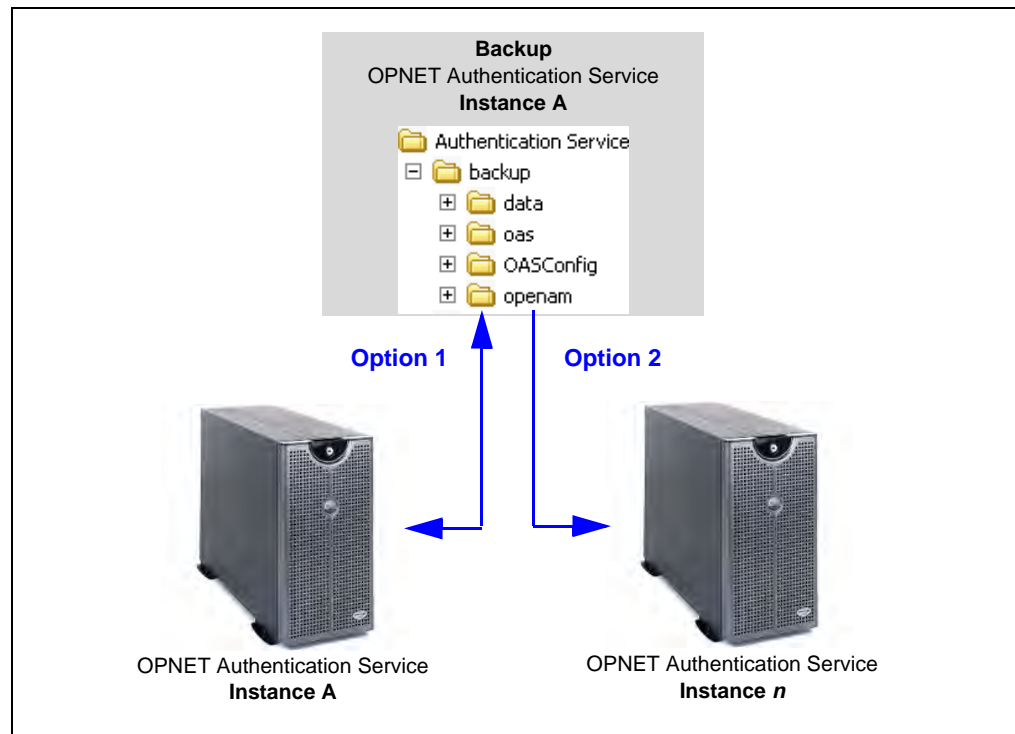
The roles/users are migrated from the AAM Server to OPNET Authentication Service.

### End of Procedure 3-1

## 4 Backups: Create and Restore

Use the “Backup OPNET Authentication Service” utility to perform a backup of an OPNET Authentication Service installation. The backup creates a snapshot of configuration and database files which can be used to:

- **Option 1:** Restore the OPNET Authentication Service installation to the time of the backup
- **Option 2:** Configure another OPNET Authentication Service installation with the same configuration and database



**Important Notes—**

- **Restore with Same Version of OPNET Authentication Service.** For best results, only restore a backup to an OPNET Authentication Service installation with the same version as the OPNET Authentication Service installation used to perform the backup.
- **Backup During Upgrades.** During an upgrade, a backup is performed on the old OPNET Authentication Service installation and restored in the new OPNET Authentication Service. The upgrade process may modify the backup files for version compatibility.
- **Perform this procedure during off-peak time.** The backup utility stops and restarts the Authentication Service service. Until Authentication Service is fully restarted, components that depend on Authentication Service for authentication/authorization will not be accessible. Therefore, to avoid interruptions, it is recommended that you perform this procedure during off-peak time.

For more information, see the following sections:

- [Create a Backup](#)
- [Restore a Backup](#)

## Create a Backup

The backup utility copies important configuration and database files to the following directory on the OPNET Authentication Service server:

C:\OPNET\Authentication Service\backup

Any previously backed up files in the backup directory are overwritten.

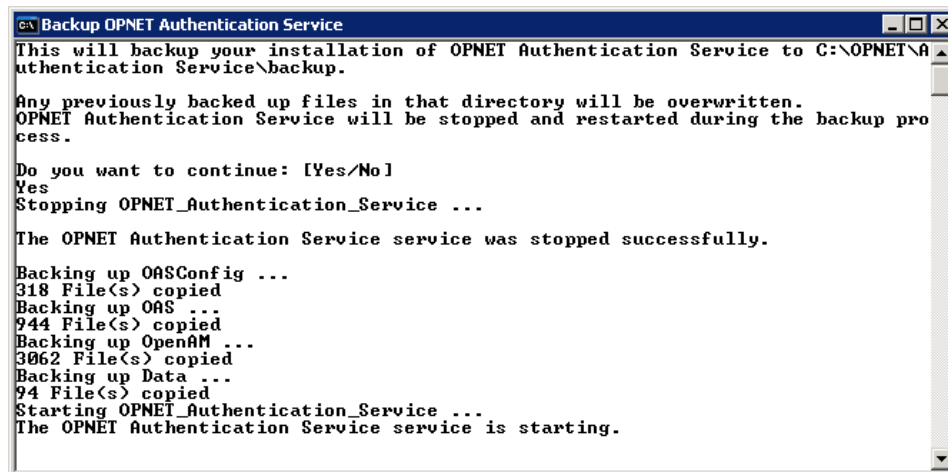
**Hint**—If you want to retain the previous backup, copy the contents of the backup directory to another location or rename the backup directory.

---

### Procedure 4-1 Creating a Backup

- 1 Login as a user with administrative privileges on the computer where OPNET Authentication Service is installed.
- 2 Choose Start > All Programs > OPNET Authentication Service > Backup OPNET Authentication Service.
  - ➔ The “Backup OPNET Authentication Service” window appears.
- 3 Enter “Yes” and press Enter.
  - ➔ The backup is performed.

The following figure shows the information typically displayed during the backup process.



```
Backup OPNET Authentication Service
This will backup your installation of OPNET Authentication Service to C:\OPNET\Authentication Service\backup.
Any previously backed up files in that directory will be overwritten.
OPNET Authentication Service will be stopped and restarted during the backup process.
Do you want to continue: [Yes/No]
Yes
Stopping OPNET_Authentication_Service ...
The OPNET Authentication Service service was stopped successfully.
Backing up OASConfig ...
318 File(s) copied
Backing up OAS ...
944 File(s) copied
Backing up OpenAM ...
3062 File(s) copied
Backing up Data ...
94 File(s) copied
Starting OPNET_Authentication_Service ...
The OPNET Authentication Service service is starting.
```

The window closes when the backup is complete.

### End of Procedure 4-1

---

### Related Topics

- [Backups: Create and Restore](#)

## Restore a Backup

---

### Procedure 4-2 Restoring a Backup

- 1 Stop Authentication Service:
    - 1.1 Choose Start > All Programs > OPNET Authentication Service > Stop Authentication Service.
  - 2 Copy the directories and files from the backup directory as follows:  
(For the first two bullet items, delete or rename the destination directory before copying.)
    - **From:** backup\data  
**To:** <oas\_install\_dir>\Tomcat\data
    - **From:** backup\OASConfig  
**To:** <oas\_install\_dir>\OASConfig
    - **From:** backup\oas\WEB-INF\classes\AMConfig.properties  
**To:** <oas\_install\_dir>\Tomcat\webapps\oas\WEB-INF\classes\AMConfig.properties  
**To:** <oas\_install\_dir>\utils\resources\AMConfig.properties
- Note**—The default <oas\_install\_dir> = "C:\OPNET\Authentication Service".
- 3 If the specially-designated administrator has changed since the backup or if the backup files are being restored on another server with a different specially-designated administrator, you must update the oas.super.user.name setting in the auth.properties files (two instances).
- For more information, see [How to change the specially-designated administrator](#).
- 4 Restart Authentication Service:
    - 4.1 Choose Start > All Programs > OPNET Authentication Service > Start Authentication Service.

---

### End of Procedure 4-2

### Related Topics

- [Backups: Create and Restore](#)

## 5 Useful How-To's and FAQs/Troubleshooting

---

This section describes commonly performed procedures.

### **Authentication Service Configuration**

[How to change the Authentication Service hostname/IP address \(post installation\)](#)

### **Start/Stop Authentication Service**

[How to start/stop Authentication Service](#)

[How to restart OPNET Authentication Service](#)

### **Access Control Management**

[How to change/reset a user password \(local user only\)](#)

[How to view a list of roles assigned to a specific user](#)

[How to view a list of users with a specific assigned role](#)

[How to temporarily revoke access for a specific user](#)

[How to add a role](#)

[How to delete a role](#)

[How to assign a role](#)

[How to change the specially-designated administrator](#)

### **Uninstall Authentication Service**

[How to uninstall Authentication Service](#)

### **Frequently Asked Questions/Troubleshooting**

[What is the purpose of Directory Manager and service-account?](#)

[How do I set and access debug logs?](#)

[What do I do if the “Error: 8dot3 name creation” dialog box appears?](#)

[What should I do if the installer freezes during the installation?](#)

[How do I restrict the permissions for the LDAP Bind DN \(admin\) user?](#)

[What configuration parameters require editing when the Authentication Service hostname changes?](#)

[What configuration parameters should be considered when switching Authentication Service to a production environment?](#)

[After upgrading Authentication Server, why does an error display when I try to login to BrowserMetrix / Transaction Trace Warehouse / OPNET Dashboards?](#)

## Authentication Service Configuration

### How to change the Authentication Service hostname/IP address (post installation)

Changing the hostname/IP address requires two sets of procedures:

- 1) [Configuring OPNET Authentication Service with a new Hostname/IP Address](#)

This procedure is performed on OPNET Authentication Service.

- 2) [Configuring OPNET components with a new OPNET Authentication Service Hostname/IP Address](#)

This procedure is performed on each OPNET component (e.g.: OPNET Authentication Service, BrowserMetrix, Transaction Trace Warehouse, and OPNET Dashboards).

---

#### Procedure 5-1 Configuring OPNET Authentication Service with a new Hostname/IP Address

**Note**—Perform this procedure on OPNET Authentication Service.

- 1 Navigate to the following directory:

```
<install_dir>/Tomcat/webapps/OAS/WEB-INF/classes/
```

- 2 Using a text editor (i.e., Notepad), open each file listed in the following table, edit the specified property setting, and save the file.

Property File	Property Setting
auth.properties	oas.deploy.url <b>Format:</b> oas.deply.url=https://<hostname   IP address>:<port>/oas
public.properties	oas.fqdn <b>Format:</b> oas.fqdn=https=<hostname   IP address>
oas.properties	oas.fqdn <b>Format:</b> oas.fqdn=https=<hostname   IP address>

- 3 Because some files exist in multiple locations, copy the updated auth.properties and public.properties files to <install\_dir>/utils/resources.
- 4 Restart the component (using the stop and start shortcut options on the Start menu).

#### End of Procedure 5-1

---

---

### Procedure 5-2 Configuring OPNET components with a new OPNET Authentication Service Hostname/IP Address

**Note**—Perform this procedure on each OPNET component (e.g.: OPNET Authentication Service, BrowserMetrix, Transaction Trace Warehouse, OPNET Dashboards).

- 1 Search for the authconfig.properties file within the installed component directory.
  - 2 Open the authconfig.properties file with a text editor (i.e., Notepad).
  - 3 Edit the following property settings:
    - `auth.host=<hostname>`  
where: `<hostname>` is the hostname
    - `auth.port=<port>`  
where: `<port>` is the communication port
    - `auth.secure=[true|false]`  
where: `true` indicates HTTPS; `false` indicates HTTP
  - 4 Optionally, edit the following property settings:
    - `app.ignorecerthostname=true`  
Specifies whether to accept certificates if hostnames are mismatched between the specified hostname and the hostname used to connect.  
The default is `true`.
    - `app.acceptallcerts=true`  
Specifies whether to accept self-signed certificates during HTTPS communication.  
The default is `true`.
- Important**—Be sure to examine these property settings when switching Authentication Service to production environment. Typically, you want stricter security for production.
- 5 Save and close the properties file.
  - 6 Restart the component (using the stop and start shortcut options on the Start menu).

### End of Procedure 5-2

---



## **Start/Stop Authentication Service**

### **How to start/stop Authentication Service**

To start/stop Authentication Service, use the Start menu shortcuts:

- **Start:**  
Choose Start > All Programs > OPNET Authentication Service > Start Authentication Service.
- **Stop:**  
Choose Start > All Programs > OPNET Authentication Service > Stop Authentication Service.

### **How to restart OPNET Authentication Service**

---

#### **Procedure 5-3 How to restart OPNET Authentication Service**

- 1 Choose Start > Control Panel > Administrative Tools > Services.
- 2 Right-click on "OPNET Authentication Service" and select Restart.

**End of Procedure 5-3**

---

## Access Control Management

### How to change/reset a user password (local user only)

---

#### Procedure 5-4 How to change/reset another user's password (local user only)

- 1 Login to Authentication Service (as a user with administrative privilege (RootAdmin role)).
- 2 Click Users tab.
- 3 Select the user from the list.
- 4 Click the "Modify User" button.
  - ➡The "Edit User" screen appears in a new browser tab.
- 5 Do one of the following:
  - To change the password, find the Password field and click Edit. Enter the old and new passwords and click OK. (Use this option to change the default administrator (admin) password.)
  - To reset the password so that the user must change the password after the next login, find the "Password Reset Options" field and click Edit. Select the "Force Change Password on Next Login" checkbox and click Save. (Use this option for non-administrative users.)

#### End of Procedure 5-4

---

**Procedure 5-5 How to change your password (local user only)**

- 1 Login to Authentication Service (as a user without administrative privilege (RootAdmin role)).

➡ Your user screen appears.

**John Smith** Save Reset

\* Indicates required field

First Name: John

\* Last Name: Smith

\* Full Name: John Smith

Password: [Edit](#)

Email Address:

Telephone Number:

Home Address:

Password Reset Options: [Edit](#)

Universal ID: id=jsmith,ou=user,dc=opnet,dc=com

- 2 Next to the Password field, click Edit.

➡ Your change password screen appears.

**Change Password for John Smith** OK Reset Close

\* Indicates required field

Type in your old password.

\* Old Password:

Type in the new password, then re-enter it.

\* New Password:

\* Re-Enter Password:

- 3 In the “New Password” and “Re-Enter Password” fields, enter your new password.
- 4 Click OK.

➡ Your new password is saved.

Enter your new password the next time you login.

**End of Procedure 5-5**

## **How to view a list of roles assigned to a specific user**

---

### **Procedure 5-6 How to view a list of roles assigned to a specific user**

- 1** Login to Authentication Service.
- 2** Click the Roles tab and the Role Assignment sub-tab.
- 3** In the first column, select the user.
- 4** Note the list of assigned roles (on the far right).

### **End of Procedure 5-6**

---

---

**How to view a list of users with a specific assigned role**

---

**Procedure 5-7 How to view a list of users with a specific assigned role**

- 1 Login to Authentication Service.
- 2 Click the Roles tab and the Role Management sub-tab.
- 3 From the list, select the role and click “Modify Role”.
  - ➡The Modify Role dialog box appears.

Modify Role

Role Name: BrowserMatrixAdmin

Role Description: Ability to view data and configure Browsi

Identifier	Description
<input type="checkbox"/>	admin

Add Member Remove

Save Cancel

- 4 In the Modify Role dialog box, note the list of users assigned to the selected role.

**End of Procedure 5-7**

---

### **How to temporarily revoke access for a specific user**

The following procedure is useful if you want to revoke access for a user without deleting the user.

---

#### **Procedure 5-8 How to temporarily revoke access for a specific user**

- 1** Login to Authentication Service.
- 2** Click the Users tab.
- 3** Select the user from the list of users.
- 4** Click the “Modify User” button.
  - ➡ The Edit User screen appears in a new browser tab.
- 5** In the “Edit User” screen, change the User Status from Active to Inactive.
- 6** Click Save.
- 7** Close the browser tab to return to the Users tab.

#### **End of Procedure 5-8**

---

## How to add a role

Use the following procedure to add a role. Adding a role is necessary if you want to assign roles to users for another component that already has defined roles. (When installed, BrowserMetrix and Transaction Trace Warehouse add default roles to Authentication Service. For a list of the default roles, see [Table 2-4 Default Roles.](#))

### Procedure 5-9 How to add a role

- 1 Login to Authentication Service.
- 2 Click the Roles tab and the Role Assignment sub-tab.

- 3 Click the “Add Role” button.
- ➡The “Add New Role” dialog box appears.

4 In the “Add New Role” dialog box, enter the following information:

- Role Name—A unique name to identify the role (required). The name cannot be changed after it is saved.

**Note**—Enter letters, numbers, spaces, and underscores only. No special characters.

- Role Description—Descriptive text to identify the role, up to 255 characters. (optional).

5 Click Save.

➡The new role appears in the list of available roles (2nd column).

**Next Step**—In other applications, assign permissions to the role.

#### End of Procedure 5-9

---

### How to delete a role

---

#### Procedure 5-10 How to delete a role

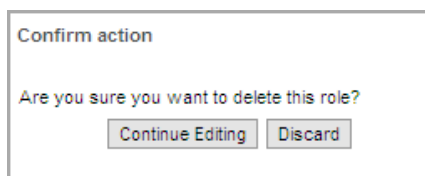
1 Login to Authentication Service.

2 Click the Roles tab and the Role Management sub-tab.

3 Select the role that you want to delete from the list of roles.

4 Click “Delete Role”.

➡The “Confirm Action” dialog box appears.



5 Click “Discard” to delete the role.

➡The selected role is deleted.

#### End of Procedure 5-10

---



## How to assign a role

### Procedure 5-11 How to assign a role

- 1 Login to Authentication Service.
- 2 Click the Roles tab and the Role Assignment sub-tab.

**Roles**

Role Assignment | Role Management

**Users and Groups**

Identifier	Description
admin	

Fetch Group... Fetch User...

**Roles**

**Available Roles**

Role Name	Role Description
BrowserMetri...	Ability to view data and configure BrowserMatrix
BrowserMetri...	Ability to view data in BrowserMatrix
guest	Guest Role
RootAdmin	Root Administrator
TTWAccess	Ability to view data in Transaction Trace Warehouse
TTWAdmin	Ability to view data and configure Transaction Trace Warehouse

Add Role...

**Assigned Roles**

Role Name	Role Description
-----------	------------------

>> > < <<

Save Cancel

- 3 In the first column, select the user/group to which you want to assign roles.
- 4 Using the buttons between the second and third column, move the roles that you want to assign to the user to the third column.
- 5 Click Save.

### End of Procedure 5-11

## How to change the specially-designated administrator

To ensure that there is always at least one user with full administrative privileges (e.g., the RootAdmin role), one of the administrative users is specially designated and cannot be disabled or deleted. By default, the specially designated administrative user is the “admin” user created during installation. The following procedure describes how to change the specially designated administrative user.

### Important Notes—

- **Be sure to remember the specially-designated administrative user.** The username and password of the specially-designated administrative user is required to perform upgrade and maintenance operations.
- **Perform this procedure during off-peak time.** This procedure requires a component restart. During the restart, Authentication Service will be shut down. Until Authentication Service is fully restarted, components that depend on Authentication Service for authentication/authorization will not be accessible. Therefore, to avoid interruptions, it is recommended that you perform this procedure during off-peak time.

---

### Procedure 5-12 How to change the specially-designated administrator

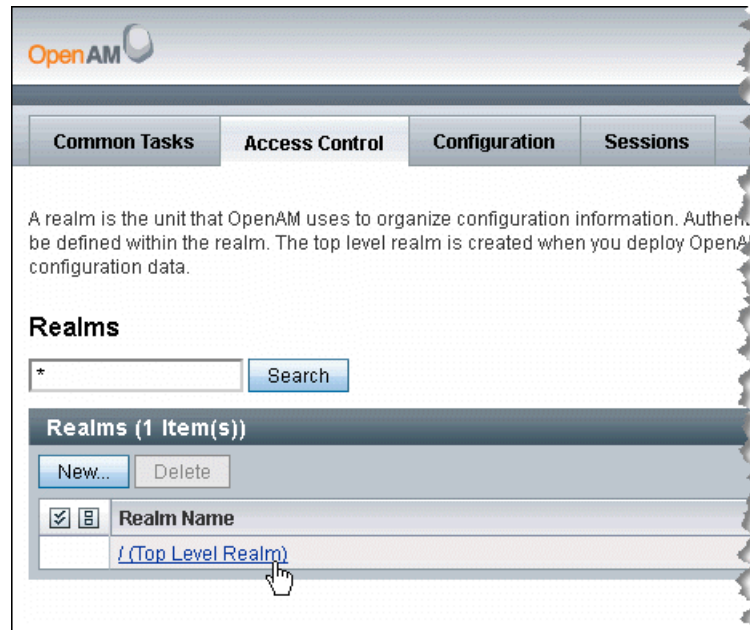
- 1 Identify the **Universal ID** of the administrator that you want to specially designate:
  - 1.1 Login to OPNET Authentication Service as administrator (with the RootAdmin role).
  - 1.2 Click the “Advanced Authentication Configuration” in the upper-right of the page to access OpenAM.



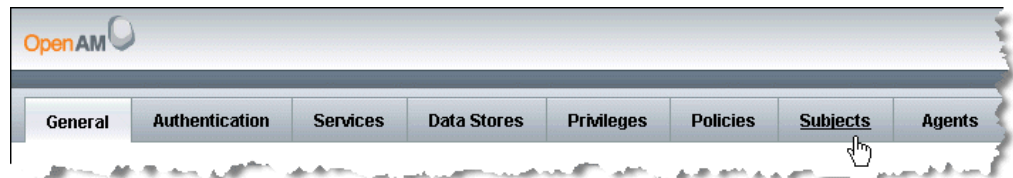
- 1.3 Click the “Access Control” tab.



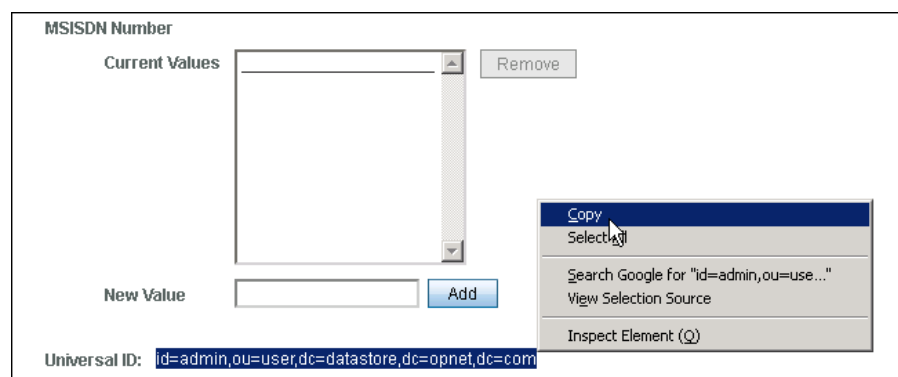
- 1.4 In the Realms table, click the “/(Top Level Realm)” hyperlink.



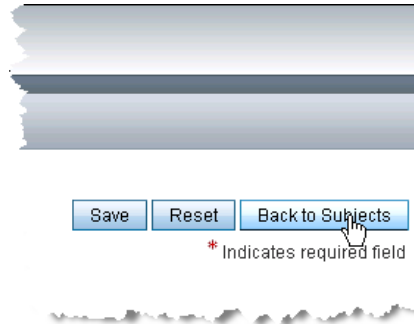
- 1.5 Click the “Subjects” tab.



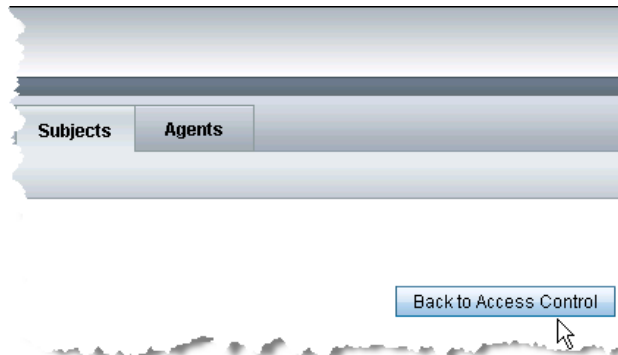
- 1.6 In the User table, click the user that you want to make the specially-designated administrator.
- 1.7 In the “Edit User - <user>” page, scroll down to the bottom to view the **Universal ID**.
- 1.8 Select and copy the **Universal ID** value.



- 1.9 Scroll up to the top of the page and click the “Back to Subjects” button.



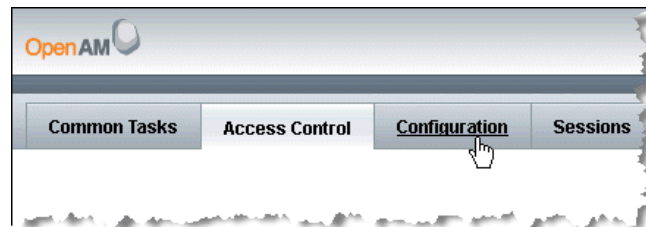
- 1.10 Click the “Back to Access Control” button.



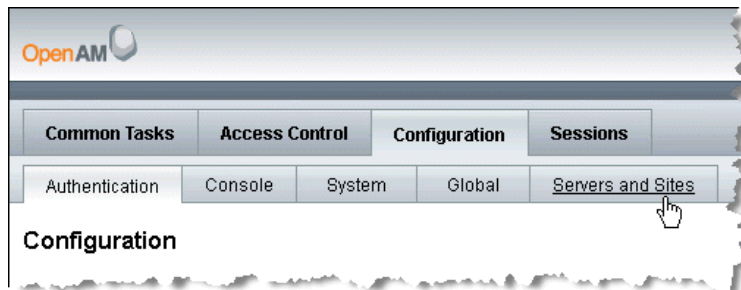
➡The “Access Control” tab appears.

- 2 Update the designated administrator’s configuration property with the Universal ID:

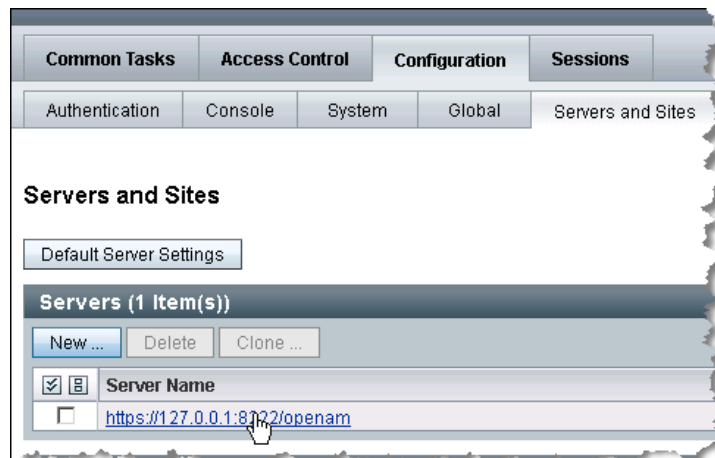
- 2.1 On the “Access Control” tab, click the Configuration tab.



- 2.2 Click the “Servers and Sites” tab.



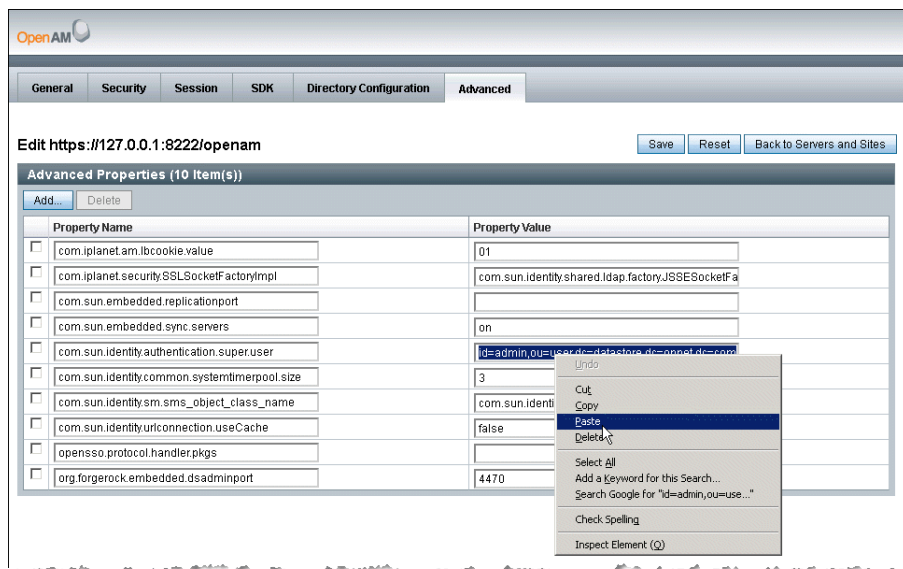
- 2.3 In the Servers table, click the hyperlink for the server starting with “https://172.0.0.1”



- 2.4 Click the Advanced tab.



- 2.5 In the property value field for `com.sun.identity.authentication.super.user`, select the existing value and paste the **Universal Id** that you copied in [step 1.8](#).



- 2.6 Click the Save button.

- 3 Update the auth.properties files with the username of the specially-designated administrator.

**Important**—Because there are two identical copies of the auth.properties file in the installation, the following sub-steps describe how to edit one instance of the file and then copy the file to replace the second instance of the file.

- 3.1 Open Windows Explorer.

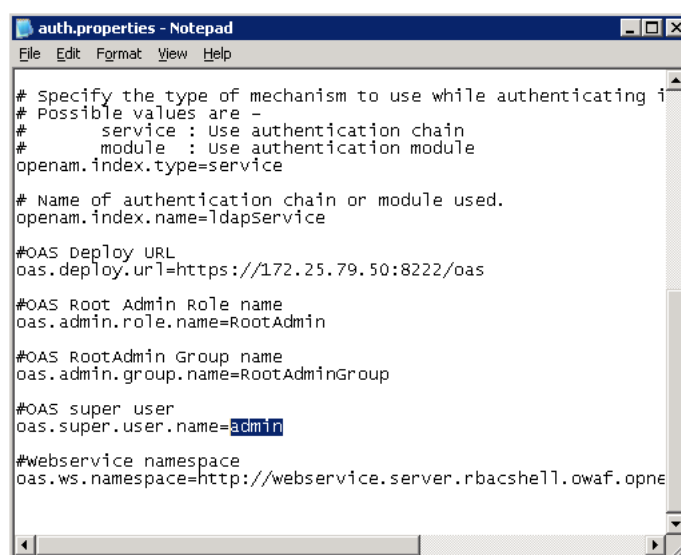
- 3.2 Navigate to <oas\_install\_dir>\Tomcat\webapps\oas\WEB-INF\classes.

For example:

C:\OPNET\Authentication Service\Tomcat\webapps\oas\WEB-INF\classes

- 3.3 Open the auth.properties file with a text editor, such as Notepad.

- 3.4 For the oas.super.user.name property, specify the name of the user that you want to make the specially-designated administrator.



- 3.5 Save and close the properties file.

- 3.6 Copy the updated auth.properties file to <oas\_install\_dir>\utils\resources.

For example:

C:\OPNET\Authentication Service\utils\resources

When prompted whether you want to replace the existing file, click Yes.

- 4 Restart OPNET Authentication Service:

- 4.1 Choose Start > All Programs > OPNET Authentication Service > Stop Authentication Service.

Wait for Authentication Service to stop.

- 4.2** Choose Start > All Programs > OPNET Authentication Service > Start Authentication Service.

Wait for Authentication Service to start.

**End of Procedure 5-12**

---

## Uninstall Authentication Service

### How to uninstall Authentication Service

---

**WARNING**—The following procedure will remove all configuration settings.

---

---

#### Procedure 5-13 How to uninstall Authentication Service

- 1 Choose Start > Control Panel > Add or Remove Programs.
- 2 From the “Add or Remove Programs” dialog box, select “OPNET Authentication Service 1.1” and click the Change/Remove button.

Wait for the uninstall to complete.

#### End of Procedure 5-13

---

For additional information, see the “Uninstall” section in the BrowserMetrix installation instructions.

## Frequently Asked Questions/Troubleshooting

### What is the purpose of Directory Manager and service-account?

*Directory Manager*, and *service-account* are service accounts/groups that are used by the Authentication Service software. When configuring the software, it is important not to change or delete these accounts/groups. Altering these accounts/groups will cause the Authentication Service software to fail.



### How do I set and access debug logs?

**Important**—After reproducing the problem, be sure to reset the logging. Otherwise, the logs could grow excessively large and fill up the disk.

---

#### Procedure 5-14 Setting Log Levels

- 1 Login to OPNET Authentication Service as administrator (with the RootAdmin role).
- 2 Click the “Advanced Authentication Configuration” in the upper-right of the page to access OpenAM.



### 3 Access Debug.jsp by updating the URL in the address bar.

For example: `http://172.25.98.23:8111/openam/Debug.jsp`.

➡ The debug logging page displays.

Category	Description
CoreSystem	Core infrastructure services, PLL, cookies, naming, logging, upgrade amComm amLogging amSecurity amMonitoring amTagLib amUtil amRequestUtils amThreadManager amNaming amXMLHandler amLog amIdentityServices amUpgrade amHa amCookieUtils amFileLookup amJAXRPC amResourceLookup PossibleLocales SystemTimerPool amJSSE amXML bundleName amMultinstall PLLClient amJSS amGateway SystemTimer LDAPConnectionPool
Policy	Policy Framework, Subject, Condition, Resource Attributes, XACML, Plugins, API amRemotePolicy amEvaluatePolicyServlet amPolicy
Session	Session framework, session management, SSO Token, session failover, API amSession amSSOProvider amSessionUtils amSessionEncodeURL
Federation	Federated SSO, protocols (SAML 1.1, ID-FF, WS-Federation, SAML2), Metadata, Hub, Circle of Trust libMultipleProtocol libSAML2Meta libXACML fmDataStoreProvider libWSFederation libPlugins libDataStoreProvider libCOT fmCOT libSAML fmConfiguration libSAML2 libIDPDiscovery libIDFF libEncryption
Configuration	Service Configuration, Delegation, SMS Schema, SMS repository, plugins amConsole amSMSLdap amSMS amSMSEmbeddedLdap amDelegation amSMSCient amSMSFlatFiles workflow amClientSchema amConfigurator amCLI amSetupServlet amEventService amSMSServerImpl amSMSEvent
IdRepo	Identity Repositories, Datastores, plugins. amIdm amIdRepoFiles amProfile amProfileListener amIdRepoDatabase amIdmJAXRPCServer LDAPv3Repo amProfile_Server amSpecialRepo amAgentsRepo amProfile_ldap amSdkRepo amIdmClient amSDK amRemoteEntity idrepoListener LDAPv3EventService amProfile_Client
Authentication	Authentication service, framework, Auth modules, Callbacks, JAAS, API amPassword fmAuthFederation amLoginModule amAuthSecurID amAuthMSISDN amAuthHOTP amAuthAD SAE amAuthCert amAuthXMLUtils amAuthLDAP amClientDetection amAuthContextLocal amAuthDataStore amLogoutViewBean amAuthInternal amAuthRadius amAuthUtils amAdmin amAuthInternalLDAPModule amCallback amAuthInternalSMModule amAuthApplication amAuthContext amLoginViewBean customModule amAuthMembership ReplayPasswd amAuthConfig amJAAS amAuthHTTPBasic amLoginServlet amAuthExceptionHandler amAuthAccountLogout amAuth amLoginLogoutMapping amCDC amAuthClientUtils amAMAuthUtils amAuthWindowsDesktopSSO amAuthAdaptive amPasswordReset amAuthAnonymous AuthAgents amAuthNT amAuthJDBC
WebServices	Web services security (WSS), STS, Identity Services FAMSTSAuthorizationProvider WebServicesSecurity fmWebServicesClients libIDWSF

### 4 Select the service to debug and level.

#### End of Procedure 5-14

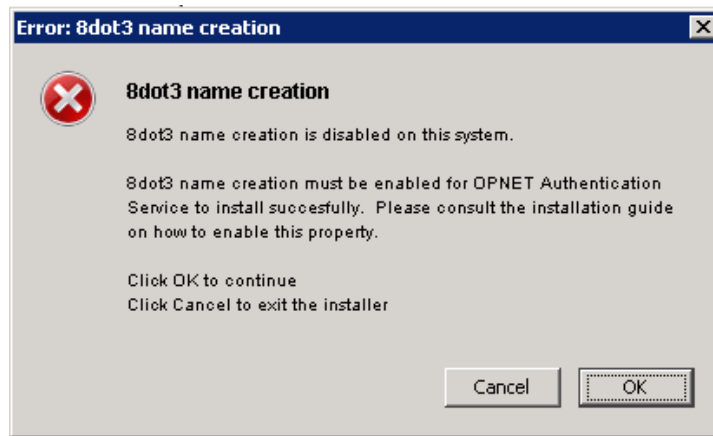
For additional information about debug logs, see Chapter 13 of the OpenAM 10.0.0 Administration Guide.

To access the debug logs, in Windows Explorer, navigate to the following directory:

`<install_directory>\Authentication Service\OASConfig\openam\log`

Additional logs are located in the following directory:

`<install_directory>\Authentication Service\Tomcat\logs`

**What do I do if the “Error: 8dot3 name creation” dialog box appears?**

This error indicates that the installer detects that the 8dot3 Windows property is not enabled, which can cause issues during installation.

To verify and set the Windows property, click the Cancel button and follow [step 4](#) in [Procedure 2-1 Installing OPNET Authentication Service](#).

If the error dialog box appears even after you have set and verified the 8dot3 Windows property, click the OK button to continue with the installation.

**What should I do if the installer freezes during the installation?**

One reason the installer can freeze during installation is because the 8dot3 Windows property is not enabled. See [step 4](#) in [Procedure 2-1 Installing OPNET Authentication Service](#).

Perform the following procedure to safely exit the installer.

**Procedure 5-15 Exiting the Installer that has Frozen**

- 1 Open Task Manager.
- 2 Click the Process tab.
- 3 Look for the following Java process:

```
java.exe *32    opnet    00    "C:\OPNET\Authentication Service\jre\bin\java.
```

The java used will always be from the OPNET Authentication Service install directory and its first parameter will always be the trustStore.

- 4 End that process. (This will free the installer from the hang and continue.)
- 5 The installer will finish but throw errors about validation.

The installer will exit and prevent any of the component installers from executing.

6 Run the OPNET Authentication Service uninstaller to clean the failed installation:

6.1 Choose Start > All Programs OPNET Authentication Service > Uninstall Authentication Service.

7 Check the Disable8dot3 property and then run the installer again.

Contact Technical Support if the installer freezes again.

#### End of Procedure 5-15

---

#### How do I restrict the permissions for the LDAP Bind DN (admin) user?

When defining the LDAP Bind DN, be sure to specify a user with only read privilege. If the user has privileges other than read, then the user can perform those operations (e.g., delete users) from OPNET Authentication Service or OpenAM.

Perform the following procedure to restrict the LDAP Bind DN user. This procedure is especially helpful after migrating admin users from AAM to OPNET Authentication Service.

---

#### Procedure 5-16 Restricting the Permission for the LDAP Bind DN User

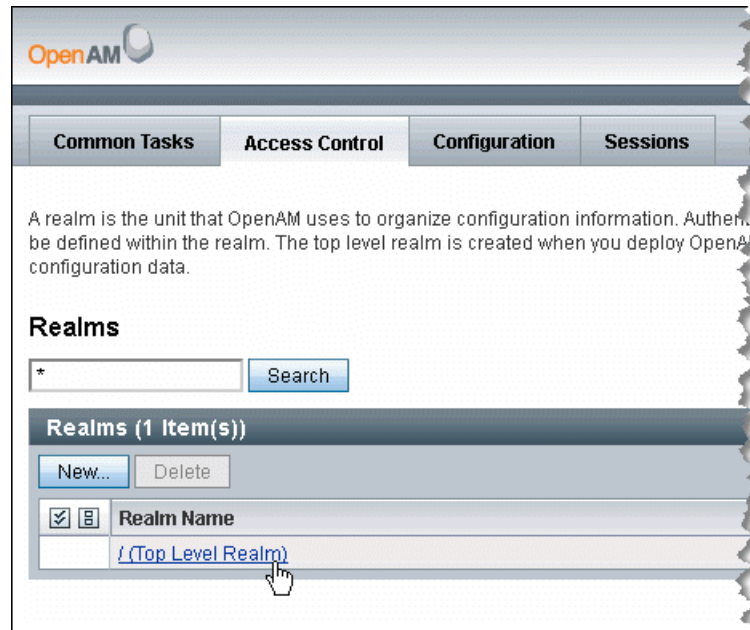
- 1 Login to OPNET Authentication Service as administrator (with the RootAdmin role).
- 2 Click the “Advanced Authentication Configuration” in the upper-right of the page to access OpenAM.



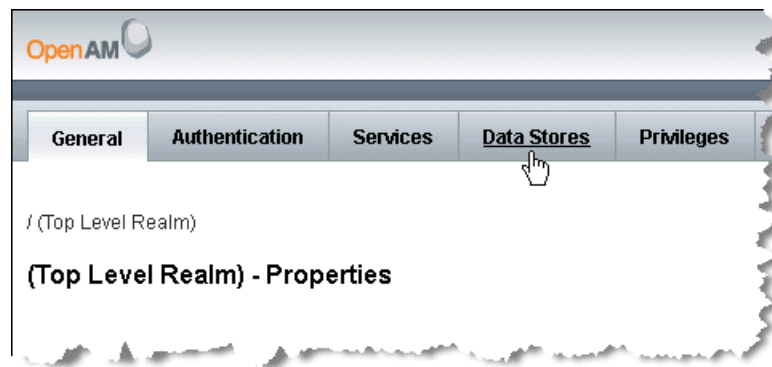
- 3 Click the “Access Control” tab.



- 4 In the Realms table, click the “/(Top Level Realm)” hyperlink.



- 5 Click the “Data Stores” tab.



- 6 In the Data Stores table, click the name given to the Active Directory module in AAM.

**Note**—If you had more than one module in AAM, then you may need to repeat the following steps for each module.

- 7 Scroll down to the section titled “Plug-in Configuration” and find the “LDAPv3 Plug-in Supported Types and Operations” field.

**Plug-in Configuration**

\* LDAPv3 Repository Plug-in Class Name:

**Attribute Name Mapping**

Current Values

New Value

**LDAPv3 Plug-in Supported Types and Operations**

Current Values

New Value

- 8 In the “Current Values” field:

- 8.1 Select the `user=read,create,edit,delete,service` entry and click the Remove button.
- 8.2 Select the `group=read,create,edit,delete` entry and click the Remove button.

- 9 In the “New Value” field (below the “Current Values” field):

- 9.1 Enter `user=read` and click the Add button.
- 9.2 Enter `group=read` and click the Add button.

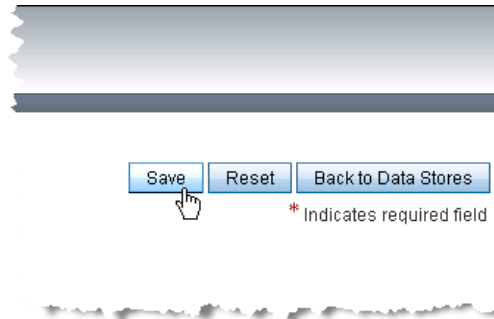
➡The “Current Values” field should look as follows:

**LDAPv3 Plug-in Supported Types and Operations**

Current Values

New Value

- 10 Scroll to the top of the page and click the Save button.



- 11 To repeat the procedure with another data store module, click the “Back to Data Stores” button and select another data store from the “Data Stores” table.

#### End of Procedure 5-16

#### What configuration parameters require editing when the Authentication Service hostname changes?

For each component (Authentication Service, BrowserMetrix, Transaction Trace Warehouse, OPNET Dashboards), be sure to edit the hostname, port, and security settings in the authconfig.properties file.

For more information, see [How to change the Authentication Service hostname/IP address \(post installation\)](#).

#### What configuration parameters should be considered when switching Authentication Service to a production environment?

Typically, when switching to a production environment, you want to enforce stricter security. Therefore, for each component (Authentication Service, BrowserMetrix, Transaction Trace Warehouse, OPNET Dashboards), be sure to edit the certificate properties described in [step 4 of How to change the Authentication Service hostname/IP address \(post installation\)](#).

#### After upgrading Authentication Server, why does an error display when I try to login to BrowserMetrix / Transaction Trace Warehouse / OPNET Dashboards?

After an upgrade to Authentication Service, you must import the new security certificate into all components that access Authentication Service for authentication/authorization. For more information, see [Upgrade Authentication Service](#).

## App A Active Directory: A Brief Introduction

---

This chapter provides a non-technical high-level overview of Active Directory. The purpose is to acquaint you with the basics so that you can more easily configure OPNET Authentication Service with Active Directory. Understanding the basics can help you to identify and request required information for configuration and to troubleshoot issues.

This chapter includes the following sections:

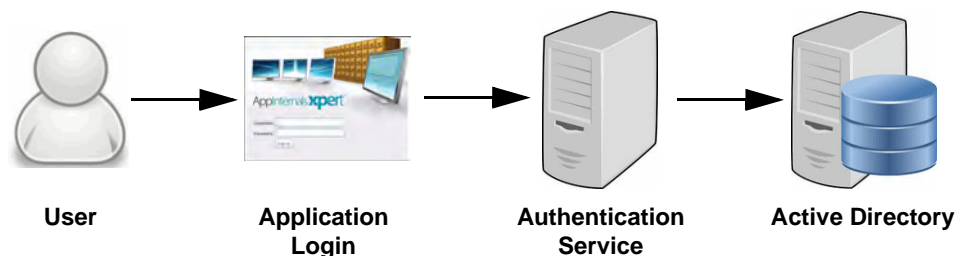
- [Active Directory: The Basics](#)
  - [About Objects](#)
  - [About the Hierarchy of Objects](#)
  - [About Organization Unit](#)
- [Active Directory: Browsing Utilities](#)
- [Active Directory: Glossary](#)

For a more technical understanding of Active Directory, consult the numerous books and online resources.

### Active Directory: The Basics

Active Directory contains a structured object-oriented hierarchical database that stores objects and attributes. This database is accessible using the LDAP protocol. It can be used to authenticate users and computer devices. For example, when a user logs into a computer that is part of an Active Directory domain, Active Directory verifies the password and determines whether the user is in an Administrator group.

The following figure shows that when a user logs in to an application, the user's credentials are sent to Authentication Service, which accesses Active Directory to authenticate and authorize the user.





## About Objects

The Active Directory database is structured in a hierarchical arrangement of information about objects. Generally, there are two categories of objects:

- resources (e.g., printers or networked hardware resources)
- security principals (e.g., users, computer accounts, groups)

Each object, uniquely identified by its distinguished name (DN), represents a single entity (e.g., a user, a computer, a printer, or a group) and its attributes. Certain objects can contain other objects.

Especially for security principals, there are three common ways to identify objects:

- DN (Distinguished Name)
- CN (Common Name), which is typically the last part of the DN
- sAMAccountName, which uses only letters, numbers and underscores (Note that if an object includes special characters other than the underscore, then use CN instead of sAMAccountName.)

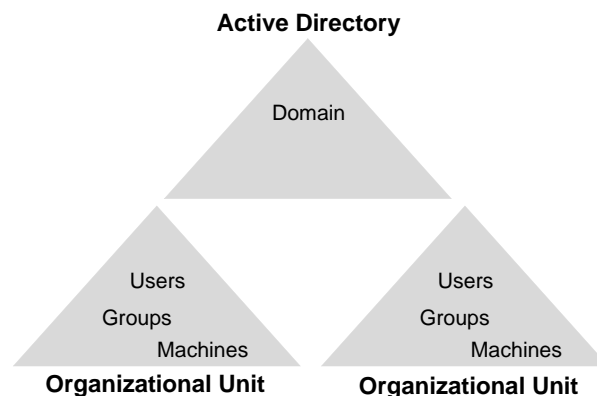
For more information, see [Active Directory: Requirements For Creating Objects](#).

## About the Hierarchy of Objects

The Active Directory database is organized hierarchically. For example:

- *Domains*  
(identified by the DNS name structure and that share the same database)
- *Groups*  
(for example: departments, divisions, locations, countries)
- *Objects*  
(for example: users, printers)

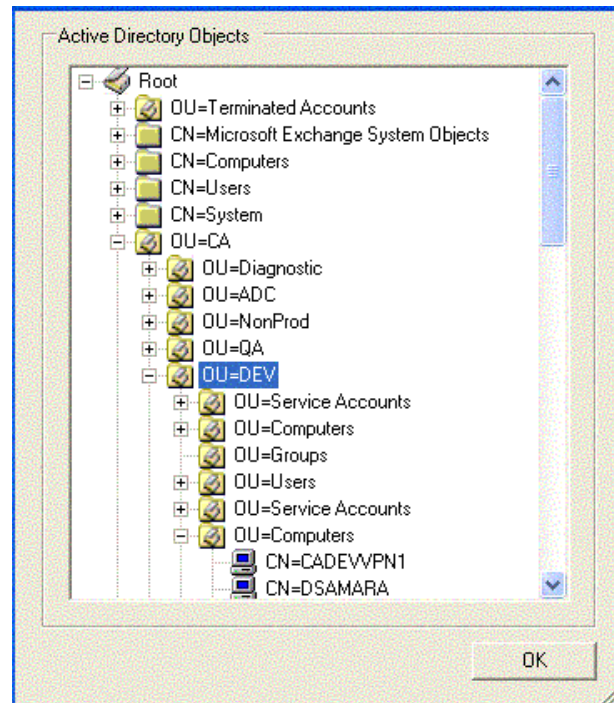
The following figures shows the hierarchy of objects.



### About Organization Unit

Within a domain, objects can be organized using a variety of container objects. One of the most common is the Organizational Unit (OU). An OU provides hierarchy grouping for a domain. This arrangement simplifies the administration of the domain and can be tailored to resemble the organizational structure in either managerial or geographic terms. An OU can be designed to contain other OUs to act as a container. The OU level is also where group policies are normally applied.

The following figure shows an example Active Directory hierarchy with Organizational Units.



## Active Directory: Browsing Utilities

The following utilities can be used to browse an Active Directory hierarchy and are available online for download:

- Microsoft Management Console - Active Directory Users and Computers Snap-In (MMC ADUC)
- Microsoft Dsquery  
(This utility is command-line based.)
- Microsoft Active Directory Explorer  
(Requires the ability to install third-party utilities)
- Apache Directory Studio  
(Requires the ability to install third-party utilities)

Many other utilities are available. Simply search online for “active directory utilities”.

## Active Directory: Glossary

The following is a list of terms and acronyms used in Active Directory and when configuring OPNET Authentication Service.

[A](#) | [B](#) | [C](#) | [D](#) | E | [F](#) | [G](#) | H | I | J | K | [L](#) | M | N | [O](#) | P | Q | [R](#) | [S](#) | T | U | V | W | X | Y | Z

### A

**Active Directory** – Active Directory stores information about objects on a network and makes this information available to users and network administrators. Active Directory provides network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects.

**Attribute** – Property or characteristic of an object in Active Directory.

**Authentication** – The process by which Active Directory verifies that an entity is who he claims to be by verifying credentials.

**Authorization** – The process by which Active Directory determines the set of permissions (i.e., roles).

### B

**binding** – A process by which an entity authenticates the Active Directory using the LDAP protocol.

### C

**CN** – Common name

### D

**DC** – Domain component

**DN** – Distinguished name. The distinguished name is unique path from the root of the tree to a particular entity in the tree. The DN is used to specify a particular entity.

**Domain** – a logical group of network objects (computers, users, devices) that share the same active directory database.

### F

**FQDN** – Fully Qualified Domain Name

### G

**group** – A collection of users, computers, contacts, and other groups.

**group membership** – The groups to which an entity belongs. Permissions and rights granted to a group are also provided to its members.

## L

**LDAP** – The lightweight directory access protocol used to access information available within Active Directory.

**LDAP Bind DN** – A user or administrator with sufficient access rights (read access) to perform the supported operations.

## O

**OpenAM** – A third-party open source software included with OPNET Authentication Service, which provides authentication and authorization services.

**OPNET Authentication Service** – provides authentication (including single sign-on) and authorization (account access privileges) to other components deployed in the environment. And since authentication and authorization are specified on a single server, the information can be quickly defined and easily maintained.

**Organizational Unit (OU)** – the standard container within Active Directory that contains objects, such as users, groups, and computers.

## R

**RADIUS** – Remote Authentication Dial-In User Services is a client/server protocol and software that enables access servers to communicate with a central server to authenticate and authorize access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing the organization to set up a policy that can be applied at a single administered network point.

## S

**sAMAccountName** – A user object attribute. This is the user identification value often used for login. Typically, sAMAccountName is less than 20 characters and only uses letters, numbers, and the underscore character.

**sn** – Last name attribute

**SSL** – Secure Sockets Layer

## App B Active Directory: Configuration Fields

The following table lists the commonly edited fields used to configure Active Directory. The table includes the Active Directory default values and descriptions of the fields.

**Table B-1 New Data Store - Active Directory**

Field	Default	Description
Name		Required field The name used to identify the data store.
Load schema when finished	No (unselected checkbox)	Do not select this checkbox.
<b>- Server Settings -</b>		
LDAP Server Current Values New Value	localhost:50389	Required field The address of the authentication server and port number used for communication. Multiple values in this field can be used to specify backup servers. Use the format hostname:port For example: "auth2k.opnet.com:389". <b>Note</b> —Only specify a single server. If necessary, remove any servers that don't belong (such as the default server). To remove a server, click the server value in the <b>Current Values</b> field and then click <b>Remove</b> .
LDAP Bind DN	CN=Administrator,CN=Users,dc=datastore,dc=opnet,dc=com	A user or admin with sufficient access rights (read access) to perform the supported operations. For example: CN=Administrator,CN=Users,dc=opnet,dc=com". Note that the Bind DN is used by the software to connect to the Active Directory server, and is <i>not</i> for logging in to Authentication Service. Normally, this is a non-user "server account". <b>WARNING</b> —Be sure to enter an LDAP Bind DN with only read privilege. If the LDAP Bind DN has privileges other than read, than those actions can be performed from either OPNET Authentication Service or OpenAM.
LDAP Bind Password LDAP Bind Password (confirm)		The password for the entity in the "LDAP Bind DN" field.

**Table B-1 New Data Store - Active Directory (Continued)**

Field	Default	Description
LDAP Organization DN	dc=datastore,dc=opnet,dc=com	Required field  The point in the hierarchy from which to search downward.
LDAP SSL/TLS	No (unslected checkbox)	Whether to use secure communication between authentication server and OPNET Authentication Service.  For information about managing certificates, click <a href="#">here</a> to see Chapter 11 of the OpenAM 10.0.0 Administration Guide. Also, see <a href="#">Certificate Management</a> .
LDAP Connection Pool Minimum Size	1	The minimum number of LDAP connections in the pool for connecting to a directory server.
LDAP Connection Pool Maximum Size	10	The maximum number of LDAP connections in the pool for connecting to a directory server.
Maximum Results Returned from Search	1000	
Search Timeout	10	In seconds
LDAP Follows Referral	No (unselected checkbox)	
LDAPv3 Plug-in Search Scope	SCOPE_SUB	How far to search through the hierarchy.  Available options are: - SCOPE_BASE - SCOPE_ONE - SCOPE_SUB  "SCOPE_SUB" will search for the LDAP organization DN and all levels of the hierarchy below that DN. Note that this provides for a broader search, but may impact performance.  "SCOPE_ONE" will search the LDAP organization DN and one level below.
<b>- Plug-in Configuration -</b>		
LDAPv3 Plug-in Supported Types and Operations Current Values New Value	realm=read,create,delete,service user=read,create,edit,delete group=read,create,edit,delete	To restrict the admin user from deleting users in Active directory, replace the default entries for user and group with the following: - user=read - group=read

**Table B-1 New Data Store - Active Directory (Continued)**

Field	Default	Description
<b>- User Configuration -</b>		
LDAP Users Search Attribute	CN	A user attribute to search for a user.
LDAP People Container Naming Attribute	cn	The container for users. If users are not organized in a common container name, leave these fields blank.
LDAP People Container Value	user	
<b>- Authentication Configuration -</b>		
Authentication Naming Attribute	cn	The users for authentication. Typically, this field should be identical to the "LDAP Users Search Attribute" field.
<b>- Group Configuration -</b>		
LDAP Groups Search Attribute	cn	How groups are identified.
LDAP Groups Search Filter	(objectclass=group)	
LDAP Groups Container Naming Attribute	cn	The container for groups. (Commonly, the OU attribute is used for groups.)
LDAP Groups Container Value	users	If groups are not organized in a common container name, leave these fields blank.
Attribute Name for Group Membership		The name of the attribute whose values are the names of all the groups to which DN belongs. Typically, this value is set to "memberOf".



# System Requirements

## Support Platforms

### Microsoft

- Windows Server 2008 (32-bit)
- Windows Server 2008 SP 2 (64-bit)
- Windows Server 2008 R2 SP 1 (64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows Server 2003 (32-bit)
- Windows Server 2003 SP 2 (64-bit)
- Windows Server 2003 R2 (64-bit)

**Note**—All platforms are supported on the English language version of each operating system.

## System Configuration

<b>RAM</b>	<b>Required:</b> 1 GB <b>Recommended:</b> 4 GB
<b>Disk Space</b>	<b>Required:</b> 1 GB <b>Recommended:</b> 1+ GB

## Supported Web Browsers

- Microsoft Internet Explorer 8+ (Compatibility mode is *not* supported)
- Mozilla Firefox 3.6+
- Google Chrome

# Index

---

## Numerics

8dot3 Windows property, [23](#)

## A

AAM migration, required files, [48](#)

Active Directory

configuration fields, [86](#)

glossary, [84](#)

hierarchy of objects, [81](#)

introduction, [80](#)

objects, [81](#)

organization units, [82](#)

utilities, [83](#)

administrative user

default, [41](#)

role, [41](#)

specially-designated administrator, [66](#)

sync, [42](#)

Apache Directory Studio, [83](#)

architecture of solution, [14](#)

authentication module configuration, [26](#)

## B

backup

create, [52](#)

important notes, [51](#)

options, [50](#)

restore, [53](#)

BrowserMetrix, [8](#)

roles, [41](#)

BrowserMetrixAdmin role, [41](#)

BrowserMetrixView role, [41](#)

browsers

supported, [89](#)

## C

certificate management, [43](#)

chain of trust, [43](#)

CN (Common Name), [81](#), [84](#)

## D

debug logs, [73](#)

deployment, typical, [6](#)

Directory Manager user, [17](#), [19](#), [72](#)

DN (Distinguished Name), [81](#), [84](#)

## E

Error

8dot3 name creation, [75](#)

external user/group

add to list of users/groups, [42](#)

## G

glossary for Active Directory, [84](#)

groups

assign roles to, [42](#)

fetch, [29](#)

## H

HTTPS support, [43](#)

## I

installation

configure authentication, [26](#)

configure authorization, [41](#)

install software, [23](#)

installer freezes, [75](#)

prepare for, [15](#)

sequence of components, [9](#)

virus scanning software, [23](#)

workflow, [15](#)

## K

keytool command, certificate management, [43](#)

## L

LDAP Bind DN, [85](#), [86](#)

local users/groups, configuration, [40](#)

logs

set debug level, [73](#)

view, [74](#)

## M

Microsoft Active Directory Explorer, [83](#)

Microsoft Dsquery, [83](#)

migration considerations

sequence, [11](#)

Transaction Trace Warehouse users and roles, [12](#)

migration utility (AAM to OAS), [45](#)

## O

objects, Active Directory, [81](#)

OpenAM

access/introduction, [13](#)

glossary term, [85](#)

OPNET Authentication Service

role, [41](#)

OPNET Dashboards, [8](#)

migration/upgrade considerations, [11](#)  
Organizational Unit  
glossary term, [85](#)

## P

password, change/reset, [58](#)

## R

### RADIUS

glossary term, [85](#)

### RADIUS server

configure authentication module, [30](#)

restart service, [57](#)

revoke user access, [62](#)

### roles

add, [63](#)

assign to user/group, [65](#)

default roles, [41](#)

delete, [64](#)

view list assigned to a user, [60](#)

RootAdmin role, [41](#)

## S

sAMAccountName, [81](#), [85](#)

service start/stop, [57](#)

service-account user/group, [17](#), [72](#)

single-sign on, requirements, [22](#)

solution architecture, [14](#)

start/stop service, [57](#)

sync admin users, [42](#)

system requirements, [89](#)

## T

Transaction Trace Warehouse, [8](#)

migration of users and roles, [12](#)

migration/upgrade considerations, [11](#)

roles, [41](#)

TTWAccess role, [41](#)

TTWAdmin role, [41](#)

## U

uninstall, [72](#)

user interface, [13](#)

access OpenAM, [13](#)

user-role mapping file, migration utility, [47](#)

### users

assign roles to, [42](#)

define local, [40](#)

fetch, [28](#)

view a list of user's with a specific assigned role, [61](#)

utility, AAM to OAS migration, [45](#)

## V

virus scanning software, installation, [23](#)

## W

web browsers

supported, [89](#)