CA Nimsoft® Unified Management™ Portal

How to Configure UMP for Use with SiteMinder

7.6

Contents

Chapter 1: Introduction 5

Chapter 2: How to Configure UMP for Use with SiteMinder 7

Prerequisites 8
    Verify LDAP Mapping 9
Configure LDAP on the Hub Probe 9
Link ACLs to LDAP Groups 11
Modify the Portal Configuration to Enable SiteMinder 11
Verify UMP Resources are Protected in SiteMinder Policy Server 12
Edit the Secure Proxy Server Configuration 13

Appendix A: Troubleshooting 15

Copyright 16

Chapter 1: Introduction

Product: CA Nimsoft® Unified Management™ Portal, CA SiteMinder®

Release: 7.6

This scenario describes how a security administrator configures the Unified Management Portal (UMP) to be protected by SiteMinder. Using SiteMinder with UMP provides greater security for your organization. In addition, you can implement single sign-on access to UMP and other web applications.

This Knowledge Base Article constitutes a portion of the official CA product documentation for this CA product. This Knowledge Base Article is subject to the following notices (see page 16), terms and conditions.

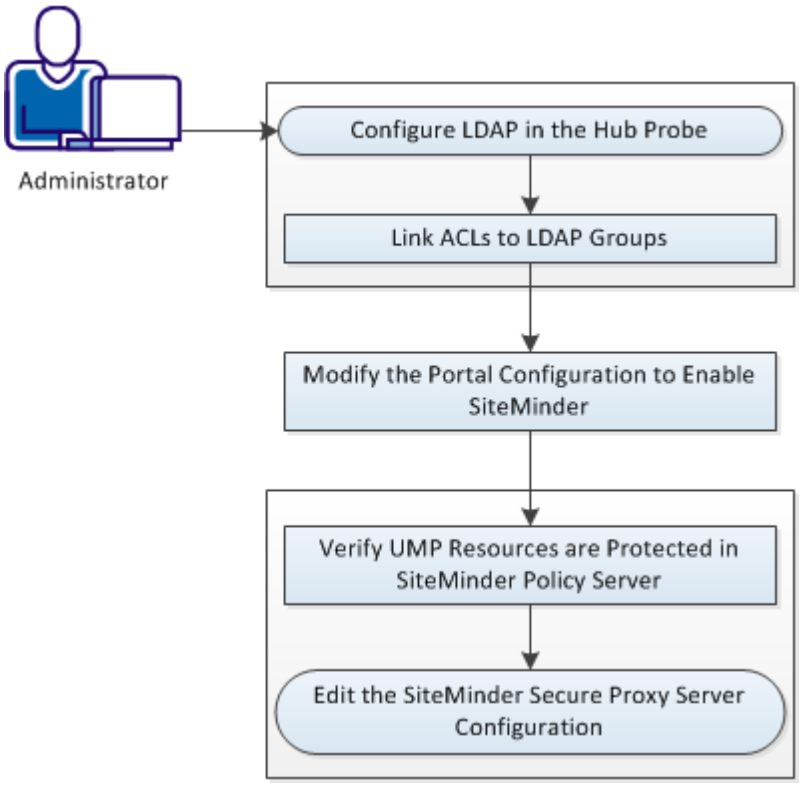
Chapter 2: How to Configure UMP for Use with SiteMinder

When a user logs in via SiteMinder, they enter a unique value, such as an email address or a user name. This unique value is matched against an attribute in the directory service for authentication.

This scenario uses the directory attribute *mail* as the <loginAttribute>. If you use Active Directory (AD), this attribute may be *sAMAccountName* or *upn.*

Note: Access to Admin Console as a portlet in UMP is not currently supported with Siteminder.

The following diagram shows how to configure UMP for Use with SiteMinder:



1. Configure LDAP in the Hub Probe (see page 9)
2. Link ACLs to LDAP Groups (see page 11)
3. Modify the Portal Configuration to Enable SiteMinder (see page 11)
4. Verify UMP Resources are Protected in SiteMinder Policy Server (see page 12)
5. Edit the Secure Proxy Server Configuration (see page 13)

The following resources are also available:

- CA SiteMinder documentation
  - SPS 12.51 Administration guide
- Nimsoft documentation
- Liferay Wiki > LDAP

Prerequisites

Important! Do not attempt to perform the procedures in this scenario unless you are proficient with CA Nimsoft Monitor, CA SiteMinder, and directory administration.

Ensure that the following prerequisites have been met before using the instructions in this scenario:

- CA Nimsoft Monitor (NMS and UMP) 7.5 or higher are installed and configured.
- CA SiteMinder r12.51 or higher is installed with an operational Secure Proxy Server.
- An LDAP directory exists for SiteMinder authentication and for linking to CA Nimsoft Monitor. The following directory services are supported:
  - Novell® eDirectory (TM) 8.8 SP1 (20114.57) and a Novell ® KDC (Key Distribution Center) server
  - SUN Java Directory Server v5.2
  - Windows 2008 and Windows 2012 Active Directory.

Verify LDAP Mapping

The following table identifies the user and group attributes that must map between your directory and the NMS hub and UMP. The attributes designated with an asterisk (*) are the required mappings for UMP. It is recommended that you determine these attributes in your directory service before continuing.

Refer to this table as needed as you perform the steps in the following sections.

Description	NMS Hub Mapping	UMP Mapping	LDAP Example
Group identifier	filter_group	ldap.import.group.search.filter	objectClass=groupOfNames
Group name	attr_grp_name	groupName	cn
Group member	attr_grp_member_name	user	member
Group description	attr_grp_description	description	description
User identifier	---	ldap.import.user.search.filter	objectClass=inetOrgPerson
*Username	---	screenName	cn
*User Password	---	password	userPassword
*User firstname	attr_usr_firstname	firstName	givenName
*User lastname	attr_usr_lastname	lastName	sn
*User email	attr_usr_mail, filter_user	emailAddress	mail

Configure LDAP on the Hub Probe

Configure the hub probe to forward login requests to your LDAP server, and to access the container with user groups.

Follow these steps:

1. Log into Infrastructure Manager and locate the hub probe.
2. Press the <Ctrl> key as you right-click the hub probe, and then select Raw Configure.

3. Expand the ldap section, and expand the templates section.
4. Select the appropriate directory service, and edit the value of key filter_user to (&(<loginAttribute>=$loginname)).
5. Depending on the directory service you are using, you may need to update the values of other keys to match your directory. Attributes that may be of particular importance are as follows:
   - filter_group
   - filter_user
   - attr_grp_name
   - attr_grp_member_name
   - attr_grp_description
   - attr_usr_firstname
   - attr_usr_lastname
   - attr_usr_mail
6. Click OK to commit your changes.

   The hub probe restarts.
7. In Infrastructure Manager, right-click on the hub probe and select Configure.
8. In the lower right of the General tab, select Settings.
9. In the LDAP tab, do the following:
   a. Select Direct LDAP.
   b. Select LDAP Authentication.
   c. In the Server Name field, enter the <*IP_address*:*port*> of LDAP server.
   d. Select the appropriate directory service from the Server Type drop-down menu.
   e. Select LDAP > Nimsoft from the Authentication Sequence drop-down menu.
   f. In the User field, enter the distinguished name (DN) of a directory user with administrative privileges.
   g. Provide a distinguished name (DN) in the Group Container (DN) and User Container (DN) fields as appropriate.

Link ACLs to LDAP Groups

Use the following steps to link ACLs to LDAP groups.

Follow these steps:

1. In Infrastructure Manager, select Security >Manage Access Control List.
2. Make a selection from the Access Control List, and click the Set LDAP Group button.
3. Select an LDAP group from list.
4. Select or de-select permissions in the list if desired.

Modify the Portal Configuration to Enable SiteMinder

Use the following steps to edit the portal-ext.properties file to map your directory to UMP.

Note: The steps in this section use the directory attribute *mail* as the <loginAttribute>. If <loginAttribute> is not *mail*, certain lines must be edited differently as indicated. In addition, line numbers in the portal-ext.properties file are provided, but may vary slightly from the line numbers in your portal-ext.properties file.

Follow these steps:

1. In Infrastructure Manager, deactivate the wasp probe.
2. On the UMP system, open the following file for editing: probes/service/wasp/web-inf/classes/portal-ext.properties.
3. Modify line 12 as follows:
   ```
   company.security.auth.type=emailAddress
   ```
   Note: If <loginAttribute> is not *mail*, modify line 12 as follows:
   ```
   company.security.auth.type=screenName
   ```
4. Comment out lines 16 and 17 as follows:
   ```
   #auth.pipeline.pre=com.firehunter.ump.auth.NmsAuth
   #auth.pipeline.enable.liferay.check=false
   ```
5. Uncomment lines 188 through 191 as follows:
   ```
   ldap.base.provider.url.0=ldap://<server:port>
   ldap.base.dn.0=ou=example,o=com
   ldap.security.principal.0=<DN of directory user>
   ldap.security.credentials.0=<password>
   ```

6. Uncomment lines 195 and 196 as follows:
   `ldap.auth.search.filter.0=(mail=@email_address@)`
   `ldap.import.user.search.filter.0=(objectClass=inetOrgPerson)`

   Note: If <loginAttribute> is not *mail*, modify line 195 as follows:
   `ldap.auth.search.filter.0=(<loginAttribute>=@screen_name@)`

7. Uncomment line 199 as follows:
   `ldap.import.method=user`

8. Uncomment lines 201 through 203, and modify the mapping as appropriate for your directory:
   `ldap.user.mappings.0=screenName=cn\npassword=userPassword\nemailAddress=mail\nfirstName=givenName\nlastName=sn\ngroup=ou`
   `ldap.import.group.search.filter.0=(objectClass=groupOfNames)`
   `ldap.group.mappings.0=groupName=cn\ndescription=description\nuser=member`

   Note: If <loginAttribute> is not *mail*, modify the screenName mapping in line 201 as follows:
   `screenName=<loginAttribute>`

9. Save the portal-ext.properties file, and reactivate the wasp probe.

Verify UMP Resources are Protected in SiteMinder Policy Server

Use the following steps to guide you in verifying that your UMP resources are protected.

Follow these steps:

1. Log into the Policy Server Admin UI.
2. Create a new agent for UMP, for example, <*nimsoft_agent*>.
3. Create a new Agent Configuration Object (ACO) by copying the SPS ACO, and naming it <*nimsoft_ACO*>.
4. Modify the default agent name key:
   `DefaultAgentName: <nimsoft_agent>`
5. Optionally modify and enable the log and trace parameters.

6. Define an Application or Domain Policy to protect the UMP resources, using the agent you just created (<*nimsoft_agent*>).
   a. The directory used for SiteMinder authentication is the same as that defined in the Nimsoft Hub and in the portal.
   b. The specific URLs to protect are as follows:
      - /web*
      - /documents*
      - /user*
      - /group*
   c. Create a response of type WebAgent-HTTP-Header-Variable. Select User Attribute as the Attribute Kind. Use the Variable Name UMP_USER, and the Attribute Name <loginAttribute>.

      Note: This response should be enabled for all resources.

Edit the Secure Proxy Server Configuration

Use the steps in this section to create a new web agent and define the virtual host for the UMP server.

Note: Do not allow direct access to the UMP server. Access should be controlled by firewall rules or other means.

Follow these steps:

1. Log into the Secure Proxy Server (SPS) host.
2. Follow the steps in the section "Web Agent Settings for the Default Virtual Host" in the CA SiteMinder Secure Proxy Server Administration Guide to copy the existing agent configuration file.
3. Issue the following commands:
   ```
   cd C:\Program Files
   (x86)\CA\secure-proxy\proxy-engine\conf\defaultagent\
   copy WebAgent.conf NimsoftWebAgent.conf
   ```
4. Modify the file NimsoftWebAgent.conf as follows:
   ```
   AgentConfigObject="<nimsoft_ACO>"
   ServerPath="ServerPath_nimsoft"
   AgentIdFile="C:\Program Files
   (x86)\CA\secure-proxy\proxy-engine\conf\defaultagent\NimsoftWeb
   AgentId.dat"
   ```

5. Edit the SPS server.conf file in the directory C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf\, and add a VirtualHost entry for UMP at the end of the file:

```
 # Nimsoft UMP Virtual Host
<VirtualHost name="nimsoftump">
  # The hostname the user sees in their browser
  hostnames="user.visible.hostname.com"
  redirectrewritablehostnames="ALL"
  enableredirectrewrite="yes"
  enablerewritecookiedomain="yes"
  enableproxypreservehost="yes"
  <WebAgent>
    sminitfile="C:\Program Files
(x86)\CA\secure-proxy\proxy-engine\conf\defaultagent\NimsoftWeb
Agent.conf"
  </WebAgent>
</VirtualHost>
```

6. Edit the proxyrules.xml in the directory C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf\, and add a rule to forward requests to the UMP server:

```
<nete:proxyrules xmlns:nete="http://www.ca.com/">
  <nete:cond type="host">
    <nete:case value="user.visible.hostname.com:80">

<nete:forward>http://nimsoft.ump.hostname.com$0</nete:forward>
    </nete:case>
    <nete:default>

<nete:forward>http://some.other.host.com/404.html</nete:forward
>
    </nete:default>
  </nete:cond>
</nete:proxyrules>
```

7. Restart the SiteMinder Proxy Engine Windows service.
8. Verify that you can access UMP via the virtual host defined previously in this section.

Appendix A: Troubleshooting

Refer to the following log files or tools:

hub.log | NMS machine | C:\Program Files (x86)\Nimsoft\hub\hub.log

- Helps show user and group import into the hub.
- Log level can be adjusted in the hub configuration.

portal.log | UMP machine | C:\Program Files (x86)\Nimsoft\probes\service\wasp\portal.log

- Helps show LDAP activity

Web Agent trace log | SPS machine| (location defined in ACO)

- Debugging is enabled in the proxy rules specification. See the SPS 12.51 Administration guide.
  - Helps show user authentication activity on the SPS.
- Ensure your SPS WebAgent has the TraceConfigFile parameter configured properly.
  - Helps show the HTTP response that is generated after authentication.

Policy Server Trace Log | PolicyServer machine | C:\Program Files (x86)\CA\siteminder\log\smtracedefault.log

- Defined under the Profiler tab in the Policy Server Management Console.

SiteMinder Test (smtest) tool | PolicyServer machine

- Useful for testing policy changes, particularly protection, authentication and authorization.
- Displays HTTP-header response information.

Copyright

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2014 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.