CA Unified Infrastructure Management Unified Management™ Portal

Configure UMP for SiteMinder

8.0

Contents

Chapter 1: Introduction

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.

Note: See the scenario *Configure UMP for SAML* if you are implementing SiteMinder with SAML.

Chapter 2: 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.*

The following resources are also available:

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

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

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

- CA Unified Infrastructure Management (UIM 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 Unified Infrastructure. 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 UIM 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	UIM Hub Mapping	UIM 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. Modify as required to agree with your specific LDAP directory attributes.

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

3. Expand the LDAP section, and expand the templates section.
4. Select the appropriate directory service, and edit the value of the key filter_user to use either attr_usr_email or attr_usr_id for log in lookups as follows:
   (|($attr_usr_mail=$loginname)($attr_usr_id=$loginname))
5. Set the value of the key attr_usr_id to cn.
6. 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
7. Click OK to commit your changes.

   The hub probe restarts.
8. In Infrastructure Manager, right-click on the hub probe and select Configure.
9. In the lower right of the General tab, select Settings.
10. 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*> or the <*server_FQDN:port*> of the 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. Click the Lookup button to verify the connection to the LDAP server.

h. Modify the distinguished name (DN) in the Group Container (DN) and User Container (DN) fields as appropriate.

i. Click the Test button to verify the credentials of the directory user with administrative privileges.

j. Click Ok and confirm the dialog to restart the hub.

Your changes are committed.

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 LDAP

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

Follow these steps:

1. In Infrastructure Manager, deactivate the wasp probe.

   Important! Do not edit the portal-ext.properties file while the wasp probe is running. Doing so will cause the wasp probe to crash.

2. On the UMP host, open the following file for editing:
   <*UMP_installation*>\probes\service\wasp\webapps\ROOT\WEB-INF\classes\portal-ext.properties

3. Locate the property company.security.auth.type and set it to screenName or emailAddress, depending on the attribute you authenticate with.

4. Comment out the two auth.pipeline.* properties to disable local authentication.
   - #auth.pipeline.pre=com.firehunter.ump.auth.NmsAuth
   - #auth.pipeline.enable.liferay.check=false

5. Uncomment and configure the LDAP properties section as follows:
   - ldap.base.provider.url.0=ldap://<server_FQDN:port>
   - ldap.base.dn.0=ou=<department>,o=<companyname>
   - ldap.security.principal.0=<DN of directory user>
   - ldap.security.credentials.0=<password>
   - ldap.auth.enabled=true
   - ldap.auth.required=true
   - ldap.auth.method=bind
   - If company.security.auth.type=screenName, uncomment and configure the following line:
     - ldap.auth.search.filter.0=(cn=@screen_name@)
   - If company.security.auth.type=emailAddress, uncomment and configure the following line:
     - ldap.auth.search.filter.0=(mail=@email_address@)
   - ldap.import.user.search.filter.0=(objectClass=<user_identifier>)
   - ldap.import.enabled=true
   - ldap.import.on.startup=true
   - ldap.import.method=user
   - ldap.import.interval=2

6. Uncomment the following properties and modify the mappings as appropriate for your directory:
   - ldap.user.mappings.0=screenName=cn\npassword=userPassword\nemailAddress=mail\nfirstName=givenName\nlastName=sn
   - ldap.import.group.search.filter.0=(objectClass=groupOfNames)
   - ldap.group.mappings.0=groupName=cn\ndescription=description\nuser=member
7. Uncomment the following LDAP properties with empty values:
   - ldap.user.custom.mappings.0=
   - ldap.contact.mappings.0=
   - ldap.contact.custom.mappings.0=

   Important! Failure to uncomment LDAP properties will result in a null pointer exception (NPE) when portal-ext.properties is read at startup.
8. 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, <UIM_*agent*>.
3. Create a new Agent Configuration Object (ACO) by copying the SPS ACO, and naming it <UIM_*ACO*>.
4. Modify the default agent name key:
   DefaultAgentName: <UIM_*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 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="<UIM_*ACO*>"
   ServerPath="ServerPath_nimsoft"
   AgentIdFile="C:\Program Files (x86)\CA\secure-proxy\proxy-engine\conf\defaultagent\NimsoftWebAgentId.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\NimsoftWebAgent.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 | UIM 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