CHAPTER 8

Authentication and Federated Identity

Revised: September 2013
OL-15762-04

Audience

We prepared this material with specific expectations of you.

- **Embedded Mode**—You understand fundamental principles of user authentication.
- **LDAP Mode**—YOU ARE A MICROSOFT ACTIVE DIRECTORY EXPERT with real-world experience in its configuration and administration.
- **Federation Mode**—YOU ARE A SAML 2.0 EXPERT with real-world experience in its configuration and administration, including import and export of SAML 2.0-compliant IdP and SP configuration files.

Concepts

Overview

User authentication features of DMS-Admin help you to:

- Authenticate **all** user sessions. (*We prevent you from disabling mandatory authentication, even though we allowed this in Cisco DMS 5.1.x and prior releases.*)
- Choose and configure an authentication method.
- Import user account settings from an Active Directory server.

- Synchronize user groups from an Active Directory server. Microsoft Active Directory is the only LDAP implementation that we support in this release.
- Use federation services with a SAML 2.0-compliant IdP to support SP-initiated "single sign-on" login authentication in your network (following an initial synchronization to a Microsoft Active Directory Server that populates the DMM user database).

Note **We support your use of one—and only one—IdP server with Cisco DMS 5.3.**

Glossary

Timesaver **Go to terms that start with...** [**A** | **C** | **D** | **F** | **I** | **L** | **O** | **P** | **R** | **S** | **U** | **X**].

A

Active Directory

Microsoft implementation of LDAP. A central authentication server and user store. Active Directory is the only LDAP implementation that we support in this release.

Active Directory forest

A domain-straddling combination of Active Directory trees within an organization that operates multiple Internet domains. Thus, the forest at "Amalgamated Examples, LLC" might straddle all trees across example.**com**, example.**net**, and example.**org**.

Or, to use Cisco as a real-world case-study, one forest could straddle **cisco.com** and **webex.com**, among others.

Note **Cisco DMS Release 5.3.x does not support Active Directory forests.**

Cisco Show and Share Release 5.3.12 does support Active Directory forests. See this white paper on Cisco.com:

http://www.cisco.com/en/US/prod/collateral/video/ps9901/ps6682/white_paper_c11-727483.html

Active Directory tree

A subdomain-straddling combination of IdPs throughout one Internet domain. These IdPs operate collectively on behalf of the Internet domain's constituent subdomains. Thus, the "tree" at **example.com** might encompass all of the IdPs to authenticate user sessions within subdomains such as these:

- **legal**.example.com
- **sales**.example.com
- **support**.example.com

Active Directory Federation Services

Active Directory Federation Services (AD FS) 2.0 is supported in Cisco Show and Share Release 5.3.12.

AD FS 2.0 is a software component that you can install on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries.

administrator DN The DN to authenticate your Active Directory server's administrator.

Note This release is more strict than most prior releases in its enforcement of proper LDAP syntax. Now, when you specify the administrator DN, **you must use proper syntax, which conforms exactly to LDIF grammar**.

- Proper syntax: `CN=admin1,OU=Administrators,DC=example,DC=com`
- Poor syntax: `EXAMPLE\admin1`

OTHERWISE

When you use poor syntax here for the first time while your DMM appliance runs DMS 5.3, we show you, the administrator, this error message: "Invalid username or password."

But if you used and validated poor syntax here before ***upgrading*** to Cisco DMS 5.3, we do not repeat the validation process. Therefore—*even though we do not show an error message to anyone*—**LDAP users simply cannot log in**.

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

authentication The process to verify if a directory service entity has correctly claimed its own identity.

C

↑ *Return to Top*

CA *certification authority*. Authority that issues and manages security credentials and public keys, which any directory service entity relies upon to encrypt and decrypt messages exchanged with any other directory service entity. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information that certificate requestors provide. After the RA verifies requestor information, the CA can then issue a certificate.

CN *common name*. An attribute-value pair that names one directory service entity but indicates nothing about its context or position in a hierarchy. For example, you might see `cn=administrator`. But `cn=administrator` is so commonplace in theory that it might possibly recur many times in an Active Directory forest, while referring to more than just one directory service entity. An absence of context means that you cannot know which device, site, realm, user group, or other entity type requires the implied "administration" or understand why such "administration" should occur.

Therefore, use of a standalone CN is limited in the LDIF grammar. Absent any context, a standalone CN is only ever useful as an RDN.

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

CoT *circle of trust*. The various SP that all authenticate against one IdP in common.

D

↑ *Return to Top*

DC

domain component. An attribute to designate one constituent part of a *fully-qualified domain name* (FQDN). Suppose for example that you manage a server whose FQDN is **americas.example.com**. In this case, you would link together three DC attribute-value pairs: **`DC=Americas,DC=example,dc=com.`**

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

digital certificate

Uniquely encrypted digital representation of one directory service entity, whether physical or logical. This trustworthy representation certifies that the entity is not an imposter when it sends or receives data through a secured channel. The CA normally issues the certificate upon request by the entity or its representative. The requestor is then held accountable as the "certificate holder." To establish and retain credibility, a certificate must conform to requirements set forth in International Organization for Standardization (ISO) standard X.509. Most commonly, a digital certificate includes the following.

- One DN to authenticate the directory service entity.
- One DN to authenticate the CA.
- A serial number to identify the digital certificate itself.
- An expiration date, after which any entity that receives the certificate should reject it.
- A copy of the certificate holder's public key.
- The CA's digital signature, so recipients can verify that the certificate is not forged.

directory service entity

Any single, named unit at any level within a nested hierarchy of named units, relative to a network. An entity's essence depends upon its context. This context, in turn, depends upon interactions between at least two service providers—one apiece for the naming service and the directory service—in your network. Theoretically, an entity might represent any tangible thing or logical construct.

- By "tangible thing," we mean something that a person could touch, which occupies real space in the physical world. For example, this entity type might represent one distinct human being, device, or building.
- By "logical construct," we mean a useful abstraction whose existence is assumed or agreed upon but is not literally physical. For example, this entity type might represent one distinct language, subnet, protocol, time zone, or ACL.

An entity's purpose is broad and flexible within the hierarchical context that defines it.

DN

distinguished name. A sequence of attributes that help a CA to distinguish a particular directory service entity uniquely for authentication. Distinct identity in this case arises from a text string of comma-delimited attribute-value pairs. Each attribute-value pair conveys one informational detail about the entity or its context. The comma-delimited string *is* the actual DN. It consists of the entity's own CN, followed by at least one OU, and then concludes with at least one DC. For example:

```
CN=username,OU=California,OU=west,OU=sales,DC=Americas,DC=example,DC=com
```

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

Thus, each DN represents more than merely one isolated element. A DN also associates the element to its specific context within the Active Directory user base that your IdP depends upon.

Tip **Any DN might change over the lifespan of its corresponding entity.** For example, when you move entries in a tree, you might introduce new OU attributes or deprecate old ones that are elements of a DN. However, you can assign to any entity a reliable and unambiguous identity that persists beyond such changes to its context. To accomplish this, merely include a *universally unique identifier* (UUID) among the entity's set of operational attributes.

F

↑ *Return to Top*

federation

The whole collection of authentication servers that synchronize their user bases to one IdP in common and thereby make SSO possible within a network. This mutualized pooling of user bases bestows each valid user with a "federated identity" that spans an array of your SPs.

I

↑ *Return to Top*

IdP

identity provider. One SAML 2.0-compliant server (synchronized to at least one Active Directory user base), that authenticates user session requests upon demand for SPs in one network subdomain. Furthermore, an IdP normalizes data from a variety of directory servers (user stores).

Users send their login credentials to an IdP over HTTPS, so the IdP can authenticate them to whichever SPs they are authorized to use. As an example, consider how an organization could use three IdPs.

- An IdP in **legal**.example.com might authenticate user sessions for one SP, by comparing user session requests to the user base records from one Active Directory server.
- An IdP in **sales**.example.com might authenticate user sessions for 15 SPs, by comparing user session requests to the user base records from three Active Directory servers.
- An IdP in **support**.example.com might authenticate user sessions for four SPs, by comparing user session requests to the user base records from two Active Directory servers.

Caution **Only a well known CA can issue the digital certificate for your IdP.** Otherwise, you cannot use SSL, HTTPS, or LDAPS in Federation mode and, thus, all user credentials are passed in the clear.

Tip **We have tested Cisco DMS federation features successfully against OpenAM, PingFederate, and Shibboleth.** We recommend that you use an IdP that we have tested with Cisco DMS. We explicitly DO NOT support Novell E-Directory or Kerberos-based custom directories.

If your IdP fails, you can switch your authentication mode to LDAP or Embedded.

L

↑ *Return to Top*

LDAP

Lightweight Directory Access Protocol. A highly complex data model and communications protocol for user authentication. LDAP provides management and browser applications with access to directories whose data models and access protocols conform to X.500 series (ISO/IEC 9594) standards.

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

LDAPS

Secure LDAP. The same as ordinary LDAP, but protected under an added layer of SSL encryption.

Note **Before you try to configure SSL encryption and before you let anyone log in with SSL, you MUST:**
- Activate SSL on your Active Directory server and then export a copy of the server's digital certificate.
- Import into DMM the SSL certificate that you exported from Active Directory.
- Restart Web Services (Tomcat) in AAI.

Caution **Is your DMM appliance one half of a failover pair?**
If so, you will trigger immediate failover when you submit the command in AAI to restart Web Services. This occurs by design, so there is no workaround.

LDIF

LDAP Data Interchange Format. A strict grammar that SPs and IdPs use to classify and designate named elements and levels in Active Directory.

O

↑ *Return to Top*

OpenAM

SAML 2.0-compliant identity and access management server platform written in Java. OpenAM is open source software available under the Common Development and Distribution (CDDL) license. OpenAM is derived from and replaces OpenSSO Enterprise, which also used CDDL licensing. See http://www.forgerock.com/openam.html.

OU

organizational unit. An LDIF classification type for a logical container within a hierarchical system. In LDIF grammar, the main function of an OU value is to distinguish among superficially identical CNs that might otherwise be conflated. For example:

- `CN=John Doe,`**`OU=sales`**`,DN=example,DN=com`
- `CN=John Doe,`**`OU=marketing`**`,DN=example,DN=com`

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

P

↑ *Return to Top*

PingFederate

SAML 2.0-compliant identity and access management server platform written in Java. PingFederate is proprietary, commercial software. See http://www.pingidentity.com.

R

↑ *Return to Top*

RDN

relative distinguished name. The CN for a directory service entity, as used exclusively (and still without any explicit context) by the one IdP that has synchronized this entity against an Active Directory user base. When an IdP encounters any RDN attribute in an LDIF reference, the IdP expects implicitly that its SAML 2.0-synchronized federation is the only possible context for the CN. It expects this because an IdP cannot authenticate—and logically should never encounter—a directory service entity whose RDN is meaningful to any other federation.

S

↑ *Return to Top*

SAML

Security Assertion Markup Language. XML-based open standard that security domains use to exchange authentication and authorization data, including assertions and security tokens. **We support SAML 2.0.**

Shibboleth

A SAML 2.0-compliant architecture for federated identity-based authentication and authorization.

SP *service provider*. Server that requests and receives information from an IdP. For example, SPs in Cisco DMS include your DMM server and your *Show and Share* server.

SSO *single sign on*. (And sometimes *"single sign **off**."*) The main user-facing benefit of federation mode is that SPs begin—and end, in some implementations—user sessions on behalf of their entire federation. SSO is a convenience for users, who can log in only once per day as their work takes them between multiple servers that are related but independent. Furthermore, SSO is a convenience to IT staff, who spend less time on user support, password fatigue, compliance audits, and so on.

- We DO NOT support single sign **off** in Cisco DMS 5.3.
- We support only **SP-initiated** SSO in Cisco DMS 5.3.

U

↑ *Return to Top*

user base The location of the user subtree in the LDAP directory tree. For example, `DC=ad,DC=com`.

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

user base DN The DN for an Active Directory user base.

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Otherwise, validation fails.

user filter A user filter limits the scope of an agreement to import filtered records from an Active Directory user base.

Note **An LDAP expression must never include a space immediately to either side of a "=" sign.** Similarly, it must never include a space immediately to either side of an "objectClass" attribute. Nor can a group name include any spaces. Otherwise, validation fails.

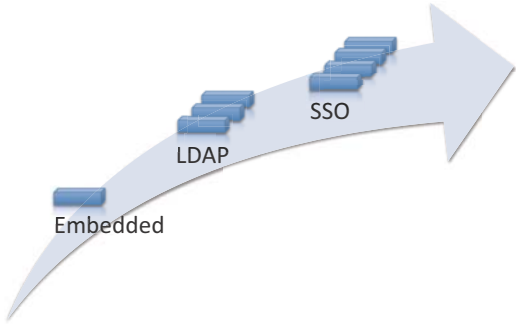
X

↑ *Return to Top*

X-509 A standard for public key infrastructure. X.509 specifies, among other things, standard formats for public key certificates and a certification path validation algorithm.

Understand the Requirement to Authenticate Users

Although Cisco DMS always authenticates users, we support three authentication methods.



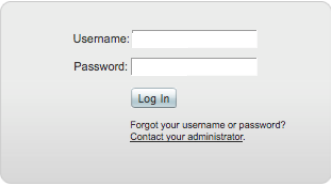
- *Embedded authentication* is completely native to Cisco DMS. It does not depend on any external servers.
- *LDAP authentication* causes Cisco DMS products to rely on one—and only one—Microsoft Active Directory server and a Microsoft Internet Information Server (IIS). Thus, setup and operation with this method are more complex than with embedded authentication.
- *Federation mode—also known as single sign-on* (SSO) causes Cisco DMS products to rely on a SAML 2.0-compliant IdP in combination with a Microsoft Active Directory server and IIS. Thus, setup and operation with this method are more complex than with LDAP authentication.

Note **You must choose one of these methods.** The method that you use determines which login screen your users will see.

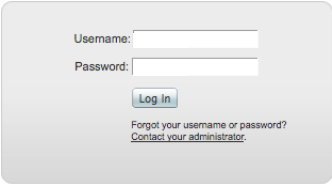
Tip

- **After a user session times out, we prompt the affected user to log in twice.**
- **Migration from one mode to another takes as long as 1 minute to finish (CSCtn22370).**
- **An unresponsive Active Directory server can hang a login prompt for 20 minutes without any error message.**

EMBEDDED MODE



LDAP MODE



FEDERATION (SSO) MODE [1]

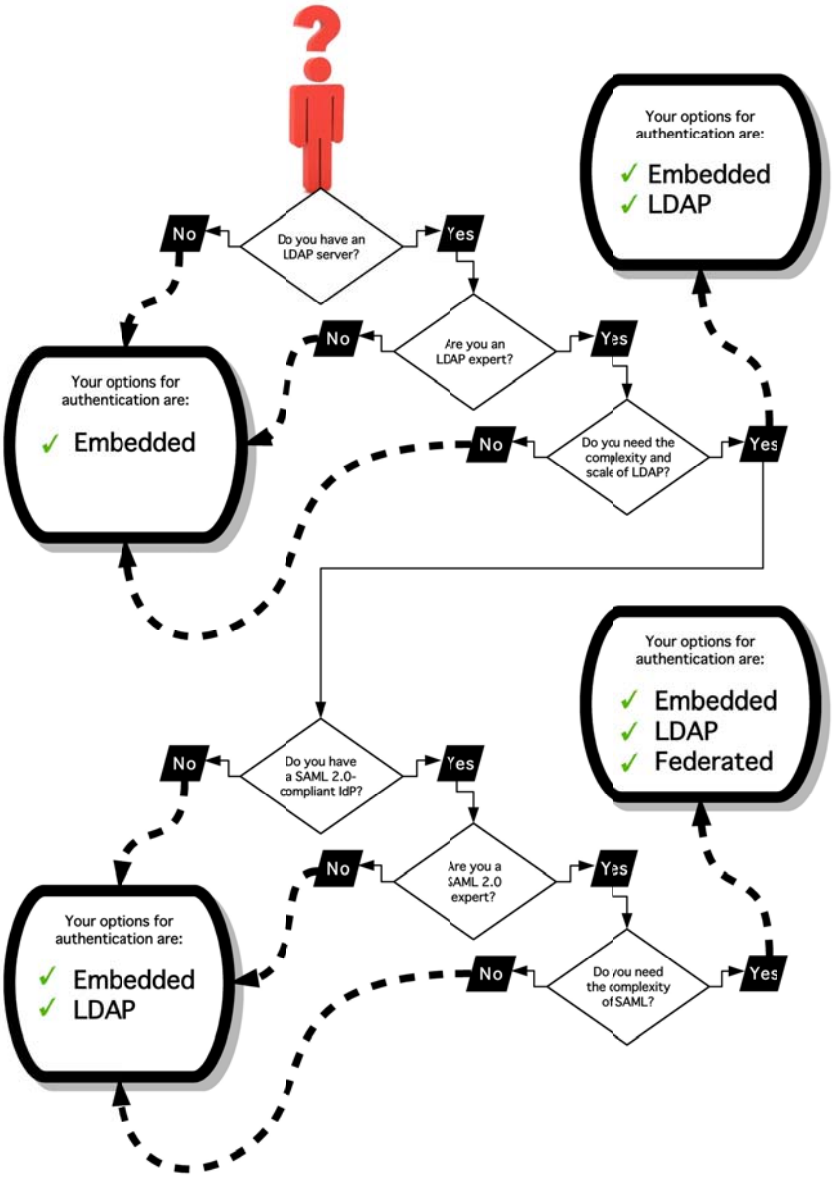
IdP-specific login screen

1. When any of your federation servers uses a self-signed certificate, we show your users **two SSL warnings** during login.

Related Topics

- LDAP and Active Directory Concepts, page 8-10
- Federated Identity and Single Sign-on (SSO) Concepts, page 8-17

Decide Which Authentication Method to Use



LDAP and Active Directory Concepts

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

- LDAP Concepts, page 8-14
- Password Concepts, page 8-16
- Understand Authentication Property Sheets for LDAP, page 8-17

LDAP is Highly Complex

Caution **LDAP-related features of Cisco DMS are meant for use by qualified and experienced administrators of Microsoft Active Directory.** Unless you are an Active Directory and LDAP expert, we recommend that you use embedded authentication.

Plan Ahead

- Install and configure Active Directory and Internet Information Services (IIS) before you try to configure LDAP authentication mode or federation mode in DMS-Admin.

Tip **We support IIS 6 on Windows Server 2003.**

- Pair your DMM appliance and your Show and Share appliance in AAI before you configure Cisco DMS to use LDAP authentication. Otherwise, video tutorials for Show and Share are not loaded onto your Show and Share appliance.
- Make sure that you have generated or imported certificates as necessary and activated SSL on the Active Directory server before you try to configure SSL encryption.

Restrictions

Cisco DMS Release	Support for Active Directory	
	Trees	Forests
5.3.0	Yes	No

Synchronization Concepts

- Synchronization (Replication) Overview, page 8-12
- Synchronization Types, page 8-12
- Understand Manual Synchronization, page 8-13
- Understand Automatic Synchronization, page 8-13
- Guidelines for Synchronization, page 8-14

Synchronization (Replication) Overview

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

When you choose LDAP authentication or SSO authentication, user account data originates from your Active Directory server. However, Cisco DMS *does not* synchronize (replicate) this data automatically, in real time. Instead, we cache it. Therefore, you must resynchronize user account data when you think it is appropriate to do so. You can:

- Resynchronize manually.
- Schedule synchronizations to recur in the future at set intervals.

Note **Features of *Digital Signs* and *Show and Share Administration* help you to manage user access privileges and permissions for Cisco DMS.**

DMS-Admin synchronizes all user accounts in the Active Directory "user base" that your filter specifies, **except users whose accounts are disabled** on your Active Directory server.

Synchronization Types

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

We support four types of Active Directory synchronization in LDAP mode or federation mode.

Initial	Update	Overwrite	Delete
Runs a one-time synchronization for a new filter that you never synchronized previously.	Runs an incremental, fast update to find and make up for any differences between user accounts that match your Active Directory filter and your local copy of those user accounts.	Overwrites your local copy of user accounts that correspond to your Active Directory filter with new copies of those user accounts. In addition, deletes your local copy of each user account that has been deleted from Active Directory since the last time that you ran a synchronization.	Deletes your local copy of user accounts that correspond to a defined Active Directory filter and deletes the entry for that filter from DMS-Admin.

Understand Synchronization of a DMM Group to an LDAP Filter

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

Is the Active Directory Filter Associated to a DMM User Group?	We Sync All Matching LDAP User Accounts to the	
	'All Users' Group in DMM	Associated User Group in DMM
Yes	Yes	Yes
No	Yes	N.A.

- In most cases, you can associate one LDAP filter apiece to one DMM user group. Likewise, in most cases, you can associate one DMM user group apiece to one LDAP filter. **The Digital Signs user group is an exception to both of these principles.** It is built-in to Cisco DMS.
- After you associate a DMM user group to an LDAP filter, you cannot use features on the Users tab to delete the DMM user group until after you delete the LDAP filter. However, even when you delete an LDAP filter, there is no requirement to delete its associated DMM user group. **Furthermore, there is no way for you to delete the Digital Signs user group.** It is built-in to Cisco DMS.

Understand Manual Synchronization

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

Manual synchronization mode requires you to choose Administration > Settings > Authentication > Synchronize Users > LDAP Bookmarks during all future synchronizations. Afterward, you must click Update.

Manual synchronization mode deletes your schedule for automatic synchronizations.

Understand Automatic Synchronization

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

Automatic synchronization mode automates and schedules incremental updates to user accounts that match Active Directory filters that you defined in DMS-Admin. When you use automatic synchronization mode, new fields and elements become available to you. These help you to configure the settings for automatic synchronization.

See the "Understand Synchronization of a DMM Group to an LDAP Filter" section on page 8-13.

Guidelines for Synchronization

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

We recommend that you synchronize your LDAP bookmarks periodically. Synchronization ensures that user and group membership associations are current and correct.

Sync Type	Best Practices
Initial	The *Initial* option is CPU-intensive for your DMM appliance and might lower performance temporarily. We recommend that you use it during *off-peak* hours only.
Update	We recommend that you use the *Update* option whenever: • A new user account in Active Directory should have login access to DMM or Show and Share. • User attributes[1] change in Active Directory for a user account in DMM or Show and Share. • A user account is disabled in Active Directory and should be deleted from DMM and Show and Share.
Overwrite	**Note** **The *Overwrite* option is CPU-intensive for your DMM appliance and might lower its performance temporarily.** We recommend that you use this option during off-peak hours only. • After a user account is deleted from Active Directory, this option deletes the corresponding user account from DMM and Show and Share. • After a user account is associated to a new first name, last name, or username, this option overwrites the outdated user account attributes.
Delete	**Caution** **The *Delete* option is destructive by design.** We advise that you use it sparingly and with great caution. Among other effects, your deletion of an LDAP bookmark can affect user access to videos in Show and Share. **Note** **Typically, the deletion process takes about 1 minute to finish.** However, when there are more than 50,000 users in the Active Directory database, this process might run in the background and take about 30 minutes to finish. In this case, the user interface in DMS-Admin can show that a bookmark was deleted even though the actual process has not finished. If you observe this behavior, simply allow 30 minutes for the operation to finish.

1. Attributes that you entered on the Manage Attributes property sheet in DMS-Admin.

Related Topics

- Manage LDAP (Active Directory) Attributes, page 8-26

LDAP Concepts

Understand LDAP Attributes

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

Ordinarily, DMS-Admin *will not* import any user account record from your Active Directory server when the value in it is blank for any of these attributes:

- **Login User Name**—This required value always must be unique.
- **First Name**—This required value might be identical for multiple users.
- **Last Name**—This required value might also be identical for multiple users.

However, you can import and synchronize all of the Active Directory user account records that match your filters. You can do this even when some of the user account records are incomplete because one or more of their attributes have blank values.

To prevent these undefined attributes from blocking the import of the user accounts they are meant to describe, you can enter generic values for most attributes in the Values to Use by Default column. DMS-Admin takes the generic values that you enter, and then inserts them automatically where they are needed.

Tip **Nonetheless, you cannot enter a default value for the Login User Name attribute.** Usernames are unique.

Guidelines for LDAP Filters

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

- Use “OU” values to impose rough limits on a filter, page 8-15
- Use “memberOf” values to pinpoint a filter more precisely, page 8-16
- Use “objectClass” values to match all user records, page 8-16

Use “OU” values to impose rough limits on a filter

- Never use a filter that defines the user base at the domain level. For example, this filter is not acceptable.

```
DC=example,DC=com
```

- Instead, use filters that define the user base at a lower level, as this one does.

```
OU=SanJose,DC=example,DC=com
```

- LDAP returns matched records **from all levels** within the user base that your filter defines.

Would a filter for "`OU=SanJose,DC=example,DC=com`" ever include any users from...?	
`OU=RTP,DC=example,DC=com`	No[1]
`OU=Milpitas,OU=SanJose,DC=example,DC=com`	**Yes**[2]
`OU=Sunnyvale,OU=SanJose,DC=example,DC=com`	**Yes**[2]

1. Research Triangle Park, NC, does not have any physical connection to San José, CA.
2. Milpitas, CA and Sunnyvale, CA, are suburbs of San José, CA, which affects them directly and in multiple ways.

Use "memberOf" values to pinpoint a filter more precisely

- But what if you did not want to include any members of Milpitas or Sunnyvale? If your Active Directory server considered these cities (organizational units) to be subsets of San José, how could you exclude their members? To do so, you would use the

  `memberOf`

  attribute. It stops LDAP from matching records at any lower level than the one you name explicitly. In this scenario for example, you would use

  `memberOf=OU=SanJose,DC=example,DC=com`

  to match only the direct members of the "SanJose" OU.

Use "objectClass" values to match all user records

- You can define a comprehensive filter that matches all user records.

  `objectClass=user`

Password Concepts

- Understand the Effects of a Changed Password in Active Directory, page 8-16
- Understand the Effects of a Blank Password in Active Directory, page 8-17

Understand the Effects of a Changed Password in Active Directory

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

After you change a user password on your Active Directory server, there is no requirement to resynchronize the affected user account in DMS-Admin.

Understand the Effects of a Blank Password in Active Directory

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

- Even though it is possible in Active Directory to use a blank value for a password, Cisco DMS does not allow it.
- When you choose LDAP authentication, any user whose Active Directory password is blank is prevented from logging in to any component of Cisco DMS.
- Access is enabled or restored after the password is populated on the Active Directory server.

Understand Authentication Property Sheets for LDAP

Note **Microsoft Active Directory is the only LDAP implementation that we support in this release.**

The Authentication page contains four tabbed property sheets.

Select Mode[1]		*Embedded, LDAP or SSO* Select Mode is by default the only active tab. Your choices on the Select Mode property sheet determine whether you have access to the other three property sheets.
Define Filter		*LDAP or SSO* Your choices on the Define Filter property sheet help you to configure and add a new agreement.
Synchronize Users		*LDAP or SSO* Your choices on the Synchronize Users property sheet help you to submit a new agreement.
Manage Attributes		*LDAP or SSO*

1. In most production environments, you can expect to use the Select Mode property sheet only one time.

Federated Identity and Single Sign-on (SSO) Concepts

IdP Requirements

To use federation (SSO) mode in Cisco DMS, you must have access to an IdP that meets our requirements. Your IdP must meet **ALL OF THESE CRITERIA IN COMBINATION**:

- Support SAML 2.0.
- Support these two SAML profiles:
  - Web Browser SSO Profile
  - Enhanced Client or Proxy (ECP) Profile

- Generate assertions in which the SAML "UID" attribute is mapped to the local portion of an authenticated user's username.
- Generate SAML responses that are no larger than 16K bytes. (CSCua10799)
- Use a digital certificate from a well-known CA (but only if you will use HTTPS).
- Include a "<SingleSignOnService>" entry with SOAP binding in its IdP metadata. For example:

```
<SingleSignOnService Location=http://idp.example.com/idp/SSO.sml2"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
```

In practice, these requirements limit your IdP to ones that we certify and NO OTHER. We certify OpenAM, PingFederate, and Shibboleth. (CSCua29696)

Configuration Workflow to Activate Federation (SSO) Mode

1. Configure and set up an Active Directory server.
2. Configure and set up a SAML 2.0-compliant IdP.

   Note When you use a "**fresh install**" of Cisco DMS 5.3 (as opposed to an upgrade), your DMM appliance is configured to use **embedded authentication mode** by default. But when you **upgrade** a DMM server that was already configured for an earlier Cisco DMS release, it might use **either embedded mode or LDAP mode**.

3. Obtain a digital certificate from a trusted CA and install it on your IdP.
4. Use DMS-Admin to configure Cisco DMS for federation mode.
5. Export SAML 2.0-compliant metadata from your DMM server and import it into your IdP.
6. Export SAML 2.0-compliant metadata from your IdP and import it into your DMM server.
7. Configure Active Directory exactly as you would in LDAP mode.
8. Click **Update** to save your work, and then advance to the Synchronize Users property sheet.
9. Synchronize DMM with your Active Directory server to populate the DMM user database.

   Note **You MUST configure at least one LDAP bookmark.**

10. Synchronize users exactly as you would in LDAP mode.

    Note **Whenever you change any setting or value on your IdP or any of your SPs, you must reestablish their pairing to restore mutual trust among them.**

11. Click **Update** to save your work.

Authentication Scenarios for User Sessions in Federation (SSO) Mode

- SSO Scenario 1—Trusted + Valid + Authorized
- SSO Scenario 2—Trusted + Valid + NOT Authorized
- SSO Scenario 3—Nothing Known

SSO Scenario 1—Trusted + Valid + Authorized

1. A web browser requests access to a protected resource on an SP.

   Your federation will not approve or deny this request until it knows more.
2. The SP asks its IdP if the browser is currently authenticated to any valid user account in the CoT.
3. The IdP verifies that:
   - The browser is already connected to an SP elsewhere in the CoT, having authenticated successfully to a valid user account and having received a SAML "token" or "passport" that authorizes at least some access.
   - **The user account has sufficient permissions to access the protected resource.**
4. The IdP acts on the SP's behalf and redirects the browser immediately to the protected resource.

SSO Scenario 2—Trusted + Valid + NOT Authorized

1. A web browser requests access to a protected resource on an SP.

   Your federation will not approve or deny this request until it knows more.
2. The SP asks its IdP if the browser is currently authenticated to any valid user account in the CoT.
3. The IdP verifies that:
   - The browser is already connected to an SP elsewhere in the CoT, having authenticated successfully to a valid user account and having received a SAML "token" or "passport" that authorizes at least some access.
   - **The user account DOES NOT have sufficient permissions.**
4. The IdP redirects the browser to the SP, where an **HTTP 403 Forbidden** message states that the user is not authorized to access the protected resource.

SSO Scenario 3—Nothing Known

1. A web browser requests access to a protected resource on an SP.

   Your federation will not approve or deny this request until it knows more.
2. The SP asks its IdP if the browser is currently authenticated to any valid user account in the CoT.
3. The IdP reports that:
   - The browser is not yet connected to any SP in the CoT.
   - The browser is not yet authenticated to any valid user account.
   - **We cannot tell if the browser's human operator is a valid and authorized user, a valid but confused user, or an intruder.**
4. The SP redirects the browser automatically to an HTTPS login prompt on the IdP, where one of the following occurs.
   - **The browser's human operator successfully logs in to a valid user account.** The IdP attaches a SAML "token" or "passport" to the browser session, authorizing at least some access. And:

     – The user account has permission to access the protected resource. So, the IdP acts on the SP's behalf and redirects the browser immediately to the protected resource.

     OR

     – The user account DOES NOT have permission to access the protected resource. So, the IdP redirects the browser to the SP, where an **HTTP 403 Forbidden** message states that the user is not authorized to access the protected resource.
   - **The browser's human operator fails to log in.** So, lacking any proof that this person is authorized, we block access to every protected resource until the human operator can log in successfully.

Migration Between Authentication Methods

Understand Migration (from Either LDAP or SSO) to Embedded

When you migrate from LDAP (via Active Directory) or federation mode to embedded authentication mode, you must explicitly choose whether to keep local copies of the:

- User accounts that were associated to LDAP filters.
- Groups and policies that were associated to LDAP filters.

Note

- **Unless you choose explicitly to keep the local copy of a user, a group, or a policy, we discard the local copy.**
- **Migration from one mode to another takes as long as 1 minute to finish (CSCtn22370).**

The result varies according to the combination of your choices.

When You Keep Local Copies of			
Users	**Groups**	**Policies**	**The Result**
Yes	**Yes**	**Yes**	• We preserve all local information. • We overwrite all LDAP-derived user account passwords with *CiscoDMMvp99999*. [1]
Yes	No	No	• We preserve all local user accounts. However, we overwrite all LDAP-derived user account passwords with *CiscoDMMvp99999*. [1] • We discard all LDAP-derived groups. • We discard all LDAP-derived policies.
No	**Yes**	**Yes**	• We discard all LDAP-derived user accounts. • We preserve all LDAP-derived groups. However, they are empty. • We preserve all LDAP-derived policies. Although they no longer apply to anyone, you can reuse them and apply them to any remaining user accounts and any future user accounts as you see fit.
No	No	No	• We discard all LDAP-derived users, groups, and policies.

1. This security feature protects your network and user data. If anyone gains unauthorized access to the exported file and tries to use it, Active Directory rejects the invalid passwords.

Understand Migration (from Embedded) to Either LDAP or SSO

Note

- **Before you migrate from embedded authentication mode to federation mode, you must install a digital certificate from a trusted CA on your IdP server.** Otherwise, you cannot migrate to federation mode at all.
- After you migrate from embedded authentication mode to either LDAP (Active Directory) mode or federation mode, the locked property sheets become unlocked. **You must use them.**
- **Migration from one mode to another takes as long as 1 minute to finish (CSCtn22370).**

Procedures

Export the Root CA X.509 Certificate from Your Active Directory Server

Procedure

Step 1 Open a web browser on your Active Directory server and connect to **http://localhost/certsrv**.

Step 2 Click **Download a CA certificate**.

Step 3 Choose the current CA certificate.

Step 4 Choose **DER encoded**.

The X.509 certificate that you export must be DER-encoded, and it can be binary or printable (Base64). However, when you use Base64, the certificate file must include these lines:

```
-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----
```

Step 5 Click **Download CA certificate**.

Step 6 Save this certificate in a file.

For example, you might call the certificate **ADcertificate.cer**.

Step 7 Stop. You have completed this procedure.

Configure DMM to Trust the Active Directory Root CA

Procedure

Step 1 Choose **Administration > Security > Authentication > Select Mode**.

Step 2 Enter the details for your Active Directory server.

Tip **Be sure to use the logical port where your Active Directory server listens for SSL connections.** The port number, by default, is **636**.

Step 3 Upload the root CA certificate file that you saved locally.

a. Click **Upload**, and then click **Add**.

b. Browse to the file on a local volume.

c. Click the filename and press **Enter**.

d. Click **OK** to save your work and dismiss the dialog box.

Step 4 As prompted, use DMS-Admin to restart Web Services (Tomcat).

The installed certificate cannot take effect until after you restart Tomcat.

Step 5 Stop. You have completed this procedure.

Choose an Authentication Method

Procedure

Step 1 Choose **Administration > Security > Authentication**.

Step 2 Use elements on the Select Mode property sheet to choose an authentication mode.

Step 3 Click **Update**.

Note **Migration from one mode to another takes as long as 1 minute to finish (CSCtn22370).**

The authentication settings that you changed are now in effect.

Step 4 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Did you choose LDAP (Active Directory) or SSO?*
  Proceed to the "Define LDAP (Active Directory) Filters" section on page 8-24

Related Topics

- Elements to Choose and Enable an Authentication Mode, page 8-50

Configure LDAP (Active Directory) Settings

Define LDAP (Active Directory) Filters

Before You Begin

- Choose LDAP or federation as your authentication method.

Procedure

Step 1 Choose **Administration > Security > Authentication**.

Step 2 Click **Define Filter**.

Step 3 Do the following.

a. Use elements on the Define Filter property sheet to define, validate, and add one LDAP filter.

b. Click **Update**.

c. Repeat this step for each filter to be added.

The authentication settings that you changed are now in effect.

Step 4 Stop. You have completed this procedure.

Related Topics

- Elements to Define, Validate, and Add LDAP Filters, page 8-53

Define LDAP (Active Directory) Bookmarks

Before You Begin

- Choose LDAP or SSO as your authentication method.
- Define LDAP filters.

Procedure

Step 1 Choose **Administration > Security > Synchronize Users > LDAP Bookmarks**,

Tip **Is the Synchronize Users tab disabled (dimmed), so that you cannot click it?** If so, refresh your browser.

Step 2 Do any or all of the following.

- *Would you like to import user accounts to Cisco DMS because they correspond to an Active Directory filter that you will define?* If so:
  - Choose the synchronization type for these user accounts.
  - Specify which default access privileges you will assign to them.
- *Should Cisco DMS synchronize user accounts that correspond to a defined Active Directory filter?* If so, use the synchronization type that you chose.

- *Would you like to sever your ties to a User Base or Active Directory server?* If so:
  - Delete from Cisco DMS all user accounts that correspond to a defined Active Directory filter.
  - Delete the entry for that filter from DMS-Admin.
- *Would you like to create a new group in DMM?*

  AND

  Populate it automatically with user accounts that correspond to an Active Directory filter that you defined previously?

  If so, delete the entry for that filter from DMS-Admin, and then recreate it while associating it to the new group.

Step 3 Validate the filter.

Step 4 Validate the DMM group name.

- Group names in DMM can include alphanumeric characters (**0-9**; **a-z**; **A-Z**), hyphens (**-**), underscores (_), and periods (**.**).
- Spaces are forbidden.
- Other forbidden characters include:

  ~`!@#$%^&*()+={[}]|\:;"“'<>?/

Step 5 Click **Update**.

Note **Please wait. Your request might take as long as 1 minute to process (CSCtn22370).**

The authentication settings that you changed are now in effect.

Step 6 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Would you like to associate a set of imported users with a new group?*
  Proceed to the "Derive LDAP (Active Directory) Group Membership Dynamically from a Query" section on page 8-28.
- **OPTIONAL**—*Would you like to configure the schedule for synchronization?*
  Proceed to the "Define the LDAP (Active Directory) Synchronization Schedule" section on page 8-26.

Related Topics

- Define LDAP (Active Directory) Filters, page 8-24
- Derive LDAP (Active Directory) Group Membership Dynamically from a Query, page 8-28
- Elements to Use LDAP Bookmarks for Synchronization, page 8-54

Define the LDAP (Active Directory) Synchronization Schedule

Before You Begin

- Choose LDAP or SSO as your authentication method.
- Define LDAP filters.
- Define LDAP bookmarks.

Procedure

Step 1 Choose **Administration > Security > Synchronize Users > Scheduling**,

Step 2 Choose between manual synchronization and automatic synchronization.

Note **You will not see any of the elements that the "Elements for Bookmarks" table describes until after you define at least one filter on the Define Filter property sheet.**

Step 3 Click **Update**.

The authentication settings that you changed are now in effect.

Step 4 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Would you like to associate attribute names in DMS-Admin and Active Directory?* If so, proceed to the "Manage LDAP (Active Directory) Attributes" section on page 8-26.
- **OPTIONAL**—*Should Cisco DMS expect that your Active Directory server uses factory-preset attribute names?* If so, proceed to the "Manage LDAP (Active Directory) Attributes" section on page 8-26.
- **OPTIONAL**—*Should Cisco DMS expect that your Active Directory server uses custom attribute names?* If so, proceed to the "Manage LDAP (Active Directory) Attributes" section on page 8-26.

Related Topics

- Define LDAP (Active Directory) Bookmarks, page 8-24
- Elements to Schedule Synchronization, page 8-55

Manage LDAP (Active Directory) Attributes

Before You Begin

- Choose LDAP or SSO as your authentication method.
- Define LDAP filters.

- Define LDAP bookmarks.
- Configure the LDAP synchronization schedule.

Procedure

Step 1 Click **Administration > Security > Authentication > Manage Attributes**.

Tip **Is the Manage Attributes tab disabled (dimmed), so that you cannot click it?** If so, refresh your browser.

Step 2 Use elements on the Manage Attributes property sheet to:

- Set the associations between DMS-Admin attribute names and their corresponding Active Directory attribute names.
- Use the predefined and typical names for Active Directory attributes (shown in grey text) or edit those attribute names so they match the names that your Active Directory server uses.
- Enter the values to use by default in DMS-Admin when a user account attribute is not defined on your Active Directory server.

You must enter a value for each mandatory attribute. You cannot enter a value to use by default for user names, because each user name is unique.

Step 3 Click **Update**.

The authentication settings that you changed are now in effect.

Step 4 Stop. You have completed this procedure.

Related Topics

- Define the LDAP (Active Directory) Synchronization Schedule, page 8-26
- Elements to Manage Attributes, page 8-56

Configure Automatic LDAP (Active Directory) Synchronization

Procedure

Step 1 Click the calendar icon ( ) to choose the start date for synchronization.

Step 2 Choose the hour and minute when synchronization should begin, and then choose either **AM** or **PM** as the period.

Step 3 From the Repeat Interval list, choose the interval of recurrence:

Interval	Description
Never	Synchronization occurs once and does not recur.
Every Day	Synchronization recurs once every 24 hours. You must set the hour and minute when it should start.
Every Week	Synchronization recurs once every 7 days. You must set the hour and minute when it should start.

Interval	Description
Every Month	Synchronization recurs once each month. You must set the hour and minute when it should start.
Custom	Synchronization recurs at an interval of your choosing. You must set the hour and minute when it should start. Choose **Days**, **Weeks**, or **Months** as the interval type. • Choose a day of the month from 1 to 30 when the interval type is Days. • Choose a day of the week when the interval type is Weeks. • Choose an interval of recurrence from 1 to 6 when the interval type is Months.

Step 4 (**Optional**)

- *Did you click the Automatic Synchronization radio button?*
- *And should a one-time synchronization start immediately, in addition to the start date and time that you specified?*

If so, check the **Synchronize users immediately** check box.

Step 5 Click **Update**.

The authentication settings that you changed are now in effect.

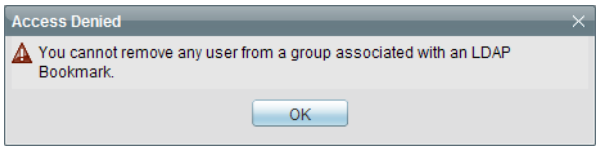
Step 6 Stop. You have completed this procedure.

Derive LDAP (Active Directory) Group Membership Dynamically from a Query

You can populate a user group with the returned output from a User Base DN query. However, a group of this kind differs in important ways from a group that you populate manually.

Note

- **Membership of such groups is dynamic—based on shared characteristics among the group of Active Directory users who match your query.**
- We update and clean these groups automatically during synchronization. **Their membership will change after synchronization runs**, when the corresponding records in Active Directory show that a user's membership should start or stop.
- An imported Active Directory group is always **read-only** in DMS-Admin. By protecting it, we ensure that it is always correct, relative to the original and subject to any delay between synchronizations. For this reason, you cannot edit their memberships rolls manually.
- When you try to delete a user from a group of this type, DMS-Admin shows an error message.



Before You Begin

- Choose LDAP as your authentication method.

Procedure

Step 1 Choose **Administration > Security > Authentication**.

Step 2 Click **Define Filter**,

Step 3 Use elements on the Define Filter property sheet to define, validate, and add one LDAP filter.

Step 4 *Would you like to add users to a group that exists already?* If so, choose that group name from the User Group (in DMM) list.

OR

Would you like to create and populate an entirely new group? If so, choose **Create a New User Group** from the User Group (in DMM) list. Then, use the Group Name field to enter a name for the new group.

Step 5 *Would you like to check your filter's syntax?* If so, click **Validate**.

Step 6 Click **Update**.

Step 7 Stop. You have completed this procedure.

Configure Federation Services for SSO

IdP Configuration Examples

This section includes configuration examples from IdP implementations that have passed internal Cisco tests for interoperability with Cisco DMS.

Note

- **We provide these rough examples as a courtesy only.** We do not endorse any IdP by name, including any whose setup we mention by name in these examples. Likewise, we do not influence the development of any IdP. We do not know when or how its configuration workflows, daily operation, or overall quality might change in the future. For these reasons, we cannot know beforehand when or how the natural course of its ongoing development might invalidate one or more of the examples in this section. Therefore: Obtain all necessary IdP documentation from your IdP vendor, not Cisco.
- **You are free to choose, configure, and use an IdP at your own discretion—and your own risk.** We do not develop, maintain, or support any IdP. Nor do we warrant that your choice of IdP is free of defects, non-infringing, or fit for any purpose.

Example: Configure OpenAM to Interoperate with Cisco DMS

Before You Begin

- Obtain a digital identity certificate from a well-known CA, install it on your IdP host system, and then enable SSL.

Procedure

Step 1 Configure OpenAM to use a datastore from Active Directory, unless it already does so.

Note **In Federation mode, we use a *synchronization* process to learn which usernames are valid in your organization.** Later and separately, we use an *authentication* process to verify user-login credentials. And even though we expect most IdPs will source both of these services from a Microsoft Active Directory server, your organization might use some other other LDAP system to authenticate user sessions. When this is the case, **you must install and configure an Active Directory server for synchronization use by Cisco DMS**. Otherwise, we cannot learn which usernames are valid. In turn, ordinary users cannot log in to Cisco DMS. To prevent this outcome, you must replicate and synchronize a datastore between your new Active Directory server and your existing LDAP server. Afterward, Cisco DMS can synchronize with the Active Directory datastore.

a. In OpenAM Web, choose **Access Control > Top Level Realm > Data Stores**.

b. Enter values to define the attributes of your Active Directory DataStore.

You might enter values for some of the attributes (like these ones, for example)...

```
LDAP Server: <IP_ADDRESS>:389
LDAP Bind DN: CN=Administrator,CN=Users,DC=win2003esx,DC=example,DC=com
LDAP Bind Password: *********
LDAP Organization DN: OU=SystemTest,DC=win2003esx,DC=example,DC=com
LDAP Users Search Attribute: sAMAccountName
LDAP Users Search Filter: (objectclass=user)
Authentication Naming Attribute: sAMAccountName
```

... while leaving other attribute values undefined.

```
Attribute Name Mapping: <Empty>
LDAP Groups Search Attribute: <Empty>
LDAP Groups Search Filter: <Empty>
LDAP Groups container Naming Attribute: <Empty>
LDAP Groups Container Value: <Empty>
Attribute Name of Unqiue Member: <Empty>
LDAP People Container Naming Attribute: <Empty>
LDAP People Container Value: <Empty>
Persistent Search Base DN: <Empty>
Persistent Search Filter: <Empty>
```

Note **These are merely examples.**

c. Click **Federation**, and then click your IdP server instance—for example, **dmsIdp**.

d. Click **Assertion Processing**.

e. Change the IDP Attribute Map value from UID=uid to **UID=sAMAccountName**.

Step 2	Install *Enhanced Client or Proxy* (ECP), a SAML profile plugin, if you will make API system calls to OpenAM[1].	**a.** Log in to your Cisco.com user account. **b.** Go to http://cisco.com/cisco/software/release.html?mdfid=280171249&softwareid=282100271&release=5.3&rellifecycle=&relind=AVAILABLE&reltype=all, navigate to the download page for our implementation of ECP[2], and then download it. **c.** Use Maven or another method to download release 1.2.14 of the open source logging framework called **log4j**. **d.** Copy your downloaded ECP and log4j files to `/$OPENSSO_HOME/WEB-INF/lib`, . **e.** Restart your servlet container—for example, tomcat. **f.** In OpenAM Web, click **Federation**, and then click your IdP server instance—for example, **dmsIdp**. **g.** Click **Advanced**. **h.** In the ECP Configuration area, set the IDP Session Mapper value to **com.cisco.dms.core.security.aaa.sso.saml2.ecp.idp.plugin.DmsIDPECPSessionMapper**. **i.** Click **Save**.
Step 3	Export SP metadata from Cisco DMS.	Export metadata from each SP that will participate in your OpenAM CoT. **Tip** For Cisco DMS, see the "Export SP Metadata from DMM" topic.
Step 4	Import SP metadata from Cisco DMS.	**a.** Go to the console page and click **Register Remote Service Provider**. **b.** Check the File check box. **c.** Click **Upload**, and then navigate to the SP metadata that you exported from DMS-Admin and saved as **dms_sp_config.xml**. **d.** Click **Configure**, and then click **Federation**. **e.** Make sure that *dmsServiceProvider (SAMLv2 SP Remote)* has a defined value.
Step 5	Make sure that OpenAM is configured to issue the *Principal* attribute.	**a.** In OpenAM Web, click **Federation**, and then click your IdP server instance—for example, **dmsIdp**. **b.** Click **Assertion Processing**. **c.** In the Attribute Mapper area, set the Attribute Map value to **UID=uid**. **d.** Click **Back**. **e.** Click the SP entity instance for your DMM appliance. The Assertion Content tab is selected automatically. **f.** In the Request/Response Signing area, check both of these check boxes: • Authentication Requests Signed • Assertions Signed **g.** Choose **Access Control > / (Top Level Realm) > Authentication**. **h.** Click **All Core Settings**. **i.** Make sure that the User Profile value is set to **Required**. This will cause OpenAM to pass the user IDs of logged-in users to DMM and your other SPs. **j.** Click **Save**, and then click **Back to Authentication**. **k.** Log out of OpenAM Web.

Step 6	Cause Cisco DMS to trust OpenAM.	See the "Import IdP Metadata into DMM" topic.
Step 7	Use the Linux CLI to export IdP metadata.	**wget --no-check-certificate https://**<IdP_serverip>**:**<service_port>**/opensso/saml2/jsp/exportmetadata.jsp -O dms_idp_config.xml**
Step 8	Stop.	You have completed this procedure.

1. Also, DMS-Admin includes a feature to test the configuration of your IdP. In the case of OpenAM, this testing feature uses ECP and fails in its absence.
2. We provide a downloadable ECP implementation as a courtesy to you. Alternatively, you can obtain ECP from another source at your discretion.

Example: Configure Shibboleth to Interoperate with Cisco DMS

Before You Begin

- Obtain a digital identity certificate from a well-known CA, install it on your IdP host system, and then enable SSL.

Procedure

Step 1 Obtain and install Shibboleth.

a. Go to http://www.shibboleth.net/downloads/identity-provider/latest/.

b. Download the latest Identity Provider software package, such as **shibboleth-identityprovider-2.3.0-bin.zip**.

c. Extract the downloaded archive, and then make the installer script within it, named *install.sh*, executable. For example:

```
$ unzip shibboleth-identityprovider-2.3.0-bin.zip
$ cd shibboleth-identityprovider-2.3.0
$ chmod u+x install.sh
```

d. Run the script to install Shibboleth.

```
$ ./install.sh
```

- The installer will prompt you to specify the installation directory. Its default is **/opt/shibboleth-idp**.
- In addition, it will prompt you to enter your Shibboleth system's FQDN, such as **shibboleth.example.com**.

Respond appropriately to these prompts.

Shibboleth is now installed and you have completed its basic configuration. Your new Shibboleth system contains these subfolders.

```
/opt/shibboleth-idp/bin/
/opt/shibboleth-idp/conf/
/opt/shibboleth-idp/credentials/
/opt/shibboleth-idp/lib/
/opt/shibboleth-idp/logs/
/opt/shibboleth-idp/metadata/
/opt/shibboleth-idp/war/
```

Step 2	Export SP metadata from Cisco DMS.	Export metadata from each SP that will participate in your Shibboleth CoT. **Tip** For Cisco DMS, see the "Export SP Metadata from DMM" topic.
Step 3	Import SP metadata from Cisco DMS.	Use SFTP or another method to save imported metadata where Shibboleth will access it: **`/opt/shibboleth-idp/metadata/`**.
Step 4	Log in remotely.	Use SSH, remote desktop, VNC, or a direct console connection to log in remotely to the system where you installed Shibboleth.
Step 5	Edit the attribute filter file.	**a.** Open **/opt/shibboleth-idp/conf/attribute-filter.xml** for editing. **b.** Change the attributeID value (at or near line 24) to **uid**. `<afp:AttributeRule attributeID="uid">`

Step 6	Edit the attribute resolver file.	**a.** Open **/opt/shibboleth-idp/conf/attribute-resolver.xml** for editing.
		b. Find this section:
		`<!- ========== ->`
		`<!- Attribute Definitions ->`
		`<!- ========== ->`
		c. Enter these lines after the Attribute Definitions section heading, at or near line 29.
		`<resolver:AttributeDefinition xsi:type="ad:Simple" id="uid" sourceAttributeID="sAMAccountName">`
		`<resolver:Dependency ref="myLDAP" />`
		`<resolver:AttributeEncoder xsi:type="enc:SAML2String" name="urn:oid:0.9.2342.19200300.100.1.1" friendlyName="uid" />`
		`<resolver:AttributeEncoder xsi:type="enc:SAML2StringNameID" nameFormat="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />`
		`</resolver:AttributeDefinition>`
		d. Find this section:
		`<!- ========== ->`
		`<!- Data Connectors ->`
		`<!- ========== ->`
		e. Enter these lines after the Data Connectors section heading, at or near line 288.
		`<resolver:DataConnector id="myLDAP" xsi:type="dc:LDAPDirectory"`
		`xmlns="urn:mace:shibboleth:2.0:resolver:dc"`
		`ldapURL="ldap://<YOUR_ACTIVE_DIRECTORY_SERVER_IP>"`
		`baseDN="cn=<USERBASE>, dc=<HOSTNAME>, dc=<EXAMPLE>, dc=<COM>"`
		`principal="cn=<ADMINISTRATOR_CN>, cn=<USERBASE>, dc=<HOSTNAME>, dc=<EXAMPLE>, dc=<COM>"`
		`principalCredential="<ADMINISTTRATOR_PASSWORD>">`
		`<dc:FilterTemplate>`
		`<![CDATA[`
		`(sAMAccountName=$requestContext.principalName)`
		`]]>`
		`</dc:FilterTemplate>`
		`<LDAPProperty name="java.naming.referral" value="follow"/>`
		`</resolver:DataConnector>`

Step 7 Edit the handler file.

a. Open **/opt/shibboleth-idp/conf/handler.xml** for editing.

b. Uncomment line 109.

```
<!--  Username/password login handler -->
<ph:LoginHandler xsi:type="ph:UsernamePassword"
jaasConfigurationLocation="file:///opt/shibboleth-idp/conf/login.config">
<ph:AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtect
edTransport</ph:AuthenticationMethod>
</ph:LoginHandler>
```

Step 8 Edit the login config file.

a. Open **/opt/shibboleth-idp/conf/login.config** for editing.

b. Find this string, at or near line 45:

```
};
```

c. Enter this material immediately before **};** .

```
edu.vt.middleware.ldap.jaas.LdapLoginModule optional
ldapUrl="ldap://<YOUR_ACTIVE_DIRECTORY_SERVER_IP>:389"
bindDn="cn=<ADMINISTRATOR_CN>, cn=<USERBASE>, dc=<HOSTNAME>, dc=<EXAMPLE>,
dc=<COM>"
bindCredential="<ADMINISTTRATOR_PASSWORD>"
baseDn="cn=<USERBASE>, dc=<HOSTNAME>, dc=<EXAMPLE>, dc=<COM>"
ssl="false"
tls="false"
userFilter="sAMAccountName={0}";
```

Step 9 Edit the replying party file.

a. Open **/opt/shibboleth-idp/conf/replying-party.xml** for editing.

b. Find this section:

```
<!-- ========================================== -->
<!-           Metadata Configuration             ->
<!-- ========================================== -->
```

c. Enter these lines after the Metadata Configuration section heading, at or near line 123.

```
<metadata:MetadataProvider
id="<HOSTNAME_ONLY_FOR_YOUR_SP>"
xsi:type="FilesystemMetadataProvider"
xmlns="urn:mace:shibboleth:2.0:metadata"
metadataFile="/opt/shibboleth-idp/metadata/<EXPORTED_SP_SETTINGS_FILENAME>.xml"
maintainExpiredMetadata="true"
/>
</metadata:MetadataProvider>
```

Step 10	Prepare your Shibboleth config for use by Cisco DMS.	**a.** Open **/opt/shibboleth-idp/metadata/opt/shibboleth-idp/metadata/Idp-metadata.xml** for editing.
		b. Delete lines 9 through 11.
		`<Extensions>`
		`<shibmd:Scope regexp="false">`*`<EXAMPLE>`*`.`*`<COM>`*`</shibmd:Scope>`
		`</Extensions>`
		c. Delete lines 67 through 69.
		`<Extensions>`
		`<shibmd:Scope regexp="false">`*`<EXAMPLE>`*`.`*`<COM>`*`</shibmd:Scope>`
		`</Extensions>`
		d. Find this string:
		`</IDPSSODescriptor>`
		e. Enter this new binding immediately before **</IDPSSODescriptor>**.
		`<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://`*`<YOUR_SHIBBOLETH_SERVER_FQDN>`***`:8443/idp/profile/SAML2/SOAP/ECP" />`**
		f. Append **:8443** to the end of every FQDN in this file.
		g. Save your edited copy of this file to your local system.
		Be sure to use your Shibboleth hostname in the local filename. For example, you might name this local copy **idp-shibboleth.xml**.

Step 11	Cause Cisco DMS to trust Shibboleth.	See the "Import IdP Metadata into DMM" topic. **Note** Make sure that before importing the IDP_metadata.xml file into the DMM, first remove the *<Extensions></Extensions>* tag.
Step 12	Deploy Shibboleth.	**`cp /opt/shibboleth-idp/war/idp.war /usr/local/tomcat/webapps/`**
Step 13	Test your work.	**a.** Restart Tomcat. **b.** Check for the "OK" message at **http://***<hostname>***:8080/idp/profile/Status**.
Step 14	Stop.	You have completed this procedure.

Example: Configure PingFederate to Interoperate with Cisco DMS

Before You Begin

- Install PingFederate and configure it with at least one Adapter instance to your authentication server, such as LDAP or OAM.

Procedure

Step 1	Export SP metadata from Cisco DMM.	Export metadata from each SP that will participate in your PingFederate CoT. **Tip** For Cisco DMS, see the "Export SP Metadata from DMM" topic.
Step 2	Import SP metadata into PingFederate.	**a.** Log in to PingFederate as its administrator. **b.** Find the SP Connections area in the My IdP Configuration column and click **Create New**. **c.** Click **Do not use a template for this connection** on the *Configuring SP Connection/Connection Template* page, and then click **Next**. **d.** Check the Browser SSO Profiles check box on the *Configuring SP Connection/Connection Type* page, choose **SAML 2.0** from the Protocols list, and then click **Next**. **e.** Check the Browser SSO check box, and then click **Next**. **f.** Click **Choose File** on the *Configuring SP Connection/Import Metadata* page, and then navigate to the SP metadata that you exported from DMS-Admin as **dms_sp_config.xml**. **g.** Click **Open**, and then click **Next** THREE TIMES.

Step 3	Configure SAML profile settings and IdP assertions.	**a.** Click **Configure Browser SSO** on the *Configuring SP Connection/Browser SSO* page. **b.** Check the SP Initiated SSO check box on the *Browser SSO/SAML Profiles* page, and then click **Next** TWO TIMES. **c.** Click **Configure Assertion Creation** on the *Browser SSO/Assertion Creation* page. **d.** Click **Transient** on the *Assertion Creation/Identity Mapping* page, check the Include attributes in addition to the transient identifier check box, and then click **Next**. **e.** Set these attribute-value relationships in the Extend the Contract area on the *Assertion Creation/Attribute Contract* page. • **SAML_AUTHN_CTX** `urn:oasis:names:tc:SAML:2.0:attrname-format:uri` • **UID** `urn:oasis:names:tc:SAML:2.0:attrname-format:uri` • **SAML_NAME_FORMAT** *`urn:oasis:names:tc:SAML:2.0:attrname-format:uri`* **f.** Click **Next**. **g.** Click **Map New Adapter Instance** on the *Assertion Creation/IdP Adapter Mapping* page. **h.** Choose your appropriate authentication type and adapter instance from the next two pages. **i.** Click **Next**. The username attribute that you need next is probably part of the adapter contract. Therefore: **j.** Click **Use only the Adapter Contract values in the SAML assertion** on the *IdP Adapter Mapping/Assertion Mapping* page, and then click **Next**. **k.** On the *IdP Adapter Mapping/Attribute Contract Fulfillment* page: • Set the source to **Text** for the SAML_AUTHN_CTX attribute contract. Then, set its value to `urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport` • Set the source to **Adapter** for the UID attribute contract. Then: – Locate an adapter value, such as **subject** or **userId**, that maps to the username. – Set the UID attribute contract value to match the adapter value that you just found. **l.** Click **Next** > **Done** > **Next** > **Done** > **Next**.
Step 4	Configure protocol settings.	**a.** Click **Configure Protocol Settings** on the *Browser SSO/Protocol Settings* page. **b.** Make sure that the default binding value is set to **POST** on the *Protocol Settings/Assertion Consumer Service URL* page, delete all other bindings, and then click **Next**. **c.** Clear the Artifact check box on the *Protocol Settings/Allowable SAML Bindings* page, and then click **Next**. **d.** Check these check boxes on the *Protocol Settings/Signature Policy* page, and then click **Next**. • Require AuthN requests to be signed when received via the POST or Redirect bindings. • Always sign the SAML Assertion. **e.** Click **None** on the *Protocol Settings/Encryption Policy* page. **f.** Click **Next > Done > Next > Done > Next**.

Step 5	Configure credentials and their digital signatures.	**a.** Click **Configure Credentials** on the *SP Connection/Credentials* page.
		b. Click **Configure** on the *Credentials/Back-Channel Authentication* page.
		c. Check the Use Digital Signatures to guarantee payload in Browser SSO profile check box on the *Back-Channel Authentication/Inbound SOAP Authentication Type* page, and then click **Next**.
		d. Click **Done** on the *Back-Channel Authentication/Summary* page.
		e. Choose the appropriate certificate on the *Credentials/Digital Signature Settings* page, check the Include the certificate in the signature <KeyInfo> Element check box, and then click **Next**.
		f. Click **Manage Signature Verification Settings...** on the *Credentials/Signature Verification Settings* page.
		g. Click **Unanchored** on the *Signature Verification/Trust Model* page, and then click **Next**.
		h. Choose your DMM certificate (example: **dmm.example.com**) from the Primary list on the *Signature Verification/Signature Verification Certificate* page, and then click **Next**.
		Note **DO NOT choose any secondary certificate.**
		
		OR
		
		If the Primary list does not include your DMM certificate, do the following.
		1. Click **Manage Certificates** on the *Signature Verification/Signature Verification Certificate* page.
		2. Click **Choose File** on the *Import Certificate/Import Certificate* page, and then navigate to the X509 digital certificate file (*.cer) that you output from DMM.
		Note **Make sure that your certificate file includes the preamble and postscript that are mandatory for PEM-formatted certificates.** The preamble and postscript look like this.
		
		`-----BEGIN CERTIFICATE-----`
		`-----END CERTIFICATE-----`
		
		3. Click **Open**, and then click **Next** THREE TIMES.
		4. Check the Make this the active certificate check box on the *Import Certificate/Summary* page, and then click **Done**.
		
		i. Click **Done** on the *Certificate Management/Manage Digital Verification Certificates* page.
		j. Click **Next** on the *Signature Verification/Signature Verification Certificate* page.
		k. Click **Done** on the *Signature Verification/Summary* page.
		l. Click **Next** on the *Credentials/Signature Verification Settings* page.
		m. Click **Done** on the *Credentials/Summary* page.
		n. Click **Next** on the *SP Connection* page.

Step 6	Activate and save the new settings.	Set the Connection Status to **Active** on the *SP Connection/Activation & Summary* page, and then click **Save**.
Step 7	Stop.	You have completed this procedure.

Export SP Metadata from DMM

Before you can use Cisco DMS in federation mode, you must export data from DMS-Admin in the form of an SP configuration file. Later, you will import this file into your IdP.

Procedure

Step 1 Make sure that your DMM appliance is running in embedded authentication mode or LDAP mode.

Step 2 Log in as **superuser**.

Step 3 Choose **Administration > Security > Authentication**.

Step 4 Check the Federation check box.

Step 5 Click **Export**.

Step 6 Save the exported file to your client PC or laptop computer as **dms_sp_config.xml**.

Note **See the technical documentation or tutorials for your IdP to understand how it imports SP configuration files.** Alternatively, see the topic for your IdP platform in this chapter's "IdP Configuration Examples" section.

Step 7 Stop. You have completed this procedure.

Related Topics

- Import IdP Metadata into DMM, page 8-39

Import IdP Metadata into DMM

Before you can use Cisco DMS in federation mode, you must export data from your IdP in the form of an IdP configuration file. This topic explains how to use the exported file after you generate and save it.

Before You Begin

- See the technical documentation or tutorials for your IdP to understand how it exports configuration files for an SP (such as DMM) to import. Alternatively, see the topic for your IdP platform this chapter's "IdP Configuration Examples" section.
- Rename the exported IdP configuration file **idp_<type>.xml**. For example:
  - idp_*openam*.xml
  - idp_*shibboleth*.xml
  - idp_*pingfederate*.xml

Procedure

Step 1 Make sure that your DMM appliance is running in embedded authentication mode or LDAP mode.

Step 2 Log in as **superuser**.

Step 3 Choose **Administration > Security > Authentication**.

Step 4 Click **Federation** to choose it as your authentication mode.

Step 5 Click **Import**.

Step 6 Choose and upload the IdP file (**idp_**<type>**.xml**) that you saved previously.

Step 7 Enter the necessary LDAP information to use your Active Directory server.

Step 8 Stop. You have completed this procedure.

Related Topics

- Define LDAP (Active Directory) Filters
- Export SP Metadata from DMM, page 8-39

Bypass External Authentication During Superuser Login, as Needed

Your DMM server features a special login form, **which rejects every username except *superuser***. You use this special form whenever Cisco DMS runs in federation mode or an error has prevented migration from one authentication mode to another.

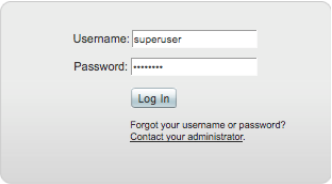
Procedure

Step 1 Go to **http://**<FQDN>**:8080/dmsadmin/admin/login**.

a. Enter **superuser** in the Username field.

b. Enter the corresponding password in the Password field.

c. Click **Log In**.



Step 2 Stop. You have completed this procedure.

Related Topics

- Federation Mode (SSO) FAQs, page 8-65

Configure Active Directory Federation Services for Cisco Show and Share Release 5.3.12

This section describes how to install and configure Active Directory Federation Services (AD FS) 2.0 for use with Cisco Show and Share Release 5.3.12. This section contains the following sections:

- Installing Active Directory Federation Services, page 8-41
- Integrating Active Directory Federation Services with Cisco DMM, page 8-42
- Testing Single Sign On, page 8-49

AD FS 2.0 is a software component that you can install on Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries. It uses a claims-based access control authorization model to maintain application security and implement federated identity.

By enabling AD FS, users can log in to the identity provider (IdP) which is AD FS. After logging in, they can access resources at one or more service providers (known as relying parties) without needing to log in at each service provider (SP). Users can also access system resources by initiating a SP login.

Note The Cisco Show and Share iOS mobile application is not supported when the AD FS feature is enabled in Show and Share Release 5.3.12.

AD FS 2.0 integrates with Active Directory Domain Services, using it as an identity provider. AD FS can interact with other Security Assertion Markup Language (SAML) 2.0-compliant federation services as federation partners.

AD FS 2.0 is a downloadable Windows Server 2008 update that is the successor to AD FS 1.0.

SAML version 2.0 is the standard for cross-domain web single sign-on in the enterprise space. Microsoft introduced SAML support in AD FS version 2.0.

Note Windows Server 2008 R2 includes AD FS 1.0, which does not support SAML 2.0. You need to download the AD FS 2.0 release to web (RTW) package.

Installing Active Directory Federation Services

Follow these steps:

Step 1 Start with Windows Server 2008 (R2) Domain Joined.

Step 2 Create a DNS name for AD FS and point it to your AD FS server. For example, *adfs-bbb.local*.

Step 3 Download and install Active Directory Federation Services 2.0 RTW.

Step 4 In the IIS manager, create a SSL certificate for your DNS name, or use SelfSSL from the IIS 6.0 resource kit to create a self-signed certificate. Bind the SSL certificate with HTTPS port 443.

Step 5 Run the AD FS Server Configuration Wizard to complete the following:

a. **Create a new Federation Service**.

b. Choose **Stand-alone federation server**.

c. **Select the certificate** that you created for your DNS name.

Step 6 Create a service principal name for the DNS name so that Kerberos authentication between the browser and the AD FS IIS instance works correctly:

```
1 setspn -a HOST/adfs-bbb.test.local test\ADFSSVR01
2 setspn -a HOST/adfs-bbb test\ADFSSVR01
```

Step 7 These certificates are automatically generated by the AD FS 2.0 installation process on the AD FS server:

- Service Communication
- AD FS Token Signing
- AD FS Token Encryption

Export the **Service Communication** certificate, name the file *idp01.cer* and save it.

Integrating Active Directory Federation Services with Cisco DMM

To build a federation between two parties you need to establish a trust by exchanging some metadata. The metadata for the AD FS 2.0 instance is entered through the Federation Metadata.xml file into the DMM configuration. The DMM metadata is downloaded as an XML file that is used by AD FS 2.0.

For this configuration, there are two network domains:

- Network A (*https://dmm-aaa.cisco.com*) is the Cisco DMM
- Network B (*https://adfs-bbb.local.cisco.com*) is the Microsoft Active Directory Domain and holds the Identity Provider

SAML 2.0 defines several roles for parties involved in single sign-on:

- Service provider/relying party (DMM)
- Identity provider (AD FS server)
- User that authenticates to access services

This is the process for an IdP-initiated login into dmm.cisco.com:

1. The user authenticates to the AD FS server by using Integrated Windows Authentication (Kerberos tokens over HTTP) and requests login to dmm.cisco.com.
2. AD FS returns a SAML assertion to the user's browser
3. The browser automatically submits the assertion to dmm.cisco.com, which logs the user in.

To integrate AD FS with Cisco DMM, see these sections:

- Configure Active Directory Federation Services, page 8-43
- Add a New Relying Party Trust, page 8-44
- Add a New Rule, page 8-45
- Configure Cisco DMM, page 8-48
- Enable SP-Initiated Login, page 8-49

Configure Active Directory Federation Services

Follow these steps:

Step 1 Generate a template with the Microsoft AD FS server details. You can access a Microsoft AD FS web page to generate XML files. Generate the AD FS output by navigating to:

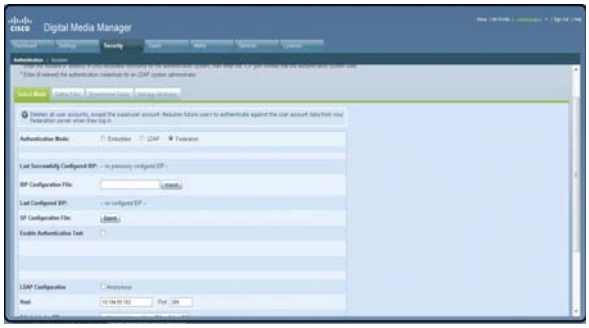
https://<*adfs-bbb.local.cisco.com*>/federationmetadata/2007-06/federationmetadata.xml


```
  <?xml version="1.0" encoding="UTF-8"?>
- <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://adfs.bbb:local.cisco.com/adfs/services/trust" ID="_0fd36f6e-f09d-4
c7e4b92783ba">
  - <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      - <KeyDescriptor use="encryption">
          - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
              - <X509Data>
                    <X509Certificate>MIIC9DCCAdygAwIBAgIQbneqlV0kcIpMauUgD0oLwTANBgkqhkiG9w0BAQsFADA2MTQwMgYDVQQDEytBREZTIEVuY3
                </X509Data>
            </KeyInfo>
        </KeyDescriptor>
      - <KeyDescriptor use="signing">
          - <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
              - <X509Data>
                    <X509Certificate>MIIC7jCCAdagAwIBAgIQMavR8Jfyn4BC3xfkeljQYzANBgkqhkiG9w0BAQsFADAzMTEwLwYDVQQDEyhBREZTIFNpZ25p
                </X509Data>
            </KeyInfo>
        </KeyDescriptor>
        <ArtifactResolutionService index="0" Location="https://adfs.bbb:local.cisco.com/adfs/services/trust/artifactresolution"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
        <SingleLogoutService Location="https://adfs.bbb:local.cisco.com/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
        <SingleLogoutService Location="https://adfs.bbb:local.cisco.com/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
        <SingleSignOnService Location="https://adfs.bbb:local.cisco.com/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
        <SingleSignOnService Location="https://adfs.bbb:local.cisco.com/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        <SingleSignOnService Location="https://dmsperf8-ilo.cisco.com/adfs/ls/" Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"/>
        <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="E-Mail Address" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-f
            Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"/>
        <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Given Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-form
            Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname"/>
        <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri
            Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"/>
```

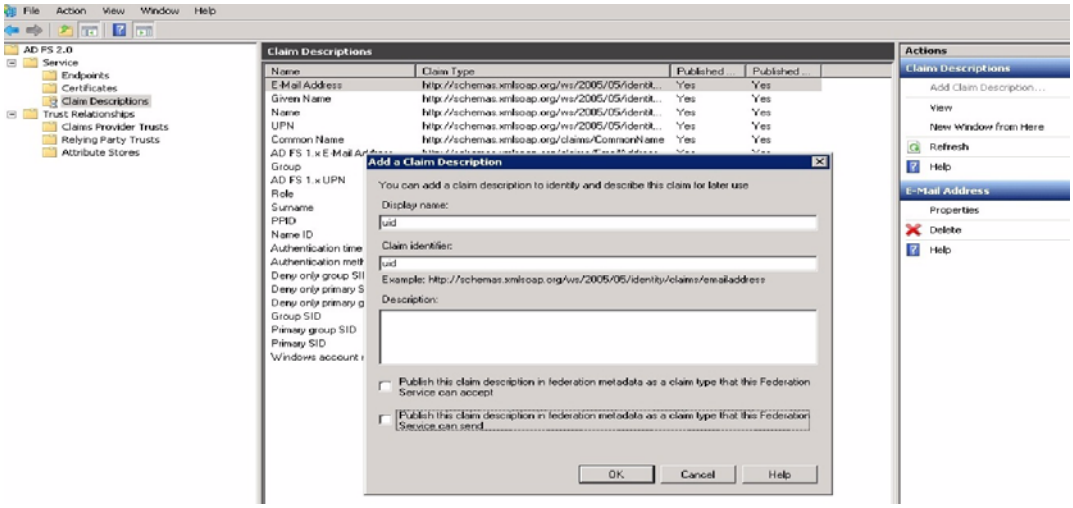

Step 2 (Optional) If using a self-signed certificate, import the Service Communication certificate that was generated by the AD FS server AAI interface. Navigate to **AAI > Certificate Management**. Select **IMPORT_ADFS_CERTS**.

Step 3 Log in to DMM as superuser. Navigate to **Administration > Security > Select Mode**.

Step 4 Click the SP Configuration File **Export** button to export the *dms_config_sp* file.



Step 5 Navigate to **AD FS management console > Service > Claim Description > Add**. In the Claim description and identifier fields, enter **uid**. Click **OK**.



Add a New Relying Party Trust

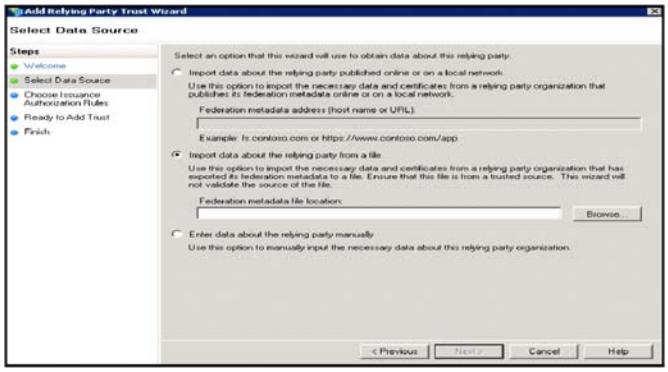
Follow these steps:

Step 1 Click **Add Relying Party Trust** in the Actions window.

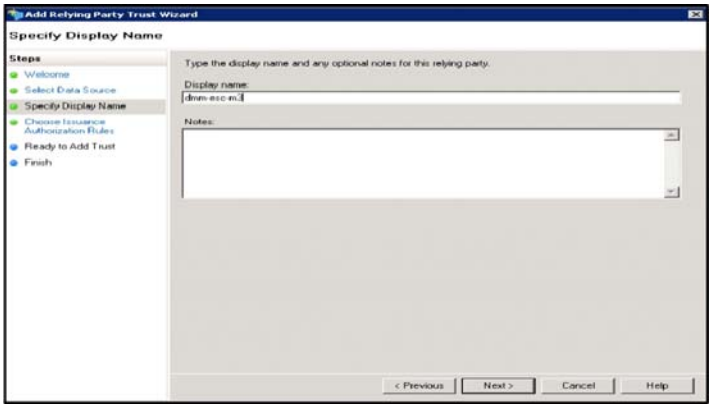
Step 2 In the Overview window, click **Required: add a trusted relying party** to start the setup wizard. Enter these When the welcome screen appears, click **Start**.

Step 3 Run the AD FS Relying Party Trust Wizard to complete the following:

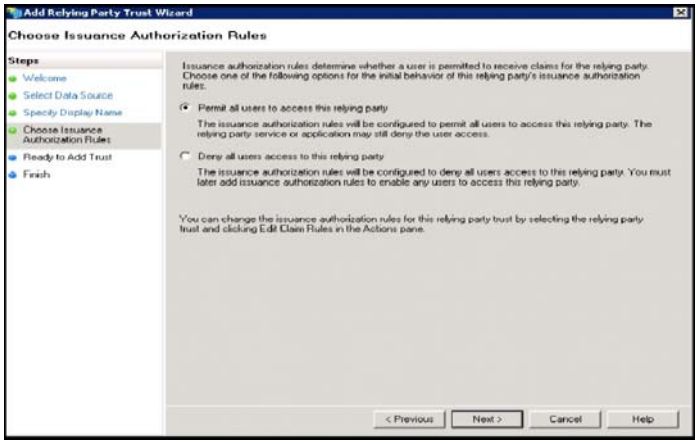
a. Select Data Source: choose **Import data about the relying party from a file** and browse to select the Federation metadata file.



b. Specify Display Name: enter relying party display name.



c. Issuance Authorization Rules: choose **Permit all users to access this relying party**.



Step 4 After importing the metadata, review the following properties:

a. On the Encryption Tab, verify that the encryption Certificate is selected.

b. On the Signature Tab, verify that the signing Certificate is selected.

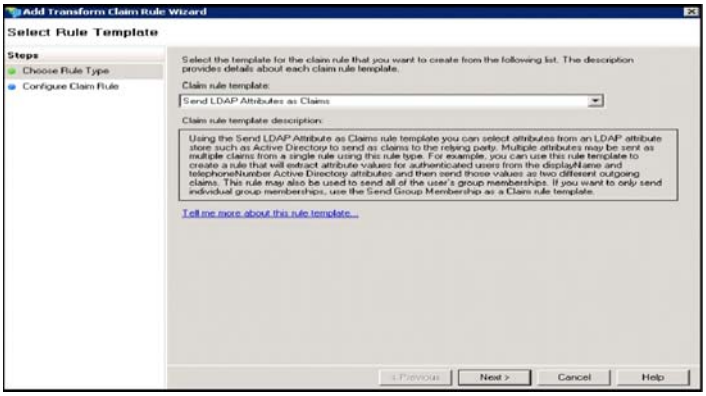
c. On the Advanced Tab, make sure that the SHA1 algorithm is selected.

Add a New Rule

Follow these steps:

Step 1 In the Claim Rules editor select the **Issuance Transform Rules** tab. Click **Add Rule**.

Step 2 In the Choose Rule Type window, choose **Send LDAP Attributes as Claims** in the Claim rules template drop-down list. Click **Next**.



Step 3 In the Edit Rule window:

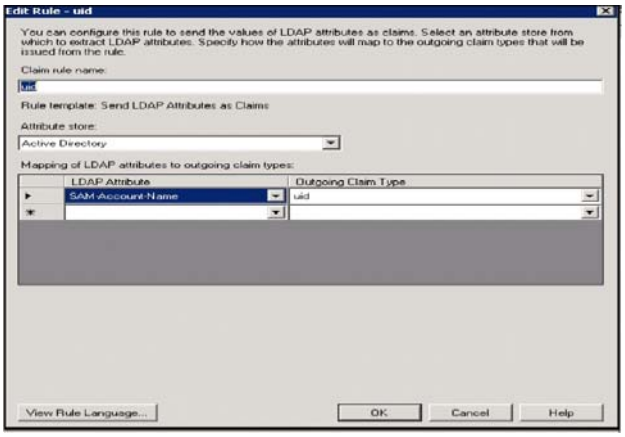
a. Add a Claim Description.

b. Enter **uid** in the Claim rule name field.

c. In the LADP Attribute drop-down list, choose **SAM-Account-Name**.

d. In the Outgoing Claim Type drop-down list, choose **uid**.

e. Click **OK**.



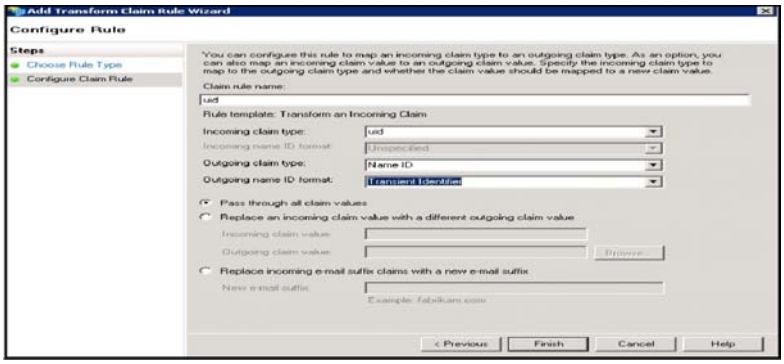
Step 4 In the Claim rule template drop-down list, choose **Transform an Incoming Claim** and click **Next**.

Step 5 In the Configure Claim Rule window:

a. In the Outgoing claim type, choose **NameID**.

b. In the Outgoing name ID format, choose **Transient Identifier**.

c. Click **Finish**.



Step 6 Click **Add Rule**. Choose **Send Claims Using a Custom Rule** and click **Next**. In the Edit Rule window:

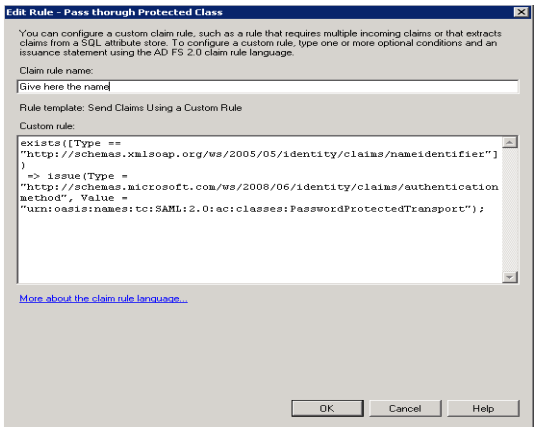
a. Enter the *Claim rule name*.

b. In the Custom Rule area, enter:

exists([Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier"]) => issue (Type = "http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod", Value = "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport");

c. Click **OK**.

Note For the form-based authentication, you need to provide the appropriate value in the relying party response by checking for the presence of *NameID* and then parsing *urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport* in the SAML response.



Configure Cisco DMM

Before you begin:

- Confirm that LDAP is configured.
- Make sure that the DMM Authentication Attribute is set to **minimum** to enable form-based authentication.
- The *SPAuthnContextMapper* is configured for the DMM (Service Provider) and maps the parameters in the incoming HTTP requests to an authentication context. For more information about the *AuthncontextComparisonType* attributes, go to:

  http://docs.oracle.com/cd/E19681-01/820-3748/ggidh/index.html

Follow these steps:

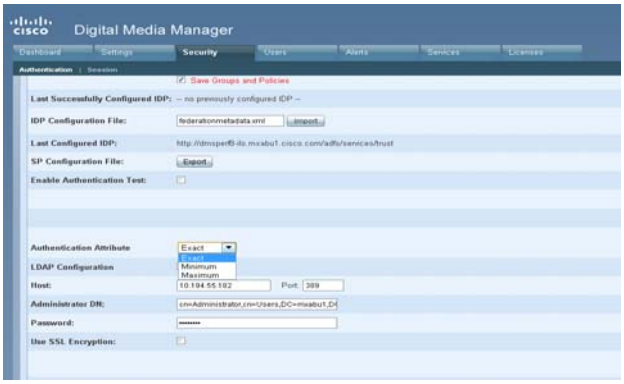
Step 1 Log in to the Cisco DMM as superuser. Navigate to **Administration > Security**.

Step 2 Click the **Save LDAP User Groups and Policies** check box.

Step 3 Import the *federationmetadata.xml* file.

Step 4 Select Authentication Attributes. (The Authentication Attributes option is visible after importing the federationmetadata.xml file.)

Step 5 Click **Update**.



Enable SP-Initiated Login

With identity provider (IdP)-initiated login you will configure a link on the company intranet that users click to access the Cisco DMM. A service provider (SP)-initiated login happens when a user clicks a direct link to Cisco DMM. For SP-initiated login to work, you need to set the AD FS Secure Hash Algorithm parameter to SHA-1. This is because the DMM uses the SHA-1 algorithm when signing SAML requests, and AD FS defaults to SHA-256.

Follow these steps:

Step 1 Log in to DMM as superuser. Navigate to **Relying Party Trust > DMM Properties > Advanced** tab.

Step 2 Set the secure hash algorithm to **SHA1**.

If you do not change the secure hash algorithm, the following message will appear in the AD FS event log:

```
1 Event ID: 378
2 SAML request is not signed with expected signature algorithm. SAML request is signed
with signature algorithm http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 . Expected
signature algorithm is http://www.w3.org/2000/09/xmldsig#rsa-sha1
```

Testing Single Sign On

Before testing the AD FS single sign-on solution, confirm that the user exists in both the AD FS and DMM user database. In the DMM, navigate to in User tab. The user should appear in the DMM user database list.

Testing the Configuration

For an SP-initiated login, you can navigate directly to the entity ID. For example, *https://dmm-aaa.cisco.com*.

For an IdP-initiated login, access *dmm-server.cisco.com* which will navigate to *adfs.aaa.local.cisco.com* and ask for authentication. After logging in to the AD FS server, it will directly navigate to the DMM Administration page.

Follow these steps:

Step 1 Bookmark a link from inside *dmm-aaa.cisco.com* then log out of the system.

Step 2 Reload your browser and select the bookmark. You should be redirected to your IdP, authenticated and then redirected back to the bookmarked link.

If you get an error from AD FS then check the AD FS logs in **Server Manager > Diagnostics > Applications and Services Logs > AD FS 2.0 > Admin**. You can also access *MSDN Claims-Identity blog* for more information about AD FS 2.0 diagnostic tools.

Reference

Software UI and Field Reference Tables

Elements to Choose and Enable an Authentication Mode

Navigation Path

Administration > Security > Authentication > Select Mode

Table 8-1 Elements for Authentication Modes

Element	Description
Authentication Mode Area	
Embedded	Requires users who log in to DMM or Show and Share to authenticate against a user account database that is native to DMM. This database is independent of every other type of authentication that you might use in your network.
LDAP	Automatically deletes all user accounts except ***superuser***. Requires future users to authenticate against the user account data from your Active Directory server when they log in to DMM or Show and Share. Microsoft Active Directory is the only LDAP implementation that we support in this release.
Federation	Automatically deletes all user accounts except ***superuser***. Requires future users to authenticate themselves to your IdP when they log in to DMM or Show and Share.
Federation Mode Elements Area	
Last Successfully Configured IdP	This value becomes populated for the first time after you **succeed** at least once in importing configuration metadata into DMM from your IdP. This element is visible in federation mode only.
IdP Configuration File	Provides the means to import configuration metadata that you previously exported from your IdP and saved to a file. Click **Import** to browse for the file, which you can then import. This element is visible in federation mode only.

Table 8-1 Elements for Authentication Modes (continued)

Element	Description
Last Configured IdP	(CSCtn15472) While it names an IdP explicitly, this value does not necessarily identify the IdP in current use. Instead, this value describes only your most recent *attempt* to import configuration metadata from an IdP, without regard for whether the attempt failed or succeeded. This element is visible only in federation mode. It becomes populated for the first time after you attempt at least once to import IdP metadata. **Tip** **Compare this value to the "Last Successfully Configured IdP" value.** When they differ, you know that your latest such attempt actually failed.
(SP Configuration File) **Export**	Provides the means to export configuration metadata from DMM. Click **Export** to begin browsing for a folder on a locally mounted drive where you can save the exported config file. Later, you will import this file into your IdP. This element is visible in federation mode only.
Enable Authentication Test	Helps you to test whether your federation mode settings are correct and will allow SSO for your ordinary users. Check this check box to expose UI elements that are otherwise hidden. Clear this check box to hide such elements.
Test Username	Enter a username that your IdP already knows. **Do not use the "superuser" username.** This element is visible only while the Enable Authentication Test check box is checked.
Test User Password	Enter the password that corresponds to the test username. This element is visible only while the Enable Authentication Test check box is checked.
LDAP Configuration Area	
Anonymous	Enables or disables an anonymous connection between your DMM appliance and your Active Directory server. • An anonymous connection is suitable when you want to see or use *public* information on the Active Directory server. • In contrast, when you want to see or use *privileged* information on your Active Directory server, the server will require you to enter login credentials to prove that you have sufficient access rights. In the latter case, your Active Directory server will reject any attempt to log in anonymously. This check box is available to you only when you choose LDAP mode or federation mode.
Host	Enter the routable IP address or DNS-resolvable hostname for the Active Directory server. This field is available to you only when you choose LDAP mode or federation mode.
Port	Enter the TCP port number that your Active Directory server uses for communications. This field is available to you only after you choose LDAP mode or federation mode. The Active Directory port number by default is: • **389** for LDAP communications. • **636** for LDAPS (*Secure LDAP*, or *LDAP over SSL*) and SSO communications.

Table 8-1 Elements for Authentication Modes (continued)

Element	Description
Administrator DN	Enter the distinguished name of the Active Directory server administrator. This field is available to you only after you choose LDAP mode or federation mode and uncheck the Anonymous check box. **Tip** **See administrator DN, page 8-3.**
Password	Enter the password that is associated with the Administrator DN. This field is available to you only after you choose LDAP mode or federation mode and uncheck the Anonymous check box.
Use SSL Encryption	The check box to enable or disable encrypted sign-on. This check box is available to you only when you use LDAP mode or federation mode. **Note** **Whenever you enable SSL or install a new SSL certificate for LDAP, you must restart Web Services (Tomcat) from AAI.** Otherwise, LDAP users cannot log in and the new (or newly enabled) SSL certificate cannot take effect. Also—if your DMM server is one half of a failover pair—the Tomcat restart will trigger immediate failover. (CSCtl09696) • Check the check box to enable encryption. • Uncheck it to disable encryption. Enabling SSL causes the connections between your DMM appliance and your Active Directory server to use LDAPS. An LDAPS connection is suitable when you want to prevent untrusted third parties from reading credentials that the servers exchange.
Active Directory Certificate File	Helps you to upload the digital certificate that your Active Directory server uses for LDAPS communications. This field is available to you only while the Use SSL Encryption check box is checked.

Command Buttons

Update	Saves and applies your work on the Authentication Mode property sheet.
Cancel	Discards your work on the Authentication Mode property sheet and resets all values to their previous configuration.

Related Topics

- Choose an Authentication Method, page 8-23
- Elements to Define, Validate, and Add LDAP Filters, page 8-53
- Elements to Use LDAP Bookmarks for Synchronization, page 8-54
- Elements to Manage Attributes, page 8-56

Elements to Define, Validate, and Add LDAP Filters

Navigation Path

Administration > Security > Authentication > Define Filter

Table 8-2 Elements for Filters

Element	Description
Description	Enter a human-readable description for the filter.
User Base DN	Enter the distinguished name of the Active Directory user base that you will search.
User Filter	Enter a user filter to limit the number of matching user accounts to import from the user base that you specified.
User Group (in DMM)	Choose or create a user group to associate with the filter. At the very least, the list includes these options. • All Users Group • Create a New User Group • Digital Signage Users
Command Buttons	
Add	Adds the filter, exactly as entered, without first validating it.
Validate	Validates the filter to confirm, before you add it, that it will return meaningful results.
Clear	Clears all entries from the Define Filters property sheet.

Related Topics

- Choose an Authentication Method, page 8-23
- Elements to Choose and Enable an Authentication Mode, page 8-50
- Elements to Use LDAP Bookmarks for Synchronization, page 8-54
- Elements to Manage Attributes, page 8-56

Elements to Use LDAP Bookmarks for Synchronization

Navigation Path

Administration > Security > Authentication > Synchronize Users

Table 8-3 Elements for Bookmarks

Element	Description
LDAP Bookmarks property sheet	
Synchronization	One of the following types. • Initial • Update • Overwrite • Delete **Note** **When you click Delete on the LDAP Bookmarks sub-tab, we ask you whether to delete groups and policies.** When you choose Yes, we delete all of the following from Cisco DMS. • **All user accounts that match the filter.** • The particular user group that is associated to the filter. • All access policies associated to the particular user group. **The deletion process can take as long as 1 minute to finish.** (CSCtn22370)
Command Buttons	
Update	Submits your selections for the type of synchronization and the scope of access that you chose and configured. Synchronization of the specified type starts immediately.
Cancel	Resets all entries to their previous values on the LDAP Bookmarks property sheet. • Discards all changes to the configuration of behaviors for synchronizations. • Discards all changes to the scope of access.

Related Topics

- Choose an Authentication Method, page 8-23
- Elements to Choose and Enable an Authentication Mode, page 8-50
- Elements to Define, Validate, and Add LDAP Filters, page 8-53
- Elements to Manage Attributes, page 8-56

Elements to Schedule Synchronization

Navigation Path

Administration > Security > Authentication > Synchronize Users

Table 8-4 Elements for Scheduling

Element	Description
Scheduling property sheet	
Synchronization Mode	Enables one synchronization mode to receive updated user account information from an Active Directory server. We support two such modes but they are mutually exclusive. Whenever you enable one, you disable the other. Click either **Manual Synchronization** or **Automatic Synchronization**.
Command Buttons	
Update	Submits your selections for the type of synchronization and the scope of access that you chose and configured. Synchronization of the specified type starts immediately.
Cancel	Resets all entries to their previous values on the Scheduling property sheet. • Discards all changes to the configuration of behaviors for synchronizations. • Discards all changes to the scope of access.

Related Topics

- Configure Automatic LDAP (Active Directory) Synchronization, page 8-27
- Choose an Authentication Method, page 8-23
- Elements to Choose and Enable an Authentication Mode, page 8-50
- Elements to Define, Validate, and Add LDAP Filters, page 8-53
- Elements to Manage Attributes, page 8-56

Elements to Manage Attributes

Navigation Path

Administration > Security > Authentication > Manage Attributes

Table 8-5 Elements for Attributes Management

Element	Description
DMM Attribute Name	Values that DMS-Admin uses to describe and identify various attributes that it associates with each user account. You cannot change the values in this column. They are for your reference only, to help you enter suitable values (and recognize suitable values when you see them) in the LDAP Attribute Name column and the Values to Use by Default column.
LDAP Attribute Name	Values that your Active Directory server uses—which correspond one-to-one with values in the DMM Attribute Row column—to describe and identify attributes of each user account. In its factory-default configuration, DMS-Admin prepopulates all fields in this column with the most commonplace values that Active Directory servers use for this purpose. When the values for these attributes differ on your Active Directory server or when you prefer to import objects that use other Active Directory attributes, you can edit the values in this column.
Values to Use by Default	Enter text to insert automatically when the value is blank for the corresponding attribute in an Active Directory user account that you import or synchronize. To ensure that DMS-Admin imports each valid user account that matches a filter, we recommend that you enter values for these attributes: • First Name • Last Name For your convenience, you can also enter values to insert automatically when the values are blank for other attributes—such as Company, Department, or Phone Number—but this is optional. **Note You cannot enter a value to use by default as the Login User Name value.**
Ignore User Account Control Flags	Tells DMM to ignore whether your Active Directory server makes use of the User Account Control Flags attribute. DMM expects to find this attribute on your Active Directory server and, when the attribute is not present, authentication fails.
Command Buttons	
Reset to Factory Default	Returns all values in the LDAP Attribute Name column to the most commonplace values that Active Directory servers use. If you entered different values manually because the labels for these attributes differ on your Active Directory server or because you prefer to import user accounts that use other Active Directory attributes, DMS-Admin deletes what you entered.
Update	Saves and applies your work in the Manage Attributes property sheet.

Related Topics

- Choose an Authentication Method, page 8-23
- Elements to Choose and Enable an Authentication Mode, page 8-50
- Elements to Define, Validate, and Add LDAP Filters, page 8-53
- Elements to Use LDAP Bookmarks for Synchronization, page 8-54

Sample SP Configuration File from DMM


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!--
 !            DMS SAML2 Service Provider Metadata
 !
 !   Actual Service Provider configuration for the IDP will be instantiated
 !   from this template and be deposited onto the IDP.
 !      (Auto-generated on/at: Wed May 11 16:58:14 PDT 2011)
 !
 !           Copyright (c) 2011 Cisco Systems, Inc.
 !-->
<EntityDescriptor entityID="http://DMMSP.example.com:8080/opensso"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
    <SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">

     <KeyDescriptor>
       <ds:KeyInfo>
         <ds:KeyName>tomcat</ds:KeyName>
         <ds:X509Data>

<ds:X509SubjectName>/C=US/ST=CA/L=SJ/O=CISCO/OU=CISCO/CN=DMMSP.example.com</ds:X509Subject
Name>
           <ds:X509IssuerSerial>
             <ds:X509IssuerName>DMMSP.example.com</ds:X509IssuerName>
             <ds:X509SerialNumber>1304558251</ds:X509SerialNumber>
           </ds:X509IssuerSerial>

<ds:X509Certificate>Mk6g1VAwAIGUk0QTNwaEzqUECAczVzAMCSDsUIgAQELICqwFQhOABhGJiQwgBBYCkAHAIB
9DGMQE COBEcGAAT0Qg4wBBMMVTzVzC1DEQAM8KlAQVKNDwDMBGF0TxWJACA0YNENgQxCSADEVNlQUwQxDV
BDbAQ0M8pvGTNUFyMtzwTYxTAMVTMMAxx3EMLEcTDDFMvzNEmwcTMNco2LmhgTVw2MTaMAmvx1ALMOQADBkjVwACMB
GNTh0F1BQVJJQAAUM1BSDQwTHAsxAVgMlNMjTCVEQEEgzCwEUCAAQxh8Y0GkMMBZZgTwSVNX0EUBglbgRvgwJrADA5
QYF32B9PNQEBVJANQIBb5K8YwNUQNYo0aQDjDJyMbhjswjcDgAM0IYJIoAGAGBr/qw1adeTiX6wNGwl+Pn2rhopPL7
cCzUI2aNCNyK+D99sLujKL/kjyCBZ9lqKPeCArxWfKycC3/QqgO/SNz33b8JSh6iG35kVwA3OMZplEtLX4CfBkdsXY
TVaKIRPRLMSOH9u9vH6ELFgSzl8dH/tL1o3aJADhnG4gcFA8tGE8QIXZBdBQdNwlDYj1AAAARYsKS6wV2vCZEgTNEI
MAQbvD A87sb03cvDpQUCJ5SQ0O/ 4xQA531HhBHSCDOFbUlq+ PeTKB4dkGsIst9BPaIr43bWO3zfkMbrU2A WNu+
dPcBZpO1raWmP2I8ZErlDYPJSEstzmaC30kkeXg4nfe10KCx1QH8BAQusegy38+ oh8NLYw3N dzQl5vs=
</ds:X509Certificate>
         </ds:X509Data>
       </ds:KeyInfo>
     </KeyDescriptor>

     <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://DMMSP.example.com:8080/opensso/SPSloRedirect/metaAlias/sp"
ResponseLocation="http://DMMSP.example.com:8080/opensso/SPSloRedirect/metaAlias/sp"/>
     <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://DMMSP.example.com:8080/opensso/SPSloPOST/metaAlias/sp"
ResponseLocation="http://DMMSP.example.com:8080/opensso/SPSloPOST/metaAlias/sp"/>
     <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://DMMSP.example.com:8080/opensso/SPSloSoap/metaAlias/sp"/>
     <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://DMMSP.example.com:8080/opensso/SPMniRedirect/metaAlias/sp"
ResponseLocation="http://DMMSP.example.com:8080/opensso/SPMniRedirect/metaAlias/sp"/>
     <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://DMMSP.example.com:8080/opensso/SPMniPOST/metaAlias/sp"
ResponseLocation="http://DMMSP.example.com:8080/opensso/SPMniPOST/metaAlias/sp"/>
     <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://DMMSP.example.com:8080/opensso/SPMniSoap/metaAlias/sp"
ResponseLocation="http://DMMSP.example.com:8080/opensso/SPMniSoap/metaAlias/sp"/>
     <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
     <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
```

```
     <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>

<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</NameID
Format>
     <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</NameIDFormat>

<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</NameIDFormat>
     <AssertionConsumerService index="0" isDefault="true"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://DMMSP.example.com:8080/opensso/Consumer/metaAlias/sp"/>
     <AssertionConsumerService index="1"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact"
Location="http://DMMSP.example.com:8080/opensso/Consumer/metaAlias/sp"/>
     <AssertionConsumerService index="2"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:PAOS"
Location="http://DMMSP.example.com:8080/opensso/Consumer/ECP/metaAlias/sp"/>
    </SPSSODescriptor>
</EntityDescriptor>
```

Summary Configuration Sample (PingFederate)

SP Connection

Connection Type	*Connection Role:*	**SP**
	Browser SSO Profiles:	**true**
	Protocol:	**SAML 2.0**
	Connection Template:	**No Template**
	WS-Trust STS:	**false**
Connection Options	*Browser SSO:*	**true**
	Attribute Query:	**false**
	SaaS Provisioning:	**false**
General Info	*Partner's Entity ID (Connection ID):*	**http://example.cisco.com:8080/opensso**

Browser SSO

SAML Profiles	*IdP-Initiated SSO:*	**false**
	IdP-Initiated SLO:	**false**
	SP-Initiated SSO:	**true**
	SP-Initiated SLO:	**false**

Assertion Lifetime	*Assertion Minutes Before:*	**5**
	Assertion Minutes After:	**5**

Assertion Creation

Identity Mapping	*Enable Transient Identifier:*	**true**
	Include additional attributes:	**true**
Attribute Contract	*Attribute:*	**SAML_AUTHN_CTX**
	Attribute:	**UID**
	Attribute:	**SAML_NAME_FORMAT**
IdP Adapter Mapping	*Adapter instance name:*	**LDAP** [1]
Authentication Type	*Authentication Type:*	**Single-Factor Authentication**
Adapter Instance	*Selected adapter:*	**LDAP** [1]
Assertion Mapping	*Adapter:*	**LDAP Authentication Service 2.2**
	Data Store or Assertion:	**Use only the Adapter Contract values in the SAML assertion**
Attribute Contract Fulfillment	*SAML_AUTHN_CTX:*	**urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport (Text)**
	UID:	**subject**[2] **(Adapter)**

Protocol Settings

Assertion Consumer Service URL	*Endpoint URL:*	**https://example.cisco.com:8443/opensso/Consumer/metaAlias/sp (POST)**

Allowable SAML Bindings	*Artifact:*	**false**
	POST:	**true**
	Redirect:	**true**
	SOAP:	**true**

Protocol Settings

Signature Policy	*Require digitally signed AuthN requests:*	**true**
	Always sign the SAML Assertion:	**true**
Encryption Policy	*Status:*	**Inactive**

Credentials

Inbound SOAP Authentication Type	*SOAP Authentication Type:*	**Use Digital Signatures to guarantee payload in Browser SSO profile**
	SSL required:	**true**
Digital Signature Settings	*Selected Certificate:*	**CN=**<your_organization>**,** **O=**<your_department>**,** **L=**<your_city_or_village>**,** **ST=**<your_state_or_province>**,** **C=**<your_country>
	Include Certificate in KeyInfo:	**true**
	Selected Signing Algorithm:	**RSA SHA1**

Signature Verification

Trust Model	*Trust Model:*	**Unanchored**
Signature Verification Certificate	*Selected Certificate:*	**CN=**<*FQDN_of_your_DMM_SP*>**,** **OU=**<*your_organization*>**,** **O=**<*your_department*>**,** **L=**<*your_city_or village*>**,** **ST=**<*your_state_or_province*>**,** **C=**<*your_country*>

1. Although we use this name value in our testbed, you might use some other name.
2. “Sample” is merely an example.

Sample IdP Metadata

Exported IdP Metadata Sample from OpenAM


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="dmsIdp" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
    <IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
MJEwVFggTTQ1MUwD9w0kQACIQNICQQWBGBYlAqqAMBGUzAwAEkVsiagAELKkCBkDCADdhAUIQIGE
CYABEMTxwVzNBKQlNQZDMAlNCEQ1ADJzAKC0E4QgQSBExwGGVwzM0AAgQOVDUDT0A8cCNTxMFBVV
BxxjNambbJAQRbThnMxjlMNFYMm8cpT2mDovLMTvENv4pAJIw2yNDRAYDMMTAG0wOyET3MLExgMw
ZEMAAVk80JDVMVT1TSghThEMxBwjAU1zkwFMYEODCAQgH0MGQQGAJCNLEUNBQEBsCCBAwQVMlQAx
DGgwkJ5EAY9vMADP2y0NbJIQo0jV5RaXw8YbsQsTVQDjx5ZNKNZaUgMBByUDjhcYjN2wJBSWQ0bNABmAo2eD4JQ1QA
hEVyPDgAQEMZBUIAtNdgrxA0BcYIB9QuG4aWYHGX/ LcxHcYOES0MIYciud6KmI+/ kq/ YpRbA30QYctD0uax/
0M7BUD/SMT+P1kQhA9dCLiOeu2WB2dKFWWOwcLIhgne7omCI+ozijrImy+4C3fz9zC/VrBA3bQZMcnsE6YbZJDC7Ih
AjNAEAoQNZ5gGAKxBYEABzXjgAQwcDpvFYK1yNqr wArSlA7b3Vkhn42iQVjvj8I3No2ssay4LZyBsffkrm+
gATatC/ HvyyNGoapGS9K4fLZNzBaXDW99/ 728x7bGciRWFdx4VOdPABkis+ a1Had9Blj8uCupvRp/ wkRkP+
6hldOYEWQyVmrwid02g3S5Gtb+ ErQO7KA5G1wKvrw=
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>
        <ArtifactResolutionService index="0" isDefault="true"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://OpenAM.example.com:8080/opensso/ArtifactResolver/metaAlias/idp"/>
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://OpenAM.example.com:8080/opensso/IDPSloRedirect/metaAlias/idp"
ResponseLocation="http://OpenAM.example.com:8080/opensso/IDPSloRedirect/metaAlias/idp"/>
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://OpenAM.example.com:8080/opensso/IDPSloPOST/metaAlias/idp"
ResponseLocation="http://OpenAM.example.com:8080/opensso/IDPSloPOST/metaAlias/idp"/>
        <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://OpenAM.example.com:8080/opensso/IDPSloSoap/metaAlias/idp"/>
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://OpenAM.example.com:8080/opensso/IDPMniRedirect/metaAlias/idp"
ResponseLocation="http://OpenAM.example.com:8080/opensso/IDPMniRedirect/metaAlias/idp"/>
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://OpenAM.example.com:8080/opensso/IDPMniPOST/metaAlias/idp"
ResponseLocation="http://OpenAM.example.com:8080/opensso/IDPMniPOST/metaAlias/idp"/>
        <ManageNameIDService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://OpenAM.example.com:8080/opensso/IDPMniSoap/metaAlias/idp"/>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>

<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>

<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</NameID
Format>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</NameIDFormat>

<NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</NameIDFormat>
```

```
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="http://OpenAM.example.com:8080/opensso/SSORedirect/metaAlias/idp"/>
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="http://OpenAM.example.com:8080/opensso/SSOPOST/metaAlias/idp"/>
        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://OpenAM.example.com:8080/opensso/SSOSoap/metaAlias/idp"/>
        <NameIDMappingService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://OpenAM.example.com:8080/opensso/NIMSoap/metaAlias/idp"/>
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="http://OpenAM.example.com:8080/opensso/AIDReqSoap/IDPRole/metaAlias/idp"/>
        <AssertionIDRequestService Binding="urn:oasis:names:tc:SAML:2.0:bindings:URI"
Location="http://OpenAM.example.com:8080/opensso/AIDReqUri/IDPRole/metaAlias/idp"/>
    </IDPSSODescriptor>
</EntityDescriptor>
```

Exported IdP Metadata Sample from Shibboleth

```
<EntityDescriptor entityID="https://sso.example.com/idp/shibboleth"
                  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
                  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
                  xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

    <IDPSSODescriptor protocolSupportEnumeration="urn:mace:shibboleth:1.0
urn:oasis:names:tc:SAML:1.1:protocol urn:oasis:names:tc:SAML:2.0:protocol">

        <KeyDescriptor>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>
MIICRTCCAa6gAwIBAgIETOrk+jANBgkqhkiG9w0BAQUFADBmMQswCQYDVQQGEwJVUzELMAkGA1UE
CBMCQ0ExCzAJBgNVBAcTAlNKMQ4wDAYDVQQKEwVDSVNDTzEOMAwGA1UECxMFQ0lTQ08xHTAbBgNV
BAMTFGZydWl0bG9vcHMuY2lzY28uY29tMCAXDTEwMTEyMjIxNDczOFoYDzIxMTAxMDI5MjE0NzM4
WjBmMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExCzAJBgNVBAcTAlNKMQ4wDAYDVQQKEwVDSVND
TzEOMAwGA1UECxMFQ0lTQ08xHTAbBgNVBAMTFGZydWl0bG9vcHMuY2lzY28uY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCX0tTliXR7pGh9NNEKbIkChNB0t/H+2ysm4xr1Y60+hFssJGGx
qnNv8UEqH7SIk7Z9eDBW6lJreiH3KtSWIJBvtV1hLGZAlwPTu/b6GzVHGX9uZaj3Jyw0N8ru18k8
BoTsdNag7ZhQ7vIfcQ1HjLw9RT3u+n5ZkD+hbwEKtKePEwIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
AA932Gf5lEY1c3w/ALuEXiDdtLnzRrNZxF7ZneDPfnjygNMOLgYTwCARdjdW40Xurd2RGSJC3MYJ
bhqMIStSTbYPBB6KLuEWkk+AW+/uprX5T49SY6hS918tcErmWdW0CYFlIiRa2hMaJz6AbWAqKR80
+n5IWxwEOlkmOPdWd1B/
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>

        <ArtifactResolutionService
Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"

Location="http://sso.example.com:8080/idp/profile/SAML1/SOAP/ArtifactResolution"
                                  index="1"/>

        <ArtifactResolutionService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

Location="http://sso.example.com:8080/idp/profile/SAML2/SOAP/ArtifactResolution"
                                  index="2"/>

        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>

        <SingleSignOnService Binding="urn:mace:shibboleth:1.0:profiles:AuthnRequest"
```

```
Location="http://sso.example.com:8080/idp/profile/Shibboleth/SSO" />

        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"

Location="http://sso.example.com:8080/idp/profile/SAML2/POST/SSO" />

        <SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"

Location="http://sso.example.com:8080/idp/profile/SAML2/POST-SimpleSign/SSO" />

        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"

Location="http://sso.example.com:8080/idp/profile/SAML2/Redirect/SSO" />

        <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

Location="http://sso.example.com:8080/idp/profile/SAML2/SOAP/SSO"/>

    </IDPSSODescriptor>

    <AttributeAuthorityDescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:1.1:protocol
urn:oasis:names:tc:SAML:2.0:protocol">

        <KeyDescriptor>
            <ds:KeyInfo>
                <ds:X509Data>
                    <ds:X509Certificate>
MIICRTCCAa6gAwIBAgIETOrk+jANBgkqhkiG9w0BAQUFADBmMQswCQYDVQQGEwJVUzELMAkGA1UE
CBMCQ0ExCzAJBgNVBAcTAlNKMQ4wDAYDVQQKEwVDSVNDTzEOMAwGA1UECxMFQ0lTQ08xHTAbBgNV
BAMTFGZydWl0bG9vcHMuY2lzY28uY29tMCAXDTEwMTEyMjIxNDczOFoYDzIxMTAxMDI5MjE0NzM4
WjBmMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExCzAJBgNVBAcTAlNKMQ4wDAYDVQQKEwVDSVND
TzEOMAwGA1UECxMFQ0lTQ08xHTAbBgNVBAMTFGZydWl0bG9vcHMuY2lzY28uY29tMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCX0tTliXR7pGh9NNEKbIkChNB0t/H+2ysm4xr1Y60+hFssJGGx
qnNv8UEqH7SIk7Z9eDBW6lJreiH3KtSWIJBvtV1hLGZAlwPTu/b6GzVHGX9uZaj3Jyw0N8rul8k8
BoTsdNag7ZhQ7vIfcQ1HjLw9RT3u+n5ZkD+hbwEKtKePEwIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
AA932Gf5lEY1c3w/ALuEXiDdtLnzRrNZxF7ZneDPfnjygNMOLgYTwCARdjdW40Xurd2RGSJC3MYJ
bhqMIStSTbYPBB6KLuEWkk+AW+/uprX5T49SY6hS918tcErmWdW0CYFlIiRa2hMaJz6AbWAqKR80
+n5IWxwEOlkmOPdWd1B/
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </KeyDescriptor>

        <AttributeService Binding="urn:oasis:names:tc:SAML:1.0:bindings:SOAP-binding"

Location="http://sso.example.com:8080/idp/profile/SAML1/SOAP/AttributeQuery" />

        <AttributeService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"

Location="http://sso.example.com:8080/idp/profile/SAML2/SOAP/AttributeQuery" />

        <NameIDFormat>urn:mace:shibboleth:1.0:nameIdentifier</NameIDFormat>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>

    </AttributeAuthorityDescriptor>

</EntityDescriptor>
```

Exported IdP Metadata Sample from PingFederate


```
<md:EntityDescriptor entityID="saml2" cacheDuration="PT1440M"
    ID="OUEOtB9WV9lj-tGu57Lzdbwmah." xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
    <md:IDPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:KeyDescriptor use="signing">
            <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:X509Data>
                    <ds:X509Certificate>
                        MIICUzAgI0xCzAJBgNVGATL3DQEBBQUA6reRuMA0GCSqGSIbCCAbygAwIBMGBAYTAl
                        VTMRMwEQYDVQQIEwpDYWxpZm9ybmlhMREwDwYDVQQHEwhTYW4gSm9zZTEeMBwGA1UE
                        ChMVRGln0ZW1zMRYwFAYaNZWRpYSBTeXNDVQQXRhbCBDEw1DaXNjbyBTeXN0ZW1zMB
                        4XDTExMTAxMzAwMjgxMloXDTEyMTAxMjAwMjgxMlowbTELMAkGA1UEBhMCVVMxEzAR
                        BgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMR4wHAYDVQQKExVEaW
                        dpdGFsIE1lZGlhIFN5c3RlbXMxFjAUBgNVBAMTDUNpc2NvIFN5c3RlbXMwgZ8wDQYJ
                        KoZIhvJAoGBALaYHMXD2DcNAQEBBQADgY0AMIGrFA+B1GubRCQIsqtpv0sHHdmLiJ8
                        CpuGtIgpHGBYHyKhPPS506YUbpduEViHM4MAqO0c0TKG8JCdhpXgoHI+/suo6zgkm6
                        x6UOZsW36+FxlUOgO4hsGG3rpNtgkLSd4YrnlwVCdb0FPgsvE58zbptosAQKF5R8iq
                        NLAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAedOWz2UZctWwUxSVhTZ1pE39wDTaf40X
                        0yN9vZiV2O3naP7rwkwles1svozpz5Cw/GJITznvRM2ez3agYaOsnz4FuDARjv3/cz
                        SED+6uMlv8xsk6gQ1zD3dJmyN2bJL/ENc+6bw8jepPGzyZBv+GwJwLeobKTgcCUI6X
                        1rIDn1U=
                    </ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </md:KeyDescriptor>

<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
        <md:SingleSignOnService
            Location="https://idp.example.com:9031/idp/SSO.saml2"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
        <md:SingleSignOnService
            Location="https://idp.example.com:9031/idp/SSO.saml2"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" />
        <md:SingleSignOnService
            Location="https://idp.example.com:9031/idp/SSO.saml2"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" />
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="SAML_AUTHN_CTX" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" />
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="UID" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" />
        <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="SAML_NAME_FORMAT" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" />
    </md:IDPSSODescriptor>
</md:EntityDescriptor>
```


FAQs and Troubleshooting

LDAP (Active Directory) FAQs

Q. Which Active Directory releases does Cisco DMS support?

A. Our completed tests succeeded as follows.

Windows Active Directory Server 2000

- Cisco DMS 5.3

Windows Active Directory Server 2003

- Cisco DMS 5.3

Windows Active Directory Server 2008R2

- Cisco DMS 5.3

Federation Mode (SSO) FAQs

Q. Are there any special APIs to use federation mode?

A. No. We support one set of API calls that work identically across all supported authentication modes. See http://developer.cisco.com.

Q. Does DMM perform trust validation of certificates that it imports with IdP metadata?

A. Yes.

Q. Do you support any use of certificate revocation lists?

A. No. Not in this release.

Q. Can I use one browser to connect simultaneously to more than one DMM appliance or more than one Show and Share appliance?

A. No. Each time that you connect to an additional instance, you are logged out of any prior instance in that browser. However, you can use multiple browsers together for this purpose.

Q. Why would user sessions time out for Show and Share or DMM users after a different interval than I set in DMM?

A. This can happen when session timeout values differ between your DMM appliance and your IdP. Reconfigure these servers to share one identical session timeout value.

Error Message FAQs

Q. Why does an error message state that an Active Directory password is not valid?

Explanation A "User must change password at next login" flag might be set on your Active Directory server. While this flag is set, the affected user cannot log in to any Cisco DMS component. DMS-Admin cannot change any password on your Active Directory server.

Recommended Action Use features that your Active Directory server provides for this purpose.

Q. Why does an error message state that filter validation has failed?

Explanation Filters fail when they point to empty containers. They also fail in response to filter expressions that includes any spaces.

Recommended Action Make sure on your Active Directory server that your filter did not refer to an empty organizational unit (OU) container. **Confirm also that your filter expression does not contain even one space.**

Q. Why would my API calls receive an HTTP 401 Unauthorized error?

Recommended Action When you use federation mode, enable ECP on your IdP server.

Network Policy FAQs

Q. When I use LDAP authentication with Cisco DMS, which ports must remain open in my network?

A. Your DMM appliance accepts user authentication requests securely through **port 443**. DMM then passes these requests securely to your Active Directory server through **port 389**. Also, SSL uses **port 636**.

User Exclusion FAQs

Q. Can I block Cisco DMS access to one particular Active Directory user account, when it is among the matched results for an otherwise useful LDAP filter?

A. Yes. Extend your query to include a logical NOT (`!`) operator for an attribute whose value is unique to this user. This example uses the LDAP "`samAccountName`" attribute name, which DMM uses by default to populate the corresponding login name for DMM. However, if your Active Directory server uses any other attribute name than "`samAccountName`" for this purpose, you must update the example syntax accordingly when you extend your query.

```
(&(currentFilter)(samAccountName!=username-to-be-excluded))
```

Tip **Information on the Manage Attributes property sheet in DMS-Admin confirms whether your Active Directory server uses the "`samAccountName`" attribute name.**