



# Authentication and Federated Identity

Revised: May 13, 2015  
OL-15762-03

- [Concepts, page 7-1](#)
- [Procedures, page 7-21](#)
- [Reference, page 7-31](#)



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.



Note

This material pertains to multiple releases of Cisco DMS.

5.2.0

5.2.1

5.2.2

5.2.3

## Concepts

- [Overview, page 7-2](#)
- [Glossary, page 7-2](#)
- [Understand the Requirement to Authenticate Users, page 7-9](#)
- [Decide Which Authentication Method to Use, page 7-10](#)
- [LDAP and Active Directory Concepts, page 7-10](#)
- [Federated Identity and Single Sign-on \(SSO\) Concepts, page 7-17](#)
- [Migration Between Authentication Methods, page 7-20](#)

## Overview

User authentication features of DMS-Admin help you to:

- **NEW IN CISCO DMS 5.2.0**—Authenticate **all** user sessions. *We now 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.
- **NEW IN CISCO DMS 5.2.1**—Synchronize user groups from an [Active Directory](#) server.
- **NEW IN CISCO DMS 5.2.3**—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 5.2.3.**

---

## Glossary



Timesaver

---

Go to terms that start with... [ [A](#) | [C](#) | [D](#) | [F](#) | [I](#) | [L](#) | [O](#) | [R](#) | [S](#) | [U](#) | [X](#) ].

---

### A

#### Active Directory

Microsoft implementation of [LDAP](#). A central authentication server and user store.

#### Active Directory forest

A domain-straddling combination of [Active Directory trees](#) within an organization that operates multiple Internet domains. Thus, the forest at “Amalgamated Example, 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** This Cisco DMS release does not support Active Directory forests.

#### 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](#)

**administrator DN** The [DN](#) to authenticate your [Active Directory](#) server's administrator.

**Note** **NEW IN CISCO DMS 5.2.3**—This release is more strict than any prior release 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 5.2.3, 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 5.2.3, 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** **NEW IN CISCO DMS 5.2.3**—*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.

**Note** A DN can 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**

**NEW IN CISCO DMS 5.2.3**—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

**NEW IN CISCO DMS 5.2.3**—*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.

**Note** **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](#) 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.

## 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

**NEW IN CISCO DMS 5.2.3**—**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.

## 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

**NEW IN CISCO DMS 5.2.3**—*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

**NEW IN CISCO DMS 5.2.3**—A **SAML 2.0**-compliant architecture for federated identity-based authentication and authorization.

## SP

**NEW IN CISCO DMS 5.2.3**—*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

**NEW IN CISCO DMS 5.2.3**—*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 5.2.3.
- We support only **SP-initiated SSO** in Cisco DMS 5.2.3.

**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.

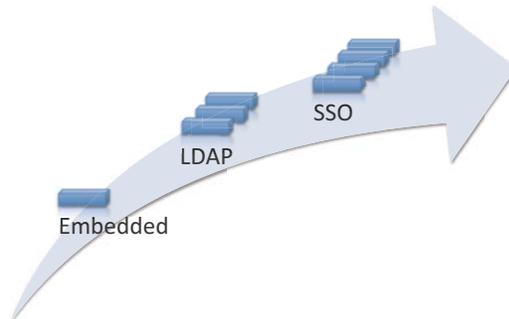
**Note** An LDAP expression must never include a space immediately to either side of a “=” sign. Similarly, it must never include a space immediately to either side of an “objectClass” attribute. Nor can a group name include any spaces. Otherwise, validation fails.

**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.
- **NEW IN CISCO DMS 5.2.3**—*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.**
- **An unresponsive Active Directory server can hang a login prompt for 20 minutes without any error message.**

### EMBEDDED MODE

### LDAP MODE

### FEDERATION (SSO) MODE<sup>1</sup>



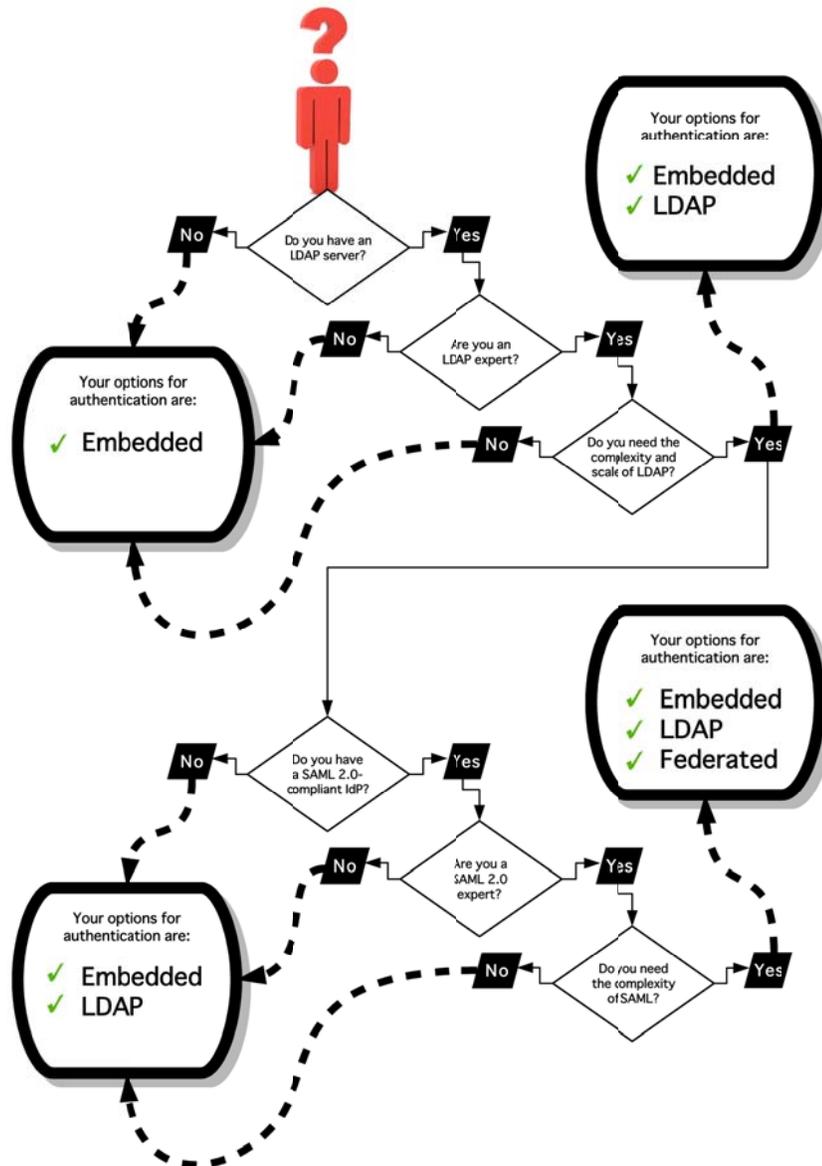
IdP-specific login screen  
(**NEW IN CISCO DMS 5.2.3**)

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 7-10](#)
- [Federated Identity and Single Sign-on \(SSO\) Concepts, page 7-17](#)

## Decide Which Authentication Method to Use



## LDAP and Active Directory Concepts

- [LDAP is Highly Complex, page 7-11](#)
- [Plan Ahead, page 7-11](#)
- [Restrictions, page 7-11](#)
- [Synchronization Concepts, page 7-11](#)
- [LDAP Concepts, page 7-14](#)
- [Password Concepts, page 7-16](#)
- [Understand Authentication Property Sheets for LDAP, page 7-16](#)

## 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
5.2.0	Yes	No
5.2.1	Yes	No
5.2.2	Yes	No
5.2.3	Yes	No

## Synchronization Concepts

- [Synchronization \(Replication\) Overview, page 7-12](#)
- [Synchronization Types, page 7-12](#)
- [Understand Manual Synchronization, page 7-13](#)
- [Understand Automatic Synchronization, page 7-13](#)
- [Guidelines for Synchronization, page 7-14](#)

## Synchronization (Replication) Overview

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

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 <a href="#">Active Directory</a> filter and your local copy of those user accounts.	Overwrites your local copy of user accounts that correspond to your <a href="#">Active Directory</a> filter with new copies of those user accounts. In addition, deletes your local copy of each user account that has been deleted from <a href="#">Active Directory</a> since the last time that you ran a synchronization.	Deletes your local copy of user accounts that correspond to a defined <a href="#">Active Directory</a> filter and deletes the entry for that filter from DMS-Admin.

## Understand Synchronization of a DMM Group to an LDAP Filter

### NEW IN CISCO DMS 5.2.1

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

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



Note

Manual synchronization mode deletes your schedule for automatic synchronizations.

## Understand Automatic Synchronization

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.



Tip

See the "[Understand Synchronization of a DMM Group to an LDAP Filter](#)" section on page 7-13.

## Guidelines for Synchronization

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 <i>Initial</i> option is CPU-intensive for your DMM appliance and might lower performance temporarily. We recommend that you use it during <i>off-peak</i> hours only.
Update	We recommend that you use the <i>Update</i> option whenever: <ul style="list-style-type: none"> <li>• A new user account in <a href="#">Active Directory</a> should have login access to DMM or Show and Share.</li> <li>• User attributes<sup>1</sup> change in <a href="#">Active Directory</a> for a user account in DMM or Show and Share.</li> <li>• A user account is disabled in <a href="#">Active Directory</a> and should be deleted from DMM and Show and Share.</li> </ul>
Overwrite	<p><b>Note</b> The <i>Overwrite</i> 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.</p> <ul style="list-style-type: none"> <li>• After a user account is deleted from <a href="#">Active Directory</a>, this option deletes the corresponding user account from DMM and Show and Share.</li> <li>• After a user account is associated to a new first name, last name, or username, this option overwrites the outdated user account attributes.</li> </ul>
Delete	<p> <b>Caution</b> The <i>Delete</i> option is destructive by design. We advise that you use it sparingly and with great caution. Among other effects, your deletion of an <a href="#">LDAP</a> bookmark can affect user access to videos in Show and Share.</p> <hr/> <p><b>Note</b> 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.</p>

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

### Related Topics

- [Manage LDAP Attributes, page 7-26](#)

## LDAP Concepts

- [Understand LDAP Attributes, page 7-15](#)
- [Guidelines for LDAP Filters, page 7-15](#)

## Understand LDAP Attributes

Ordinarily, DMS-Admin *will not* import any user account 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 accounts that match your filters. You can do this even when some of the user accounts 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

- Use “OU” values to impose rough limits on a filter, [page 7-15](#)
- Use “memberOf” values to pinpoint a filter more precisely, [page 7-16](#)
- Use “objectClass” values to match all user records, [page 7-16](#)

### 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 <sup>1</sup>
OU=Milpitas,OU=SanJose,DC=example,DC=com	Yes <sup>2</sup>
OU=Sunnyvale,OU=SanJose,DC=example,DC=com	Yes <sup>2</sup>

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

**Note**

**NEW IN CISCO DMS 5.2.3**—User passwords in Cisco DMS are no longer case-sensitive.

- [Understand the Effects of a Changed Password in Active Directory, page 7-16](#)
- [Understand the Effects of a Blank Password in Active Directory, page 7-16](#)

### Understand the Effects of a Changed Password in Active Directory

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

- 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

The Authentication page contains four tabbed property sheets.

<b>Select Mode<sup>1</sup></b>		<i>Embedded, <a href="#">LDAP</a>, or (NEW IN CISCO DMS 5.2.3) <a href="#">SSO</a></i> 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.
<b>Define Filter</b>		<i><a href="#">LDAP</a> or (NEW IN CISCO DMS 5.2.3) <a href="#">SSO</a></i> Your choices on the Define Filter property sheet help you to configure and add a new agreement.

<b>Synchronize Users</b>		<i>LDAP</i> or ( <b>NEW IN CISCO DMS 5.2.3</b> ) <i>SSO</i> Your choices on the Synchronize Users property sheet help you to submit a new agreement.
<b>Manage Attributes</b>		<i>LDAP</i> or ( <b>NEW IN CISCO DMS 5.2.3</b> ) <i>SSO</i>

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, page 7-17](#)
- [Configuration Workflow to Activate Federation \(SSO\) Mode, page 7-17](#)
- [Authentication Scenarios for User Sessions in Federation \(SSO\) Mode, page 7-18](#)

### IdP Requirements

**NEW IN CISCO DMS 5.2.3**—To use [federation \(SSO\)](#) mode in Cisco DMS, you must have access to an [IdP](#) that meets our requirements. Your [IdP](#) must:

- 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.
- Use a digital certificate from a well-known [CA](#) (but only if you will use HTTPS).

### Configuration Workflow to Activate Federation (SSO) Mode

#### **NEW IN CISCO DMS 5.2.3**

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 5.2.3 (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.

- Synchronize DMM with your [Active Directory](#) server to populate the DMM user database.




---

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

---

- 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.

---

- 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

#### NEW IN CISCO DMS 5.2.3

- 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.

- The **SP** asks its **IdP** if the browser is currently authenticated to any valid user account in the **CoT**.
  - 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.**
  - The **IdP** acts on the **SP**’s behalf and redirects the browser immediately to the protected resource.
-

## SSO Scenario 2—Trusted + Valid + NOT Authorized

### NEW IN CISCO DMS 5.2.3

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

### NEW IN CISCO DMS 5.2.3

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, page 7-20](#)
- [Understand Migration \(from Embedded\) to Either LDAP or SSO, page 7-21](#)

### Understand Migration (from Either LDAP or SSO) to Embedded

When you migrate from **LDAP** 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.**

The result varies according to the combination of your choices.

When You Keep Local Copies of			The Result
Users	Groups	Policies	
Yes	Yes	Yes	<ul style="list-style-type: none"> <li>We preserve all local information.</li> <li>We overwrite all LDAP-derived user account passwords with <i>CiscoDMMvp99999</i>.<sup>1</sup></li> </ul>
Yes	No	No	<ul style="list-style-type: none"> <li>We preserve all local user accounts. However, we overwrite all LDAP-derived user account passwords with <i>CiscoDMMvp99999</i>.<sup>1</sup></li> <li>We discard all LDAP-derived groups.</li> <li>We discard all LDAP-derived policies.</li> </ul>
No	Yes	Yes	<ul style="list-style-type: none"> <li>We discard all LDAP-derived user accounts.</li> <li>We preserve all LDAP-derived groups. However, they are empty.</li> <li>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.</li> </ul>
No	No	No	<ul style="list-style-type: none"> <li>We discard all LDAP-derived users, groups, and policies.</li> </ul>

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 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.**

## Procedures

- [Export the Root CA X.509 Certificate from Your Active Directory Server, page 7-22](#)
- [Configure DMM to Trust the Active Directory Root CA, page 7-22](#)
- [Choose an Authentication Method, page 7-23](#)
- [Configure LDAP Settings, page 7-23](#)
- [Configure Federation Services for SSO, page 7-29](#)

## 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.

---

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 or SSO?*  
Proceed to the [“Define LDAP Filters”](#) section on page 7-23

### Related Topics

- [Elements to Choose and Enable the Authentication Mode](#), page 7-31

## Configure LDAP Settings

- [Define LDAP Filters](#), page 7-23
- [Define LDAP Bookmarks](#), page 7-24
- [Define the LDAP Synchronization Schedule](#), page 7-25
- [Manage LDAP Attributes](#), page 7-26
- [Configure the Settings for Automatic LDAP Synchronization](#), page 7-27
- [Derive LDAP Group Membership Dynamically from a Query](#), page 7-28

## Define LDAP 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 7-33](#)

## Define LDAP 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.

---

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 Group Membership Dynamically from a Query](#)” section on page 7-28.
- **OPTIONAL**—*Would you like to configure the schedule for synchronization?*  
Proceed to the “[Define the LDAP Synchronization Schedule](#)” section on page 7-25.

#### Related Topics

- [Define LDAP Filters](#), page 7-23
- [Derive LDAP Group Membership Dynamically from a Query](#), page 7-28
- [Elements to Use LDAP Bookmarks for Synchronization](#), page 7-34

## Define the LDAP 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 [Table 7-3 on page 7-34](#) 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 Attributes”](#) section on page 7-26.
- **OPTIONAL**—*Should Cisco DMS expect that your Active Directory server uses factory-preset attribute names?* If so, proceed to the [“Manage LDAP Attributes”](#) section on page 7-26.
- **OPTIONAL**—*Should Cisco DMS expect that your Active Directory server uses custom attribute names?* If so, proceed to the [“Manage LDAP Attributes”](#) section on page 7-26.

**Related Topics**

- [Define LDAP Bookmarks](#), page 7-24
- [Elements to Schedule Synchronization](#), page 7-35

## Manage LDAP 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 Synchronization Schedule, page 7-25](#)
- [Elements to Manage Attributes, page 7-36](#)

## Configure the Settings for Automatic LDAP 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.
Every Month	Synchronization recurs once each month. You must set the hour and minute when it should start.
Custom	<p>Synchronization recurs at an interval of your choosing. You must set the hour and minute when it should start.</p> <p>Choose <b>Days</b>, <b>Weeks</b>, or <b>Months</b> as the interval type.</p> <ul style="list-style-type: none"> <li>• Choose a day of the month from 1 to 30 when the interval type is Days.</li> <li>• Choose a day of the week when the interval type is Weeks.</li> <li>• Choose an interval of recurrence from 1 to 6 when the interval type is Months.</li> </ul>

**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 Group Membership Dynamically from a Query

**NEW IN CISCO DMS 5.2.1**—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

- **NEW IN CISCO DMS 5.2.3**—[Export an SP Configuration File from DMM, page 7-29](#)
- **NEW IN CISCO DMS 5.2.3**—[Import an IdP Configuration File into DMM, page 7-29](#)
- **NEW IN CISCO DMS 5.2.3**—[Bypass External Authentication During Superuser Login, page 7-30](#)

### Export an SP Configuration File from DMM

**NEW IN CISCO DMS 5.2.3**—Before you can use Cisco DMS in [federation](#) mode, you must export data from it 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 like this one.

---

- Step 7** Stop. You have completed this procedure.
- 

#### Related Topics

- [Import an IdP Configuration File into DMM, page 7-29](#)

### Import an IdP Configuration File into DMM

**NEW IN CISCO DMS 5.2.3**—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.
- Rename the exported [IdP](#) configuration file **dms\_idp\_config.xml**.

#### Procedure

---

- Step 1** Choose **Administration > Security > Authentication**.
- Step 2** Click **Federation** to choose it as your authentication mode.

- Step 3** Click **Import**.
- Step 4** Choose and upload the IdP file that you saved previously.
- Step 5** Enter the necessary **LDAP** information to use your **Active Directory** server.
- Step 6** Stop. You have completed this procedure.
- 

**Related Topics**

- [Define LDAP Filters](#)
- [Export an SP Configuration File from DMM, page 7-29](#)

**Bypass External Authentication During Superuser Login**

**NEW IN CISCO DMS 5.2.3**—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**.
- Enter **superuser** in the Username field.
  - Enter the corresponding password in the Password field.
  - Click **Log In**.



- Step 2** Stop. You have completed this procedure.
- 

**Related Topics**

- [Federation Mode \(SSO\) FAQs, page 7-42](#)

# Reference

- [Software UI and Field Reference Tables, page 7-31](#)
- [Sample SP Configuration File from DMM, page 7-37](#)
- [Sample IdP Configuration Files, page 7-38](#)
- [FAQs and Troubleshooting, page 7-41](#)

## Software UI and Field Reference Tables

- [Elements to Choose and Enable the Authentication Mode, page 7-31](#)
- [Elements to Define, Validate, and Add LDAP Filters, page 7-33](#)
- [Elements to Use LDAP Bookmarks for Synchronization, page 7-34](#)
- [Elements to Schedule Synchronization, page 7-35](#)
- [Elements to Manage Attributes, page 7-36](#)

## Elements to Choose and Enable the Authentication Mode

### Navigation Path

Administration > Security > Authentication > Select Mode

**Table 7-1** Elements for the Authentication Mode

Element	Description
<b>Authentication Mode Area</b>	
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 <i>superuser</i> . Requires future users to authenticate against the user account data from your <a href="#">Active Directory</a> server when they log in to DMM or Show and Share.
Federation	Automatically deletes all user accounts except <i>superuser</i> . Requires future users to authenticate themselves to your <a href="#">IdP</a> when they log in to DMM or Show and Share.
<b>Federation Mode Elements Area</b>	
Last Successfully Configured IdP	This value becomes populated for the first time after you <b>succeed</b> at least once in importing configuration metadata into DMM from your <a href="#">IdP</a> . This element is visible only in <a href="#">federation</a> mode.
IdP Configuration File	Provides the means to import configuration metadata that you previously exported from your IdP and saved to a file. Click <b>Import</b> to browse for the file, which you can then import. This element is visible only in <a href="#">federation</a> mode.

Table 7-1 Elements for the Authentication Mode (continued)

Element	Description
Last Configured IdP	<p>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 <i>attempt</i> to import configuration metadata from an IdP, without regard for whether the attempt failed or succeeded.</p> <p>This element is visible only in <a href="#">federation</a> mode. It becomes populated for the first time after you attempt at least once to import IdP metadata.</p> <p><b>Tip</b> Compare this value to the “Last Successfully Configured IdP” value. When they differ, you know that your latest such attempt actually failed.</p>
(SP Configuration File) Export	<p>Provides the means to export configuration metadata from DMM. Click <b>Export</b> to begin browsing for a locally mounted drive and folder where you can save the exported config file. Later, you will import this file into your IdP.</p> <p>This element is visible only in <a href="#">federation</a> mode.</p>
Enable Authentication Test	<p>Helps you to test whether your <a href="#">federation</a> mode settings are correct and will allow <a href="#">SSO</a> for your ordinary users.</p> <p>Check this check box to expose UI elements that are otherwise hidden. Clear this check box to hide such elements.</p>
Test Username	Enter a username that your IdP already knows. <b>Do not use the “superuser” username.</b> 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	<p>Enables or disables an anonymous connection between your DMM appliance and your <a href="#">Active Directory</a> server.</p> <ul style="list-style-type: none"> <li>An anonymous connection is suitable when you want to see or use <i>public</i> information on the <a href="#">Active Directory</a> server.</li> <li>In contrast, if you want to see or use <i>privileged</i> information on your <a href="#">Active Directory</a> server, the server will require you to enter login credentials to prove that you have sufficient access rights.</li> </ul> <p>In the latter case, your <a href="#">Active Directory</a> server will reject any attempt to log in anonymously. This check box is available to you only when you choose <a href="#">LDAP</a> mode or <a href="#">federation</a> mode.</p>
Host	Enter the routable IP address or DNS-resolvable hostname for the <a href="#">Active Directory</a> server. This field is available to you only when you choose <a href="#">LDAP</a> mode or <a href="#">federation</a> mode.
Port	<p>Enter the TCP port number that your <a href="#">Active Directory</a> server uses for communications. This field is available to you only after you choose <a href="#">LDAP</a> mode or <a href="#">federation</a> mode.</p> <p>The <a href="#">Active Directory</a> port number by default is:</p> <ul style="list-style-type: none"> <li><b>389</b> for <a href="#">LDAP</a> communications.</li> <li><b>636</b> for <a href="#">LDAPS</a> (<i>Secure LDAP</i>, or <i>LDAP over SSL</i>) and <a href="#">SSO</a> communications.</li> </ul>
Administrator DN	<p>Enter the distinguished name of the <a href="#">Active Directory</a> server administrator.</p> <p>This field is available to you only after you choose <a href="#">LDAP</a> mode or <a href="#">federation</a> mode and uncheck the Anonymous check box.</p> <p><b>Tip</b> See <a href="#">administrator DN</a>, page 7-3.</p>

**Table 7-1** Elements for the Authentication Mode (continued)

Element	Description
Password	Enter the password that is associated with the Administrator DN. This field is available to you only after you choose <a href="#">LDAP</a> mode or <a href="#">federation</a> 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 <a href="#">LDAP</a> mode or <a href="#">federation</a> mode. <b>Note</b> Whenever you enable SSL, you must restart Web Services (Tomcat) from AAI. And if your DMM server is one half of a failover pair, the Tomcat restart will trigger immediate failover. <ul style="list-style-type: none"> <li>• Check the check box to enable encryption.</li> <li>• Uncheck it to disable encryption.</li> </ul> Enabling SSL causes the connections between your DMM appliance and your <a href="#">Active Directory</a> server to use <a href="#">LDAPS</a> . An <a href="#">LDAPS</a> 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 <a href="#">Active Directory</a> server uses for <a href="#">LDAPS</a> 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 7-23](#)
- [Elements to Define, Validate, and Add LDAP Filters, page 7-33](#)
- [Elements to Use LDAP Bookmarks for Synchronization, page 7-34](#)
- [Elements to Manage Attributes, page 7-36](#)

**Elements to Define, Validate, and Add LDAP Filters****Navigation Path**

Administration &gt; Security &gt; Authentication &gt; Define Filter

**Table 7-2** 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.

Table 7-2 Elements for Filters (continued)

Element	Description
User Group (in DMM)	Choose or create a user group to associate with the filter. At the very least, the list includes these options. <ul style="list-style-type: none"> <li>All Users Group</li> <li>Create a New User Group</li> <li>Digital Signage Users</li> </ul>
<b>Command Buttons</b>	
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 7-23](#)
- [Elements to Choose and Enable the Authentication Mode, page 7-31](#)
- [Elements to Use LDAP Bookmarks for Synchronization, page 7-34](#)
- [Elements to Manage Attributes, page 7-36](#)

**Elements to Use LDAP Bookmarks for Synchronization****Navigation Path**

Administration &gt; Security &gt; Authentication &gt; Synchronize Users

Table 7-3 Elements for Bookmarks

Element	Description
<b>LDAP Bookmarks property sheet</b>	
Synchronization	One of the following types. <ul style="list-style-type: none"> <li>Initial</li> <li>Update</li> <li>Overwrite</li> <li>Delete</li> </ul> <p><b>Note</b> When you click <b>Delete</b> on the <b>LDAP Bookmarks</b> sub-tab, we ask you whether to delete groups and policies. When you choose Yes, we delete all of the following from Cisco DMS.</p> <ul style="list-style-type: none"> <li><b>All user accounts that match the filter.</b></li> <li><b>NEW IN CISCO DMS 5.2.1</b>—The particular user group that is associated to the filter.</li> <li><b>NEW IN CISCO DMS 5.2.1</b>—All access policies associated to the particular user group.</li> </ul> <p><b>The deletion process can take as long as 1 minute to finish.</b></p>

**Table 7-3** Elements for Bookmarks (continued)

Element	Description
<b>Command Buttons</b>	
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. <ul style="list-style-type: none"> <li>Discards all changes to the configuration of behaviors for synchronizations.</li> <li>Discards all changes to the scope of access.</li> </ul>

**Related Topics**

- [Choose an Authentication Method, page 7-23](#)
- [Elements to Choose and Enable the Authentication Mode, page 7-31](#)
- [Elements to Define, Validate, and Add LDAP Filters, page 7-33](#)
- [Elements to Manage Attributes, page 7-36](#)

**Elements to Schedule Synchronization****Navigation Path**

Administration &gt; Security &gt; Authentication &gt; Synchronize Users

**Table 7-4** Elements for Scheduling

Element	Description
<b>Scheduling property sheet</b>	
Synchronization Mode	Enables one synchronization mode to receive updated user account information from an <a href="#">Active Directory</a> server. We support two such modes but they are mutually exclusive. Whenever you enable one, you disable the other. Click either <b>Manual Synchronization</b> or <b>Automatic Synchronization</b> .
<b>Command Buttons</b>	
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. <ul style="list-style-type: none"> <li>Discards all changes to the configuration of behaviors for synchronizations.</li> <li>Discards all changes to the scope of access.</li> </ul>

**Related Topics**

- [Configure the Settings for Automatic LDAP Synchronization, page 7-27](#)
- [Choose an Authentication Method, page 7-23](#)
- [Elements to Choose and Enable the Authentication Mode, page 7-31](#)

- [Elements to Define, Validate, and Add LDAP Filters, page 7-33](#)
- [Elements to Manage Attributes, page 7-36](#)

## Elements to Manage Attributes

### Navigation Path

Administration > Security > Authentication > Manage Attributes

**Table 7-5** *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 <a href="#">Active Directory</a> 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 <a href="#">Active Directory</a> servers use for this purpose. When the values for these attributes differ on your <a href="#">Active Directory</a> server or when you prefer to import objects that use other <a href="#">Active Directory</a> attributes, you can edit the values in this column.
Values to Use by Default	<p>Enter text to insert automatically when the value is blank for the corresponding attribute in an <a href="#">Active Directory</a> 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:</p> <ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> </ul> <p>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.</p> <p><b>Note</b> You cannot enter a value to use by default as the Login User Name value.</p>
Ignore User Account Control Flags	<b>NEW IN CISCO DMS 5.2.3</b> —Tells DMM to ignore whether your <a href="#">Active Directory</a> server makes use of the User Account Control Flags attribute. DMM expects to find this attribute on your <a href="#">Active Directory</a> 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 <a href="#">Active Directory</a> servers use. If you entered different values manually because the labels for these attributes differ on your <a href="#">Active Directory</a> server or because you prefer to import user accounts that use other <a href="#">Active Directory</a> 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 7-23](#)
- [Elements to Choose and Enable the Authentication Mode, page 7-31](#)

- [Elements to Define, Validate, and Add LDAP Filters, page 7-33](#)
- [Elements to Use LDAP Bookmarks for Synchronization, page 7-34](#)

## 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 COBEcGAAT0Qg4wBBMMVTzVzC1DEQAM8K1AQVKNDwDMBGF0TxWJACA0YNENgQxCSADEVNlQUwQxDV
BDbAQ0M8pvGTNUFyMtzWtYxTAMVtMMAxx3EMLEcTDDFMvzNEMwCtMnco2LmhgTVw2MTaMAMvx1ALMOQADBkjVwAcMB
GNTh0F1BQVJJQAAUM1BSDQwTHAsxAVgM1NMjTCVEQEegzCwEUCAAQxh8Y0GkMMBZzGtwSVNX0EUBglbgRvgwJrADA5
QYF32B9PNQEBVJANQIBb5K8YwNUQNYo0aQDjDJyMbhjswjcDgAM0IYJIoAGAGBr/qwladetiX6wNGw1+Pn2rhopPL7
cCzUI2aNCNyK+d99sLujKL/kjyCBZ9lqKPeCarxWfKycC3/Qqg0/SNz33b8JSh6iG35kVwa3OMZplEtLX4CfBkdsXY
TVaKIRPRMSOH9u9vH6ELFgSz18dH/tLlo3aJADhnG4gcFA8tGE8QIXZBdBQdNw1DYj1AAAARYsKS6wV2vCZEgTNEI
MAQbvD A87sb03cvDpQUUCJ5SQ00/ 4xQA531HhBHSCDOFbUlq+ PeTKB4dkGsIst9BPaIr43bW03zfkMbrU2A WNu+
dPcBzP01raWmP2I8ZErlDYPJSEstzmaC30kkeXg4nfe10KCx1QH8BAQusegy38+ oh8NLYw3N dzQ15vs=
</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"/>
  </SPSSODescriptor>
</EntityDescriptor>
```

```

    <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>

```

## Sample IdP Configuration Files

- [Exported IdP Configuration Sample from OpenAM, page 7-38](#)
- [Exported IdP Configuration Sample from Shibboleth, page 7-39](#)

## Exported IdP Configuration 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>
MJEwVfGgTTQ1MUwD9w0kQACIQNICQQWBGBY1AqqAMBGUzAwAEkVsiagAELKkCBkDCADdhAUIQIGE
CYABEMTxwVzNBKQ1NQZDMALNCEQ1ADJzAKC0E4QgQSBExwGGVwzM0AAGQOVDUDT0A8cCNTxMFBVV
BxxjNambbJAQRbThnMxj1MNFYm8cpT2mDovLMTvENV4pAJIw2yNDRAYDMMTAG0wOyET3MLExgMw
ZEMAAVvk80JDVMVT1TSghThEMxBwjAU1zkwFMYEODCAQgH0MGQQGAJCNLEUNBQEBsCCBAwQVM1QAx
DGgwkJ5EAY9vMADP2y0NbJIQo0jV5RaXw8YbsQsTVQDjx5ZKNKNZaUgMBByUDjhcYjN2wJBSWQ0bNABmAo2eD4JQ1QA
hEVyPDgAQEMZBUiAtNdgrxA0BcYIB9QuG4aWYHGx/LcxHcYoes0MIYciud6KmI+/kq/YpRbA30QYctD0uax/
0M7BUD/SMT+P1kQhA9dCLiOeu2WB2dKfWwOwLihgne7omCI+ozijrImy+4C3fz9zC/VrBA3bQZMcnsE6YbZJDC7Th
AjNAEAoQNZ5gGAKxBYEABzXjgAQwcDpvFYK1yNqr wArS1A7b3VkhN42iQVjvj8I3No2ssay4LZyBsffkrM+
gATatC/HvyyNGoapGS9K4fLZNzBaXDW99/728x7bGciRWFdx4V0dPABkis+alHad9Blj8uCupvRp/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"/>

```





```

        </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>

```

## FAQs and Troubleshooting

- [FAQs, page 7-41](#)

### FAQs

- [LDAP \(Active Directory\) FAQs, page 7-41](#)
- [Federation Mode \(SSO\) FAQs, page 7-42](#)
- [Error Message FAQs, page 7-42](#)
- [Network Policy FAQs, page 7-42](#)
- [User Exclusion FAQs, page 7-43](#)

### 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 5.2.1
- Cisco DMS 5.2.2
- Cisco DMS 5.2.3

**Windows Active Directory Server 2003**

- Cisco DMS 5.2.1
- Cisco DMS 5.2.2
- Cisco DMS 5.2.3

**Windows Active Directory Server 2008R2**

- Cisco DMS 5.2.3

## Federation Mode (SSO) FAQs

- Q. NEW IN CISCO DMS 5.2.3—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. NEW IN CISCO DMS 5.2.3—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. NEW IN CISCO DMS 5.2.3—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. NEW IN CISCO DMS 5.2.3—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.

---

