Sun Java™ System

Communications Services 6 Schema Reference

2004Q2

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 817-5702-10

Contents

About This Manual

This manual serves as a reference for schema information for Sun Java™ System Communication Services products using LDAP, specifically Sun Java™ System Messaging Server and Sun Java™ System Calendar Server.

Topics covered in this chapter include:

Who Should Read This Manual

You should read this manual if you want to provision Sun Java™ System Messaging Server, or Sun Java™ System Calendar Server, using LDAP. The audience for this manual consists of:

- System architects who want to develop customized provisioning tools that interface between Coummication Services product entries in the LDAP directory and their existing source of users, groups, and domains information such as a company database or billing system.
- Site Administrators who want to know how to create domain, user, group, or resource entries using LDAP.

What You Need to Know

This manual assumes that you have a general understanding of the following:

- The Internet and the World Wide Web
- Sun Java™ System Administration Server
- Sun Java™ System Directory Server and LDAP
- Email and email concepts
- Calendar and calendar concepts
- Sun Java™ System Console
- RFC 2798, and RFC 2445

  The RFC's may be found at the IETF web sites:

  - http://www.ietf.org/rfc/rfc2798.txt
  - http://www.ietf.org/rfc/rfc2445.txt
- ISO8601 DateTime Format

  For a list of time zone names used with these products, see Appendix A, Standard Time Zones.

In addition, you probably need to have a general understanding of either the two following products:

- iPlanet Delegated Administrator for Messaging, for use with Sun Java™ System LDAP Schema 1
- Sun Java™ System Identity Server, for use with Sun Java™ System LDAP Schema 2

How This Manual is Organized

This manual contains the following chapters and appendix:

- About This Manual (this chapter)
- Chapter 1, "Overview"
- Chapter 2, "Object Classes"
- Chapter 3, "Attributes"

- Chapter 4, “Sun Java™ System Identity Server Classes and Attributes”
- Chapter 5, “iPlanet Delegated Administrator for Messaging Classes and Attributes”
- Appendix A, “General Information”
- Glossary

Document Conventions

Monospaced Font

`Monospaced font` is used for any text that appears on the computer screen or text that you should type. It is also used for filenames, distinguished names, functions, and examples.

Bold Monospaced Font

`Bold monospaced font` is used to represent text within a code example that you should type. For example, you might see something like this:

```
./installer
```

In this example, **`./installer`** is what you would type at the command line.

Italicized Font

Italicized font is used to represent text that you enter using information that is unique to your installation (for example, variables). It is used for server paths and names.

For example, throughout this document you will see path references of the form:

msg_svr_base`/...`

The Messaging Server Base (*msg_svr_base*) represents the directory path in which you install the server. The default value of the *msg_svr_base* is `/opt/SUNWmsgsr`.

Square or Straight Brackets

Square (or straight) brackets [] are used to enclose optional parameters.

Command Line Prompts

Command line prompts (for example, % for a C-Shell, or $ for a Korn or Bourne shell) are not displayed in the examples. Depending on which operating system you are using, you will see a variety of different command line prompts. However, you should enter the command as it appears in the document unless specifically noted otherwise.

Platform-specific Syntax

All paths specified in this manual are in UNIX® format. If you are using a Windows 2000-based Communications Services, you should assume the Windows 2000 equivalent file paths whenever UNIX file paths are shown in this book.

Where to Find Related Information

In addition to this manual, the Communications Services products come with supplementary information for administrators, end users, and developers.

Messaging Server Documents

Use the following URL to see all the Messaging Server documentation:

http://docs.sun.com/coll/MessagingServer_04q2

The following documents are available:

- *Sun Java™ System Messaging Server Release Notes*
- *Sun Java™ System Messaging Server Deployment Planning Guide*
- *Sun Java™ System Messaging Server Administration Guide*
- *Sun Java™ System Messaging Server Administration Reference*
- *Sun Java™ System Messaging Server Developer's Reference*

- *Sun Java™ System Messaging Server Messenger Express Customization Guide*

  If you are using LDAP Schema 1, use the Provisioning Guide found in the iPlanet Messaging Server 5.2 documents.

  If you are using LDAP Schema 2, use information found in the Sun Java Enterprise System documentation.

The Messaging Server product suite contains other products such as Sun Java™ System Console, Directory Server, and Administration Server. Documentation for these and other products can be found at the following URL:

http://docs.sun.com/db/prod/sunone

In addition to the software documentation, see the Messaging Server Software Forum for technical help on specific Messaging Server product questions. The forum can be found at the following URL:

http://swforum.sun.com/jive/forum.jsp?forum=15

Calendar Server Documents

Use the following URL to see all the Calendar Server documentation:

http://docs.sun.com/coll/CalendarServer_04q2

The following documents are available:

- *Sun Java™ System Calendar Server Release Notes*
- *Sun Java™ System Calendar Server Administration Guide*
- *Sun Java™ System Calendar Server Developer's Guide*

Communications Services Documents

Use either one of the following URLs to see the documentation that applies to all Communications Services products:

http://docs.sun.com/coll/MessagingServer_04q2

or

http://docs.sun.com/coll/CalendarServer_04q2

The following documents are available:

- *Sun Java™ System Communications Services User Management Utility Administration Guide*
- *Sun Java System Communications Services Enterprise Deployment Planning Guide*
- *Sun Java™ System Communications Services Schema Migration Guide*
- *Sun Java™ System Communications Services Schema Reference*
- *Sun Java™ System Communications Services Event Notification Service Guide*
- *Sun Java™ System Communications Express Administration Guide*
- *Sun Java™ System Communications Express Customization Guide*

Where to Find This Manual Online

You can find the *Sun Java™ System Communication Services Schema Reference* online in HTML and PDF formats.

To find this manual or other Messaging Server documentation, use the URL:

`http://docs.sun.com/coll/MessagingServer_04q2`

Or, for this manual and other Calendar Server documentation, use the URL:

`http://docs.sun.com/coll/CalendarServer_04q2`

Related Third-Party Web Site References

Third-party URLs are referenced in this document and provide additional, related information.

NOTE Sun is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Chapter 1

Overview

This chapter gives an overview of Sun Java™ System Communications Services schema. It contains the following sections:

Data Model for Sun Java™ System LDAP Schema 2

The basic data model of Sun Java™ System object classes is to extend LDAP entry *types* (for example, user, group, domain) created by *core object classes* by overlaying them with *shared classes* (object classes can be shared by more than one service) and *service-specific object classes* (classes specific to a certain type of server).

In addition, there are two ways to structure the LDAP data model: native mode (the preferred way) using only an Organization Tree, and compatibility mode (for backwards compatibility with earlier versions of Sun Java™ System or iPlanet™ LDAP based products) using both a DC Tree and an Organization Tree. The LDAP data model for compatibility mode is essentially the same as data model for the Sun Java™ System LDAP Schema 1. Provisioning your LDAP differs depending on whether you chose the native or compatibility mode at installation time.

Use the Sun Java™ System Communications Services User Management Utility (a command line utility) to add, modify and delete users, groups and domains.

For a discussion of the differences in LDAP data models between the native and compatibility modes (and LDAP Schema 1), see “LDAP Directory Information Tree Requirements” in Chapter 3, “Understanding Product Requirements and Considerations,” in the *Sun Java System Communications Services Enterprise Deployment Planning Guide*.

For more information on RFC 2798, RFC 2252, and internet standards, use the following URL:

http://www.imc.org/rfcs.html

Table 1-1 shows the core classes, shared classes and server specific classes for the three types of entries for native mode: domains, users and groups. Note that for Calendar Server, there is an additional type of entry for resources that need to be scheduled, such as conference rooms and equipment.

Note that while `userPresenceProfile` is not specifically a Messaging Server object class (it is used to store vacation start and end dates), Calendar Server does not use it at all.

This table also includes the classes used by Identity Server in these types of entries. Identity Server classes are shown in italicized font. Note that the object classes and attributes defined for Identity Server are subject to change. See the *Sun Java™ Enterprise System Technical Overview* for a discussion of provisioning concepts.

Table 1-1 Native Mode Entry types and Corresponding Object Classes

Types	Core Classes	Shared Classes	Server Specific Classes

Domain	`organization`
	`domain`
	`sunManagedOrganization`
	`sunNameSpace`
			`mailDomain`
			`icsCalendarDomain`

User	`person`
	`inetUser`
	`organizationalPerson`
	`inetOrgPerson`
		`ipUser`
		`userPresenceProfile`
		`iplanet-am-managed-person`
			`inetMailUser`
			`inetLocalMailRecipient`

Group	`groupOfUniqueNames` *`iplanet-am-managed-group`*	*`iplanet-am-managed-filtered-group`* *`iplanet-am-managed-assignable-group`* *`iplanet-am-managed-static-group`*	`inetMailGroup` `inetLocalRecipient`

Table 1-1 Native Mode Entry types and Corresponding Object Classes

Types	Core Classes	Shared Classes	Server Specific Classes
Resource	inetResource		icsCalendarResource

Table 1-2 shows the core classes, shared classes and server specific classes for the four types of entries for compatibility mode: DC Tree domains, Organization Tree domains, users and groups.

Note that for Calendar Server, there is an additional type of entry for resources that need to be scheduled, such as conference rooms and equipment. Also note that userPresenceProfile is used only by Messaging Server, even though it is not a messaging specific object class.

This table also includes the classes used by Identity Server in these types of entries.

Table 1-2 Compatibility Mode Entry types and Corresponding Object Classes

Types	Core Classes	Shared Classes	Server Specific Classes
DC Tree Domain	domain inetDomain		mailDomain icsCalendarDomain
Org Tree Domain	organization sunManagedOrganization sunNameSpace		
User	person inetUser organizationalPerson inetOrgPerson	ipUser userPresenceProfile iplanet-am-managed-person	inetMailUser inetLocalMailRecipient
Group	groupOfUniqueNames iplanet-am-managed-group	iplanet-am-managed-filtered-group iplanet-am-managed-assignable-group iplanet-am-managed-static-group	inetMailGroup inetLocalRecipient
Resource	inetResource		icsCalendarResource

Data Model for Sun Java™ System LDAP Schema 1

The basic data model of Sun Java™ System object classes is to extend LDAP entry *types* (for example, user, group, domain) created by *core object classes* by overlaying them with *shared classes* (object classes can be shared by more than one service) and *service-specific object classes* (classes specific to a certain type of server).

This model has an Organization Tree for holding user and group information and a Domain Component Tree (DC Tree) that holds the domain information.

This model is administered by the iPlanet Delegated Administrator for Messaging graphical user interface.

For more information on RFC 2798, RFC 2252, and internet standards, use the following URL:

`http://www.imc.org/rfcs.html`

Table 1-3 shows the core classes, shared classes and server specific classes for the four types of entries: DC Tree domains, Organization Tree domains, users and groups. Note that for Calendar Server, there is an additional type of entry for resources that need to be scheduled, such as conference rooms and equipment. This table also includes the marker classes used by Delegated Administrator.

Table 1-3 Two-DIT Entry types and Corresponding Object Classes

Types	Core Classes	Shared Classes	Server Specific Classes

DC Tree Domain	`domain`
	`inetDomain`
			`mailDomain`
			`nsManagedDomain`
			`icsCalendarDomain`

Org Tree Domain	`organization`		`nsManagedDomain`

User	`person`
	`inetUser`
	`organizationalPerson`
	`inetOrgPerson`
		`ipUser`
		`userPresenceProfile`
			`inetMailUser`
			`inetLocalMailRecipient`
			`nsManagedPerson`

Group	`groupOfUniqueNames`		`inetMailGroup`
			`inetLocalRecipient`
			`inetMailGroupManagement`
			`nsManagedMailingList`

Table 1-3 Two-DIT Entry types and Corresponding Object Classes

Types	Core Classes	Shared Classes	Server Specific Classes
Family Account	inetManagedGroup		nsManagedDept
Resource	inetResource		icsCalendarResource

Messaging Server Schema Overview

The basic Messaging Server schema model is to extend LDAP entries created by structural object classes. Extensions are made to a base LDAP entry using auxiliary object classes. The extensions made for Messaging Server are defined in this manual.

For example, `inetOrgPerson` is the structural class used to make a base user entry. This user entry becomes an email user when overlaid by the auxiliary classes defined in this document. Similarly, `groupOfUniqueNames` is the structural class used to make a base group entry, which becomes an email distribution list when overlaid by the distribution list auxiliary object classes.

Messaging Server auxiliary object classes can be grouped by function into the following categories and subcategories:

- Mail Recipient
  - Email Users
  - Email Groups (Distribution Lists)
  - Email Routing
- Personal Address Book
  - Personal Address Book
  - Personal Address Book Group
  - Personal Address Book Person
- Domains
  - Hosted Domain Entries
  - Domain Aliases
  - Domain Organizations
- Delegation of Management

- Managed Group
- Store Administrator

Mail Recipient

There are two types of mail recipients: users and groups. Both user and group email use the `inetLocalMailRecipient` auxiliary object class for local mail routing attributes.

Email Users

LDAP entries created by `inetOrgPerson` can be enabled for messaging services by overlaying the entry with `inetUser`, `ipUser`, `inetMailUser`, `inetLocalMailRecipient`, and `userPresenceProfile`. Optionally, `inetSubscriber` may be used for holding subscriber type attributes for the user, but it is not required for creating messaging server users.

Email Groups

LDAP entries created by `groupOfUniqueNames` can be enabled for messaging services by overlaying the entry with `inetMailGroup`, `inetMailUser`, and `inetLocalMailRecipient`. These object classes define distribution lists and how they are to be used by the messaging server.

Email Routing

For email routing attributes, the messaging server uses the object class `inetLocalMailRecipient`.

Personal Address Book

LDAP entries created by `inetOrgPerson` can be enabled for personal address books by overlaying the entry with object classes `pab`, `pabGroup`, and `pabPerson`. The data model for personal address book entries is the address book (`pab`), which contains zero or more persons (`pabPerson`) and zero or more group (`pabGroup`) entries.

Personal Address Book

The personal address book (pab object class) contains zero or more pabPerson and zero or more pabGroup entries. All users and groups belong to the default personal address book called All.

Personal Address Book Group

The personal address book group object class, pabGroup, corresponds to a personal distribution list. A group belongs to zero or more personal address books. The link between groups and personal address books is established by memberOfPAB, a multi-valued attribute of pabGroup.

Personal Address Book Person

The personal address book user object class, pabPerson, is a user entry in a personal address book. A user (pabPerson) can belong to zero or more personal address book groups (pabGroup) and zero or more personal address books (pab).

The link between users and groups is established by memberOfPABGroup, a multi-valued attribute of pabPerson, which allows the user to belong to many groups. A user can also belong to many personal address books. This link is established by memberOfPAB, a multi-valued attribute of pabPerson.

Domains

Domain object classes are used to specify email-addressable organizations. These domains are known as hosted domains.

This section discusses the following:

- Hosted Domain Entries
- Domain Aliases
- Domain Organizations

Hosted Domain Entries

LDAP entries created by domain and inetDomain can be enabled for hosted domains using the object class mailDomain.There must be an instance of both mailDomain, and inetDomain for each hosted domain. Optionally, to hold attributes suitable for overriding the default behavior of mailDomain and for stored certmaps, inetDomainAuthInfo can be used.

For LDAP Schema 2, each hosted domain entry must also carry the Identity Server marker class, sunManagedOrganization and its attribute, sunPreferredDomain. This is true in both native and compatibility modes. In addition, if the hosted domain is also to be a namespace, the domain entry must contain the sunNameSpace object class and sunNameSpaceUniqueAttrs attribute.

For LDAP Schema 1, each hosted domain entry must carry the Delegated Administrator marker class nsManagedDomain.

Domain Aliases

A hosted domain can have aliases. In LDAP Schema 1, and LDAP Schema 2 compatibility mode, these aliases are separate nodes on the DC Tree, and depending on what type of aliasing is being one, can carry separate routing information. However, for LDAP Schema 2 native mode, there is no DC Tree. All aliasing is handled by adding the associatedDomain attribute (which lists all the alias names) to the domain node. This means a loss of functionality for native mode. That is for native mode, there can not be separate domain information (and thus different mail routing) for alias domains.

For LDAP Schema 2, compatibility mode, the DC Tree domain alias nodes are still present, and can be provisioned using the Sun Java™ System User Management Utility.

For the User Management Utility (commadmin), see the *Sun Java™ System Communications Services User Management Utility Administration Guide.*

Domain Organizations

To support a managed domain organization in LDAP Schema 1, the auxiliary object classes inetDomainOrg is used in conjunction with the structural class organization. A domain organization is usually created as a way of introducing hierarchy beneath a customer subtree and assigning administrators for that domain organization. The resulting structures are not domains. They are usually denoted with the attribute organizationalUnit (ou).

LDAP Schema 2 does not support “domain organizations” as used by earlier versions of Messaging Server. Especially do not use iplanet-am-managed-organizational-unit, which despite its name, is treated exactly the same as a regular domain named by sunManagedOrganization. Since this organization is not a domain, and there is no marker class for this in Identity Server, if you want to use the “domain organization” concept in your LDAP Schema 2 directory, you must provision and manage these structures by directly writing LDAP entries (using ldapmodify).

Delegation of Management

Managed group object classes are used to specify arbitrary groupings of users or groups (and possibly other resources defined in the LDAP directory) so that management of these resources can be delegated to another user. Examples of such groupings are DNS domain boundaries, and departments.

Managed Group

Managed groups commonly have different rules for adding or deleting members. To enable policy differences in the administration of groups, an instance of the object class `inetOrgPerson`, with its associated policy attributes, must exist for each managed group.

Store Administrator

To define a group of administrators for domains, the object class `inetMailAdministrator` is used to grant members administrative privileges over users in the same domain where the group is defined.

Calendar Server Schema Overview

This section lists the Calendar Server object classes and their attributes.

Table 1-4 shows the calendar-specific object classes and their attributes. In addition, Calendar Server also uses one non-calendar object class, inetResource.

Table 1-4 Calendar-Specific Object Classes

Object Classes	Required Attributes	Allowed Attributes
icsAdministrator (not currently used)	N/A	icsAdminRole, icsExtended, icsExtendedGroupPrefs

Table 1-4 Calendar-Specific Object Classes *(Continued)*

Object Classes	Required Attributes	Allowed Attributes
icsCalendarDomain (not all attributes are currently used)	N/A	icsAllowedServiceAccess, icsAllowRights, icsAnonymousAllowWrite, icsAnonymousCalendar, icsAnonymousDefaultSet, icsAnonymousLogin, icsAnonymousSet, icsDefaultAccess, icsDomainAllowed, icsDomainNames, icsDomainNotAllowed, icsDWPBackEndHosts, icsExtended, icsExtendedDomainPrefs, icsMandatorySubscribed, icsMandatoryView, icsPreferredHost, icsQuota, icsRecurrenceBound, icsRecurrenceDate, icsSessionTimeout, icsSourceHtml, icsStatus, icsTimezone
icsCalendarDWPHost (not currently implemented)	N/A	cn, description, icsDomainNames, icsDWPHost, icsExtended, icsRegularExpressions, icsStatus
icsCalendarGroup (not currently implemented)	icsStatus	N/A
icsCalendarResource (not all attributes are currently used)	N/A	cn, icsAlias, icsCalendar, icsCapacity, icsContact, icsDWPHost, icsExtended, icsExtendedResourcePrefs, icsGeo, icsPartition, icsPreferredHost, icsQuota, icsStatus, icsTimezone, mailAlternateAddress, mail, uid

Table 1-4 Calendar-Specific Object Classes *(Continued)*

Object Classes	Required Attributes	Allowed Attributes
icsCalendarUser (not all attributes are currently used)	N/A	cn, givenName, icsAllowedServiceAccess, icsCalendar, icsCalendarOwned, icsDefaultSet, icsDWPHost, icsExtended, icsExtendedUserPrefs, icsFirstDay, icsFreeBusy, icsGeo, icsPartition, icsPreferredHost, icsQuota, icsSet, icsStatus, icsSubscribed, icsTimezone, mail, mailAlternateAddress, nswcalDisallowAccess, preferredLanguage, sn, uid, userPassword

Chapter 2

Object Classes

This chapter describes LDAP object classes for Communications Services products. The objects are listed alphabetically.

Note that the object classes and attributes specific only to Identity Server are found in a separate chapter, Chapter 4, “Sun Java™ System Identity Server Classes and Attributes.”

Note also that the object classes and attributes specific only to iPlanet Delegated Administrator for Messaging are found in a separate chapter, Chapter 5, “iPlanet Delegated Administrator for Messaging Classes and Attributes.”

List of Object Classes

This chapter describes the following object classes:

Object Classes

domain

Supported by
Messaging Server 5.0, Calendar Server 5.1

Definition
Object class used to define entries that represent DNS domains.

This class can only be used with an entry that doe not correspond to an organization, organizational unit, or other type of object for which an object class has been defined.

This is a core class for both Messaging and Calendar products.

Superior Class
top

Object Class Type
structural

OID
0.9.2342.19200300.100.4.13

Required Attributes
dc, objectClass

Allowed Attributes
associatedName, businessCategory, description, destinationIndicator, fax (facsimileTelephoneNumber), internationalIsdnNumber, localityName, manager, o (organizationName (see o)), physicalDeliveryOfficeName, postOfficeBox, postalAddress, postalCode, preferredDeliveryMethod, registeredAddress, searchGuide, seeAlso, st, street, telephoneNumber, telexTerminalIdentifier, telexNumber, userPassword, x121Address

groupOfUniqueNames

Supported by
Messaging Server 5.0, Calendar Server 5.1

Definition
Defines entries for a group of unique names. A static group entry must be extended by this class. (A group entry may also be extended by inetUser.) Use roles to define dynamic groups. For information on roles, see the *Sun Java™ System Directory Server Administrator's Guide.*

Superior Class
top

Object Class Type
structural

OID
2.5.6.17

Required Attributes
cn, objectClass, uniqueMember

Allowed Attributes
businessCategory, description, o, ou, owner, seeAlso

icsAdministrator

Supported by
Not currently used.

Definition
Specifies a calendar administrator. Must be used in conjunction with other object classes.

Superior Class

Object Class Type
structural

OID
2.16.840.1.113730.3.2.145

Required Attributes
N / A

Allowed Attributes
icsAdminRole, icsExtended, icsExtendedGroupPrefs

icsCalendarDomain

Supported by
Calendar Server 5.1.1

Definition
Specifies a calendar domain. Must be used in conjunction with inetDomain.

Superior Class
top

Object Class Type
structural

OID
1.3.6.1.4.1.42.2.27.9.2.4

Required Attributes
N / A

Allowed Attributes
The following attributes are currently used:

icsAllowedServiceAccess, icsAllowRights, icsDefaultAccess, icsDomainNames, icsExtendedDomainPrefs, icsStatus, icsTimezone

The following attributes are reserved but not implemented for this object class:

icsAnonymousAllowWrite, icsAnonymousCalendar, icsAnonymousDefaultSet, icsAnonymousLogin, icsAnonymousSet, icsDomainAllowed, icsDomainNotAllowed, icsDWPBackEndHosts, icsExtended, icsMandatorySubscribed, icsMandatoryView, icsPreferredHost, icsQuota, icsRecurrenceBound, icsRecurrenceDate, icsSessionTimeout, icsSourceHtml,

icsCalendarDWPHost

Supported by
Calendar Server 5.1.1

Definition
Reserved; not implemented.

Contains configuration and other information specific to one DWP server. Each entry tracks which domain it serves. The domain names are used to scope searches.

Superior Class

Object Class Type
structural

OID
1.3.6.1.4.1.42.2.27.9.2.1

Required Attributes
N / A

Allowed Attributes
`cn`, `description`, `icsDomainNames`, `icsDWPHost`, `icsExtended`, `icsRegularExpressions`, `icsStatus`

icsCalendarGroup

Supported by
Calendar Server 5.1

Definition

Reserved, not implemented.

Superior Class

Object Class Type
structural

OID
1.3.6.1.4.1.42.2.27.9.2.5

Required Attributes
`icsStatus`

Allowed Attributes
N/A

icsCalendarResource

Supported by
Calendar Server 5.1, Sun Java™ System Communication Services User Management Utility 1.0

Modified in 5.1.1 – attributes added: `icsDWPHost`, `icsPartition`, `uid`

Definition
Specifies a calendar resource, such as a conference room or piece of equipment that must be scheduled. Must be used in conjunction with `inetResource`. Not all attributes are currently used.

Identity Server 6.1 reserves this as a marker class for calendar resources but does not support calendar resources yet.

Superior Class
`inetResouce`

Object Class Type
structural

OID
1.3.6.1.4.1.42.2.27.9.2.3

Required Attributes
`N/A`

Allowed Attributes
The following attributes are currently used:

`cn`, `description`, `icsCalendar`, `icsDWPHost`, `icsPartition`, `icsStatus`, `icsTimezone`, `mail`, `mailAlternateAddress`, `uid`

The following attributes are reserved but not implemented for this object class:

`icsAlias`, `icsCapacity`, `icsContact`, `icsExtended`, `icsExtendedResourcePrefs`, `icsGeo`, `icsPreferredHost`, `icsQuota`

icsCalendarUser

Supported by
Calendar Server 5.1

Modified in 5.1.1 – attributes added: icsDWPHost, icsPartition

Definition
Specifies a calendar user, including the DWP host name.

Superior Class
top

Object Class Type
auxiliary

OID
1.3.6.1.4.1.42.2.27.9.2.2

Required Attributes
N / A

Allowed Attributes
These attributes are currently in use:

cn, givenName, icsAllowedServiceAccess, icsCalendar, icsCalendarOwned, icsDWPHost, icsExtendedUserPrefs,icsFirstDay, icsPartition, icsSet, icsStatus, icsSubscribed, icsTimezone, mail, mailAlternateAddress, preferredLanguage, sn, uid, userPassword

These attributes are reserved but not currently used:

icsDefaultSet, icsExtended, icsFreeBusy, icsGeo, icsPreferredHost, icsQuota, nswcalDisallowAccess

inetAdmin

Supported by
Messaging Server 5.0

Definition
Identifies administrator user or group.

Superior Class
top

Object Class Type
Auxiliary

OID
2.16.840.1.113730.3.2.112

Required Attributes
`objectClass`

Allowed Attributes
`memberOf`, `adminRole`

inetDomain

Supported by
Messaging Server 5.0

Definition
Used in two-tree LDAP data models to extend the base entry created by `domain` in the DC Tree. It represents a hosted domain account and is used in conjunction with `mailDomain` and (optionally `inetDomainAuthInfo`) for creating a hosted domain node in the DC Tree suitable for mail services for the hosted organization. This object class must be used for all hosted domain entries in the DC Tree.

Identity Server uses this as a marker class for domains in the DC Tree.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.129

Required Attributes
`inetDomainBaseDN`

Allowed Attributes
`inetDomainStatus`

inetDomainAlias

Supported by
Messaging Server 5.0

Definition
Structural class for creating domain alias entries in the DC Tree for the compatibility mode LDAP data model. Entries may be created that point at other hosted domain objects. Such domain alias entries must be extended by this object class. Attribute `aliasedObjectName`, inherited from the parent object class `alias` (see RFC 2256), holds the DN of the LDAP entry for which the node is an alias.

Use this object class when you want two identical domains with different names. If you want two domains that have different attribute settings, create two `inetDomain` entries and use the `inetCanonicalDomainName` attribute to decorate the domain to use for mail routing.

This object class is not used in the native mode LDAP data model. Instead, to show the aliases for a domain, the (Organization Tree) domain entry is extended by `sunManagedOrganization` and decorated with the `businessCategory` attribute.

Superior Class
alias

Object Class Type
structural

OID
2.16.840.1.113730.3.2.131

Required Attributes
`aliasedObjectName`, `dc`

Allowed Attributes
N / A

inetDomainAuthInfo

Supported by
Messaging Server 5.0

Definition
This object class is used to extend the `domain` entry with search filter, domain cert map, and a canonical domain name if more than one hosted domain refers to the same organization subtree.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.133

Required Attributes
N / A

Allowed Attributes
`domainUidSeparator`, `inetDomainSearchFilter`, `inetDomainCertMap`, `inetCanonicalDomainName`

inetLocalMailRecipient

Supported by
Messaging Server 5.0

Definition
Stores information that provides a way to designate an LDAP entry as one that represents a local (intra-organizational) email recipient, to specify the recipient's email address(es), and to provide routing information pertinent to the recipient. This is intended to support SMTP message transfer agents in routing RFC 822-based email within a private enterprise only, and is not to be used in the process of routing email across the public Internet.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113.730.3.2.147

Required Attributes
N / A

Allowed Attributes
`mail`, `mailAlternateAddress`, `mailHost`, `mailRoutingAddress`

inetMailAdministrator

Supported by
Messaging Server 5.0

Definition
LDAP group defined with `groupOfUniqueNames` can be overlaid with this object class. Members (listed in the attribute `uniqueMember`) of a group overlaid with this object class and where `mailAdminRole` is set to `storeAdmin` get IMAP proxyauth (proxy authentication) rights over all users in the same domain in which the group entry exists.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.148

Required Attributes
N / A

Allowed Attributes
`mailAdminRole`

inetMailGroup

Supported by
Messaging Server 5.0

Definition
Used to extend the base entry created by `groupOfUniqueNames` to define a group of mail recipients. `inetMailGroup` is used to store attributes of a mailing list. It is used in conjunction with `inetLocalMailRecipient` and `inetMailGroupManagement` (for mailing lists managed by the Delegated Administrator).

Superior Class
`top`

Object Class Type
auxiliary

OID
1.3.6.1.4.1.42.2.27.2.2.2

Required Attributes
N / A

Allowed Attributes
`dataSource`, `inetMailGroupStatus`, `mailConversionTag`, `mailDeferProcessing`, `mailDeliveryFileURL`, `mailDeliveryOption`, `mailEquivalentAddress`, `mailMsgMaxBlocks`, `mailProgramDeliveryInfo`, `mailRejectText`, `memberURL`, `mgrpAddHeader`, `mgrpAllowedBroadcaster`, `mgrpAllowedDomain`, `mgrpAuthPassword`, `mgrpBroadcasterPolicy`, `mgrpDeliverTo`, `mgrpDisallowedBroadcaster`, `mgrpDisallowedDomain`, `mgrpErrorsTo`, `mgrpModerator`, `mgrpMsgMaxSize`, `mgrpMsgPrefixText`, `mgrpMsgRejectAction`, `mgrpMsgRejectText`, `mgrpMsgSuffixText`, `mgrpNoDuplicateChecks`, `mgrpRemoveHeader`, `mgrpRFC822MailMember`, `preferredLanguage`, `uniqueMember`

inetMailUser

Supported by
Messaging Server 5.0

Definition
Used to extend the base entry created by `inetOrgPerson` to define a messaging service user. It represents a mail account and is used in conjunction with `inetUser` and `inetLocalMailRecipient`. Optionally, `inetSubscriber` may also be used for general account management purposes.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.146

Required Attributes
N / A

Allowed Attributes
`cn`, `dataSource`, `icsQuota`, `mailAllowedServiceAccess`, `mailAntiUBEService`, `mailAutoReplyMode`, `mailAutoReplySubject`, `mailAutoReplyTimeOut`, `mailAutoReplyText`, `mailAutoReplyTextInternal`, `mailConversionTag`, `mailDeferProcessing`, `mailDeliveryOption`, `mailEquivalentAddress`, `mailForwardingAddress`, `mailMessageStore`, `mailMsgMaxBlocks`, `mailMsgQuota`, `mailProgramDeliveryInfo`, `mailQuota`, `mailSieveRuleSource`, `mailSMTPSubmitChannel`, `mailUserStatus`, `nswmExtendedUserPrefs`

inetOrgPerson

Supported by
Specified here for reference only.

Definition
All user entries are created with this object class. Refer to the internet draft *The LDAP inetOrgPerson Object Class* for further details.

Superior Class
`organizationalPerson`

Object Class Type
structural

OID
2.16.840.1.113730.3.2.2

Required Attributes
N / A

Allowed Attributes
businessCategory, givenName, mail, uid, preferredLanguage

inetResource

Supported by
Calendar Server 5.1

Definition
Specifies a resource, which is defined as an object to which calendar services are provided. For example, a conference room, or a piece of equipment shared by many that needs to be scheduled.

Superior Class
top

Object Class Type
structural

OID
2.16.840.1.113730.3.2.142

Required Attributes
cn

Allowed Attributes
facsimileTelephoneNumber, inetResourceStatus, mail, postalAddress, telephoneNumber

inetSubscriber

Supported by
Messaging Server 5.0

Definition
Used to extend the base entry created by `inetOrgPerson` to define a user. It represents a subscriber account and may be used in conjunction with `inetUser`, `inetMailUser`, and `ipUser` for creating a mail account.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.134

Required Attributes
N / A

Allowed Attributes
`inetSubscriberAccountId`,`inetSubscriberChallenge`, `inetSubscriberResponse`

inetUser

Supported by
Messaging Server 5.0, Calendar Server 5.1.1

Definition
It represents a user account, or a resource (defined as any object to which services are provided) account, and is used in conjunction with `inetMailUser` and `ipUser` for creating a mail account. When creating user accounts, this object class extends the base entry created by `inetOrgPerson`.

This attribute can be used with `icsCalendarUser` for creating a calendar user account. (Note that `inetResource` is used by Calendar Server to create resource accounts.)

User and resource entries must be extended by this object class. Group entries may be extended with this class.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.130

Required Attributes
N / A.

Allowed Attributes
`inetUserHttpURL` (see note),`inetUserStatus`, `memberOf` (see note),`uid`, `userPassword`

NOTE The attributes `inetUserHttpURL`, and `memberOf` are deprecated for this object class and are likely to be removed from the class in future versions of the schema.

ipUser

Supported by
Messaging Server 5.0

Superior Class
`top`

Definition
Object class for services like mail and calendar. Used to extend the base entry created by `inetOrgPerson` and `inetUser`. This object class holds the reference to the personal address book container and the class of service specifier.

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.135

Required Attributes
N / A

Allowed Attributes
inetCoS, memberOfPAB, maxPabEntries, pabURI

mailDomain

Supported by
Messaging Server 5.0

Definition
Auxiliary class used to extend the base entry created by domain and inetDomain for enabling messaging services for the hosted domain. It represents a hosted domain account with access to Messaging Service. This object class must be used for all hosted domain entries.

In the absence of the mailPublicFolderDefaultRights attribute for a maliPublicFolder entry, the presence of the attribute in the mailDomain entry allows administrators to specify the default rights to assign to the public folder.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.151

Required Attributes
N / A

Allowed Attributes
mailAccessProxyPreAuth, mailAccessProxyReplay, mailClientAttachmentQuota, mailDomainAllowedServiceAccess, mailDomainConversionTag, mailDomainCatchallAddress, mailDomainDiskQuota, mailDomainMsgMaxBlocks, mailDomainMsgQuota, mailDomainReportAddress, mailDomainSieveRuleSource,mailDomainStatus, mailDomainWelcomeMessage, mailPublicFolderDefaultRights, mailQuota,mailRoutingHosts, mailRoutingSmartHost, preferredLanguage, preferredMailHost,

mailPublicFolder

Supported by
Sun ONE Messaging Server 6.0

Definition
Defines a public folder.

Superior Class
top

Object Class Type
structural

OID

Required Attributes
mailFolderName

Allowed Attributes
mailMessageStore, mailPublicFolderDefaultRights, mailDeliveryOption

msgVanityDomainUser

Supported by
Messaging Server 5.0

Definition
This object class and its attribute are deprecated in the current release, and may not be supported in future releases. Sites should stop using this feature and consider migrating current vanity domains to hosted domains.

Auxiliary class for supporting the notion of a vanity domain for messaging. Used to extend the base mail user entry to assign a vanity domain to the user.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.150

Required Attributes
N / A

Allowed Attributes
msgVanityDomain

organization

Supported by
Messaging Server 5.0

Definition
Defines entries that represent organizations. An organization is generally assumed to be a large, relatively static grouping within a larger corporation or enterprise.

Superior Class
top

OID
2.5.6.4

Required Attributes
objectClass, o (organizationName)

Allowed Attributes
businessCategory, description, destinationIndicator, facsimileTelephoneNumber, internationalIsdnNumber, l (localityName), physicalDeliveryOfficeName, postalAddress, postalCode, postOfficeBox, preferredDeliveryMethod, registeredAddress, searchGuide, seeAlso, st, street, telephoneNumber, teletexTerminalIdentifier, telexNumber, userPassword

organizationalUnit

Supported by
Messaging Server 5.0

Definition
Defines entries that represent organizations. An organization is generally assumed to be a large, relatively static grouping within a larger corporation or enterprise.

Superior Class
top

OID
2.5.6.5

Required Attributes
objectClass, ou

Allowed Attributes
businessCategory, description, destinationIndicator, facsimileTelephoneNumber, internationalIsdnNumber, l (localityName), physicalDeliveryOfficeName, postalAddress, postalCode, postOfficeBox, preferredDeliveryMethod, registeredAddress, searchGuide, seeAlso, st, street, telephoneNumber, teletexTerminalIdentifier, telexNumber, userPassword

pab

Supported by
Messaging Server 5.0

Definition
The data model used is as follows:

pabPerson is a user entry in the personal address book.

pabGroup is the group entry and corresponds to a personal distribution list. For example, the pabGroup "pab-notes" may contain pabPersons micky and john.

pab is the address book that contains zero or more pabPerson and zero or more pabGroup entries. This is the top level logical container. pab may contain pabPerson and / or pabGroup. A pabPerson may belong in zero or more pabGroup and zero or more pab.

pabPerson may belong to zero or more pabGroup entries. This link is established by memberOfPABGroup, a multi-valued attribute holding the DN of the pabGroup in which the pabPerson belongs. A pabPerson may also belong to many personal address book's. This link is established by having the DN of the pab listed as a value of the attribute memberOfPAB.

All users and groups belong in the default personal address book called "All."

Superior Class
top

Object Class Type
structural

OID
2.16.840.1.113730.3.2.140

Required Attributes
cn

Allowed Attributes
description, un

pabGroup

Supported by
Messaging Server 5.0

Definition
pabGroup is a group entry in a personal address book (pab) and corresponds to a personal distribution list. For example, the pabGroup "pab-notes" may contain pabPersons micky and john.

Superior Class
top

Object Class Type
structural

OID
2.16.840.1.113730.3.2.139

Required Attributes
cn

Allowed Attributes
description, memberOfPAB, nickName, un

pabPerson

Supported by
Messaging Server 5.0

Definition
A user entry in the personal address book (pab).

Superior Class
inetOrgPerson

Object Class Type
structural

OID
2.16.840.1.113730.3.2.138

Required Attributes
N / A

Allowed Attributes
calCalURI, calFBURL, co, dateOfBirth, mailAlternateAddress, memberOfPAB, memberOfPABGroup, nickName, organizationName (see o), ou (oranizationalUnitName), un

userPresenceProfile

Supported by
Messaging Server 5.0

Definition
Used to store the presence information for a user.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.136

Required Attributes
N / A

Allowed Attributes
vacationEndDate, vacationStartDate

Chapter 3

Attributes

This chapter describes attributes required or allowed by LDAP object classes for Communications Services products. The attributes are listed alphabetically.

Note that attributes used exclusively by Identity Server are covered in Chapter 4, "Sun Java™ System Identity Server Classes and Attributes." Whereas, attributes used exclusively by iPlanet Delegated Administrator for Messaging are covered in Chapter 5, "iPlanet Delegated Administrator for Messaging Classes and Attributes."

List of Attributes

This chapter describes the following attributes:

Attribute Definitions

aclGroupAddress

Origin
Messaging Server 6.0

Syntax
cis

Object Classes
inetMailUser

Definition
Adds a user to a dynamic group specified as an identifier in an ACL entry. Members of the group share the particular access rights defined in the ACL entry. The group is represented by a dynamic mailing list with a filter on the aclGroupAddr attribute.

Example
```
aclGroupAddr: lee-staff@siroe.com
```

OID
1.3.6.1.4.1.42.2.27.9.1.686

adminRole

Origin
Messaging Server 5.0

Syntax
cis

Object Classes
inetAdmin

Definition
Specifies the administrator role for this administrator entry.

Example

OID
2.16.840.1.113730.3.1.601

aliasedObjectName

Origin
Messaging Server 5.0

Syntax
dn

Object Classes
inetDomainAlias

Definition
Used only in compatibility mode (with a DC Tree) for LDAP Schema 2, not in native mode (no DC Tree).

Used by the directory server to identify alias entries in the directory. Contains the distinguished name of the entry for which it is an alias. The domain attribute values are taken only from the referenced domain. So that routing will be identical between these domains.

Example
```
aliasedObjectName: cn=jdoe,o=sesta.com
```

OID
2.5.4.1

businessCategory

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
groupOfUniqueNames, organization, organizationalUnit

Definition
Identifies the type of business in which the entry is engaged. This should be a broad generalization such as is made at the corporate division level.

Example
```
businessCategory:Engineering
```

OID
2.5.4.15

calCalURI

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
pabPerson

Definition
Contains URI to user's entire default calendar. For details see RFC 2739.

Example
Varies according to the version of calendar server implemented. For details see RFC 2739.

OID
1.2.840.113556.1.4.478

calFBURL

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
pabPerson

Definition
URL to the user's default busy time data. For details see RFC 2739.

Example
Varies according to the version of calendar server implemented. For details see RFC 2739.

OID
1.2.840.113556.1.4.479

cn

Origin
Calendar Server

Syntax
cis, single-valued

Object Classes
`icsCalendarResource`, `icsCalendarUser`, `inetResource`

Definition
For users, full name of person. For resources, a unique identifier. In either case, it may contain spaces and special characters. Abbreviation for `commonName`.

Example
For a user: `cn: John Doe`.

For a resource: `cn: Conference Room #3`

or

`commonName: John Doe`

`commonName: Conference Room #3`

OID
2.5.4.3

co

Origin
LDAP

Syntax
cis

Object Classes
`pabPerson`

Definition
Contains the name of a country, using a two character code. Abbreviation for `countryName`.

The attribute `friendlyCountryName` is used to spell out the actual country name.

Example
`co:IE`

or

`countryName:IE`

`friendlyCountryName:Ireland`

OID
2.5.4.4

commonName (see cn)

countryName (see co)

dataSource

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailUser`, `inetMailGroup`

Definition
Text field to store a tag or identifier. Value has no operational impact.

Example
`dataSource:1.0`

OID
2.16.840.1.113730.3.1.779

dateOfBirth

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`pabPerson`

Definition
Date of birth of the `pabPerson`. Format is: `YYYYMMDD`.

Example
`dateOfBirth: 19740404`
(date of birth on April 6, 1974.)

OID
2.16.840.1.113730.3.1.779

dc

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetDomainAlias`

Definition
The domain component of the domain alias entry.

Example
`dc=sesta`

For example a domain alias entry DN might be:
`dn: dc=sesta, dc=fr, o=internet`.

OID
0.9.2342.19200300.100.1.25

description

Origin
LDAP

Syntax
cis, multi-valued

Object Classes
`icsCalendarDWPHost`, `icsCalendarResource`, `groupOfUniqueNames`, `inetOrgPerson`, `organization`, `organizationalUnit`, `pab`, `pabGroup`, `sunServiceComponent`

Definition
Provides a human readable description of the object. For people and organizations, this often includes their role or work assignment.

Example
description: Quality control inspector.

OID
2.5.4.13

domainUidSeparator

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetDomainOrg

Definition
This attribute is used only for LDAP Schema 1.

This attribute is used by the messaging server to override the default mailbox (MB) home. When present, this attribute specifies that compound user identifications (UIDs) are used in this domain and this attribute specifies the separator. For instance, if + is the separator, the mailbox names in this domain are obtained by replacing the right most occurrence of + in the uid with @. To map an internal mailbox name to the UID, the right most occurrence of @ is replaced with a + in the mailbox name.

While substitution of an @ for the UID separator is sufficient to generate a mailbox name, this may not be the same as any of the user's actual email addresses.

NOTE	Format of internal mailbox names is uid@domain, where "domain" is DNS domain mapping to the namespace. The only exception to this rule is mailbox names for users in default domain where only the uid is used to construct internal mailbox names. See inetCanonicalDomainName on how the default value of domain name used can be overridden in specific cases.

The MTA option used to override this attribute's value is LDAP_DOMAIN_ATTR_UID_SEPARATOR.

Example
```
domainUIDSeparator: #
```

OID
2.16.840.1.113730.3.1.702

domOrgMaxUsers

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetDomainOrg

Definition
This attribute is used only for LDAP Schema 1.

Maximum number of user entries in a domain organization.

Example
```
domOrgMaxUser: 500
```

OID
2.16.840.1.113730.3.1.697

domOrgNumUsers

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetDomainOrg

Definition
Number of current user entries in a domain organization.

Example
```
domOrgNumUsers: 345
```

OID
2.16.840.1.113730.3.1.698

facsimileTelephoneNumber

Origin
Calendar Server

Syntax
tel, single-valued

Object Classes
icsCalendarResource, inetResource, organization, organizationalUnit

Definition
Fax telephone number for resources.

Example
facsimileTelephoneNumber 1-800-555-1212

OID
2.5.4.23

givenName

Origin
LDAP

Syntax
cis

Object Classes
icsCalendarUser

Definition
Identifies the entry's given name, usually a person's first name.

Example
```
givenName: John
```

OID
2.5.4.42

icsAdminRole

Origin
Calendar Server

Syntax
cis

Object Classes
icsAdministrator

Definition
Administrative calendar role that can be assigned to a group.

Example

OID
2.16.840.1.113730.3.1.724

icsAlias

Origin
Calendar Server

Syntax
cis, UTF8 encoded

Object Classes
icsCalendarResource

Definition
Alias associated with a resource. An alias can make a resource name easier for the end user to work with.

Example
The resource named “halleyscomet” can be aliased as “Halley’s Comet”.

```
icsAlias: Halley’s Comet
```

OID
2.16.840.1.113730.3.1.725

icsAllowedServiceAccess

Origin
Calendar Server 6.0

Syntax
cis, single-valued

Object Classes
`icsCalendarDomain`, `icsCalendarUser`

Definition
This attribute is used only if the icsStatus attribute is not set, or in other words, if icsStatus is set, this attribute is ignored.

Use this attribute to disallow calendar services to a user. As a default all users are allowed access with `http`, but if you specify this attribute as shown in the example, it disallows the user from receiving calendar access (user is disabled):

Any other setting, or absence of the attribute entirely, results in the user having access to `http` services (user is enabled).

Example
```
icsAllowedServiceAccess:http
```

OID
2.16.840.1.113730.3.1.726

icsAllowRights

Origin
Calendar Server

Syntax
int, single valued

Object Classes
`icsCalendarDomain`

Definition

A numeric string used to hold bit fields, each corresponding to a set of rights. Each bit corresponds to a setting in the `ics.conf` file. After you have figured out the bit string settings you want, convert the bits to an integer.

If the property is set (`1`), the right is not allowed. If the bit is not set (`0`), the right is allowed.

If this attribute does not exist, the corresponding `ics.conf` default settings are used.

Table 3-1 defines the meaning of each bit position for bits 0-15:

Table 3-1 Bit Definitions and ics.conf Settings

Property Name and ics.conf Setting Name	Bit	Allows (0) or Disallows (1)
`allowCalendarCreation` `service.wcap.allowcreatecalendars`	`0`	Creation of calendars
`allowCalendarDeletion` `service.wcap.allowdeletecalendars`	`1`	Deletion of calendars
`allowPublicWritableCalendars` `service.wcap.allowpublicwriteablecalendars`	`2`	Publicly writable calendars for users
`N/A`	`3`	Reserved. Defaults to `0`
`allowModifyUserPreferences` `service.admin.calmaster.wcap.allowgetmodifyuserprefs`	`4`	Domain Administrator allowed to change user preferences
`allowModifyPassword` `service.wcap.allowchangepassword`	`5`	Users allowed to change their password
`N/A`	`6`	Reserved. Defaults to `0`
`N/A`	`7`	Reserved. Defaults to `0`
`allowUserDoubleBook` `user.allow.doublebook`	`8`	Double booking of user calendars
`allowResourceDoubleBook` `resource.allow.doublebook`	`9`	Double booking of resource calendars
`allowSetCn` `service.wcap.allowsetprefs.cn`	`10`	User preference `cn` modified by `set_userprefs` command

Table 3-1 Bit Definitions and ics.conf Settings

Property Name and ics.conf Setting Name	Bit	Allows (0) or Disallows (1)
`allowSetGivenName` `service.wcap.allowsetprefs.givenname`	11	User preference `givenname` modified by `set_userprefs` command
`allowSetGivenMail` `service.wcap.allowsetprefs.mail`	12	User preference `mail` modified by `set_userprefs` command
`allowSetPrefLang` `service.wcap.allowsetprefs.preferredlanguage`	13	User preference `preferredlanguage` modified by `set_userprefs` command
`allowSetSn` `service.wcap.allowsetprefs.sn`	14	User preference `sn` modified by `set_userprefs` command
`N/A`	15-31	Reserved. Defaults to all `0`

Example

If you decide that you want to disallow the following bits:

- publicly writable user calendars (bit 2),
- double booking of resources (bit 9),
- and modifying the given name (bit 11),

then your bit pattern would look like this:

‘00000000000000000000101000000100’

which you would convert into the integer 2564 so that:

```
icsAllowRights: 2564
```

OID

2.16.840.1.113730.3.1.727

icsAnonymousAllowWrite

Origin

Calendar Server

Syntax
boolean (yes, no)

Object Classes
icsCalendarDomain

Definition
Specifies if anonymous users can write events in public calendars. The value comes from the `ics.conf` setting `service.wcap.anonymousallowpubliccalendarwrite`.

Example
```
icsAnonymousAllowWrite: yes
```

OID
2.16.840.1.113730.3.1.728

icsAnonymousCalendar

Origin
Calendar Server

Syntax
ces

Object Classes
icsCalendarDomain

Definition
Calendar ID for anonymous users. The value is taken from the `ics.conf` setting `calstore.anonymous.calid`.

Example
```
icsAnonymousCalendar: guest1
```

OID
2.16.840.1.113730.3.1.729

icsAnonymousDefaultSet

Origin
Not implemented.

Syntax
ces, UTF8 encoded

Object Classes
icsCalendarDomain

Definition
Default calendar set for anonymous users.

Example

OID
2.16.840.1.113730.3.1.730

icsAnonymousLogin

Origin
Calendar Server

Syntax
boolean (yes, no))

Object Classes
icsCalendarDomain

Definition
Specifies if anonymous login is allowed. Value is taken from the `ics.conf` file setting `service.http.allowanonymousLogin`.

Example
```
icsAnonymousLogin: yes
```

OID
2.16.840.1.113730.3.1.798

icsAnonymousSet

Origin
Not implemented.

Syntax
ces, UTF8 encoded

Object Classes
icsCalendarDomain

Definition
Reserved. Not implemented.

Default calendar set for anonymous users.

Example

OID
2.16.840.1.113730.3.1.732

icsCalendar

Origin
Calendar Server

Syntax
ces, single-valued

Object Classes
icsCalendarResource, icsCalendarUser

Definition
The calendar ID (calid) of the default calendar for a user or resource. Required attribute. It is a policy of Calendar Server to construct calids based on the user's uid, since it is guaranteed to be unique.

Example
```
icsCalendar: jdoe
```

OID
2.16.840.1.113730.3.1.731

icsCalendarOwned

Origin
Calendar Server

Syntax
ces, multi-valued

Object Classes
icsCalendarUser

Definition
Calendars owned by this user. At least one instance of this attribute must exist for each user and must be set with the user's default calendar value. Multiple instances of this attribute can be used to specify other calendars the user owns.

Example
```
icsCalendarOwned: jdoe
icsCalendarOwned: jdoe:BaseballSchedule
icsCalendarOwned: jdoe:Project
icsCalendarOwned: jdoe:Holidays
```

OID
1.3.6.1.4.1.42.2.27.9.1.6

icsCapacity

Origin
Not implemented.

Syntax
int, single-valued

Object Classes

Definition
Reserved, not implemented.

Example

OID
2.16.840.1.113730.3.1.800

icsContact

Origin
Not implemented.

Syntax
cis, UTF8 encoded

Object Classes
icsCalendarResource

Definition
Reserved, not implemented.

Resource contact name.

Example
```
icsContact: John Doe jdoe@sesta.com
```

OID
2.16.840.1.113730.3.1.733

icsDefaultAccess

Origin
Calendar Server

Syntax
cis, single valued

Object Classes

Definition
Default access control string applied to the user's default calendar. For more information about access control, see "Access Control Entries" in the *Sun Java™ System Calendar Server Programmer's Manual*. If this attribute is not present, the value is taken from the `ics.conf` file setting `calstore.calendar.default.acl`.

Example
Granting the user both freebusy and scheduling permission for calendar components.

```
icsDefaultAccess: @sesta.com^c^sf^g
```

OID
2.16.840.1.113730.3.1.734

icsDefaultSet

Origin
Calendar Server

Syntax
ces, single-valued

Object Classes
`icsCalendarUser`

Definition
User preference for what calendars to display at login. User's can specify any of their calendar sets (groups they have created) to be displayed at login instead of a single calendar.

Example
```
icsDefaultSet: MyCalendarGroup
```

OID
2.16.840.1.113730.3.1.735

icsDomainAllowed

Origin
Not implemented.

Syntax
cis, single-valued (see mgrpAllowedDomain)

Object Classes
icsCalendarDomain

Definition
What domains are allowed. The value has the following format:

`service-list:client-list`

where `service-list` is a blank- or comma-separated list of one or more service names or wildcards, and client-list is a blank- or comma-separated list of one or more host names or addresses, patterns or wildcards.

The following are the explicit wildcards recognized by the system:

ALL	Always matches
LOCAL	Matches any host whose name does not contain a dot character.
UNKNOWN	Matches any host whose name or address are unknown. Use this with care.
KNOWN	Matches any host whose name and address are known. Use with care.
DNSSPOOFER	Matches any host whose name does not match its address.

There is one operator that can be used in the service-list and the client-list:

EXCEPT	Matches anything that matches list 1 unless it matches anything in list 2. The expected form: list1 EXCEPT list2. List1 and list2 are comma-separated.

You can use patterns to distinguish clients by the network address that they can connect to. For example: `service@host_pattern:client-list`.

The default value comes from `service.http.domainallowed` in the `ics.conf` file.

Example
Allow local access to anyone in the sesta.com domain.

```
icsDomainAllowed: ALL:sesta.com
```

OID
2.16.840.1.113730.3.1.736

icsDomainNames

Origin
Calendar Server.1

Syntax
cis, multi-valued, ASCII

Object Classes
icsCalendarDomain

Definition
For cross-domain searching, each external domain to be searched must be listed using this attribute.

Example

```
icsDomainNames: sesta.com
icsDomainNames: siroe.com
```

OID
1.3.6.1.4.1.42.2.27.9.1.3

icsDomainNotAllowed

Origin
Calendar Server

Syntax
cis, single-valued (see mgrpDisallowedDomain)

Object Classes
icsCalendarDomain

Definition

What domains are not allowed. The value has the following format:

service-list:client-list

where service-list is a blank- or comma-separated list of one or more service names or wildcards, and client-list is a blank- or comma-separated list of one or more host names or addresses, patterns or wildcards.

The following are the explicit wildcards recognized by the system:

ALL	Always matches
LOCAL	Matches any host whose name does not contain a dot character.
UNKNOWN	Matches any host whose name or address are unknown. Use this with care.
KNOWN	Matches host whose name and address are known. Use with care.
DNSSPOOFER	Matches any host whose name does not match its address.

There is one operator that can be used in the service-list and the client-list:

EXCEPT	Matches anything that matches list 1 unless it matches anything in list 2. The expected form: list1 EXCEPT list2. List1 and list2 are comma-separated.

The value comes from `ics.conf` setting `service.http.domainnotallowed`.

Example 1

If you want to allow access to all but a selected few hosts, you can explicitly deny access as in the following example:

Deny access to anyone at the company22.com domain.

```
icsDomainNotAllowed: ALL:company22.com
```

In this instance, you would not need to have any specific `icsDomainAllowed` attributes.

Example 2

If you want to implement a no-access default, a single instance of this attribute will do it. This denies all service to all hosts, unless they are specifically permitted access by `icsDomainAllowed` attributes.

```
icsDomainNotAllowed: ALL:ALL
```

Example 3
The following example shows how to deny access to any unknown users.

```
icsDomainNotAllowed: ALL:UNKNOWN@ALL
```

OID
2.16.840.1.113730.3.1.737

icsDWPBackEndHosts

Origin
Calendar Server 5.1.1

Syntax
cis, multi-valued

Object Classes
icsCalendarDomain

Definition
The list of all possible back end hosts used for calendars found in this domain. This attribute is required if the calendar installation is using the Database Wire Protocol (DWP).

Example

```
icsDWPBackEndHosts: machine1
icsDWPBackEndHosts: machine2
```

OID
1.3.6.1.4.1.42.2.27.9.1.5

icsDWPHost

Origin
Calendar Server.1

Syntax
cis, single-valued, ASCII

Object Classes
icsCalendarDWPHost, icsCalendarResource, icsCalendarUser

Definition
Stores a DWP host name so that the calendar ID can be resolved to the Database Wire Protocol (DWP) server that stores the calendar and its data. When the calendar database is distributed across several back end servers, the attribute value is the DNS name of user's back end host. Each user's entire calendar will be on a single back end server. Required if using the Calendar Lookup Database (CLD).

This attribute is required if the Calendar installation is using DWP to distribute calendar data across back end calendar data servers. If DWP is not being used, every user's calendar will be found on the same host as the calendar server. If an installation initially does not use DWP, but later switches to it, the calendar server will fill in this value based on the default DWP host name found in the domain entry. If there is no value or such entry (calendar server is not in hosted domain mode) then the value will be picked up from the `ics.conf` configuration file.

Example
`icsDWPHost:calserv1`

OID
1.3.6.1.4.1.42.2.27.9.1.1

icsExtended

Origin
Calendar Server 5.1.1

Syntax
cis, multi-valued

Object Classes
icsCalendarDWPHost

Definition
Extensions for calendar. Reserved.

Example

OID
2.16.840.1.113730.3.1.738

icsExtendedDomainPrefs

Origin
Calendar Server

Syntax
cis, multi- valued

Object Classes
icsCalendarDomain

Definition
Preferences for calendar domains can be set using the properties found in Table 3-2. Each attribute value is a property-value pair. The default settings for these properties are found in the domain server's `ics.conf` file. In the absence of this attribute, the `ics.conf` settings will be used.

Table 3-2 Domain Preferences

Property	Value	Description
`allowProxyLogin`	yes, no	Allow proxy login
`calmasterAccessOverride`	yes, no	Domain administrator can override access control
`calmasterCred`	string	Bind credentials (password) for user specified in `ics.conf` setting `service.admin.calmaster.userid`
`calmasterUid`	string	User ID for the domain administrator
`createLowerCase`	yes, no	Make calendar name lowercase for creating new calendars and looking up calendars.
`domainAccess`	valid acl string	Access control string for domain. Used in cross-domain searches to permit external domains to search this domain.
`fbIncludeDefCal`	yes, no	User's default calendar included in freebusy calendar list.
`filterPrivateEvents`	yes, no	Filter the private and confidential events on queries to server.
`resourceDefaultAcl`	valid access string	Resource calendars' default ACL
`setPublicRead`	yes, no	Set default user calendars to public read and private write (yes), or private read and private write (no).
`subIncludeDefCal`	yes, no	User's default calendar included in subscribed calendar list
`uiAllowAnyone`	yes/no	Everybody ACL shows and can be used in the user interface.
`uibaseURL`	valid URL	Base server address. For example, `https://proxyserver/`

Table 3-2 Domain Preferences *(Continued)*

Property	Value	Description
uiConfigFile	string	Specifies the configuration file for the user interface. (Allows items in the user interface to be turned off.)
uiProxyUrl	string	Proxy server address prepended in user interface JavaScript file. For example, https://web_portal.com/

Example

```
icsExtendedDomainPrefs: createLowerCase=yes
```

```
icsExtendedDomainPrefs:
domainAccess=@@d^a^slfrwd^g;anonymous^a^r^g;@^a^s^g
```

In this example, any external domain matching the access rights shown above can search this domain.

OID

2.16.840.1.113730.3.1.739

icsExtendedGroupPrefs

Origin

Calendar Server

Syntax

cis

Object Classes

icsAdministrator

Definition

Extensions for calendar group preferences.Reserved.

Example

OID

2.16.840.1.113730.3.1.740

icsExtendedResourcePrefs

Origin
Not implemented.

Syntax
cis

Object Classes

Definition
Reserved, not implemented.

Example

OID
2.16.840.1.113730.3.1.741

icsExtendedUserPrefs

Origin
Calendar Server

Syntax
cis, multi-valued

Object Classes
`icsCalendarUser`

Definition
Extensions for calendar user preferences. The attribute value is a property-value pair. The following are the properties and their values

Table 3-3 Extended User Preferences

Properties	Values	Description
`ceAllCalendarTZIDS`	a standard time zone	Time zone TZID for this calendar.
`ceClock`	12, 24	Defines whether a 12- or 24-hour clock is used.

Table 3-3 Extended User Preferences *(Continued)*

Properties	Values	Description
ceColorSet	pref_group1 pref_group2 pref_group3 pref_group4 pref_group7	Defines which of the five UI color schemes to use.
ceDateOrder	M/D/Y D/M/Y Y/M/D	Determines what order the three elements of a date (month (M), day (D), and year (Y)) are displayed.
ceDateSeparator	Any single printable character. For example: / or -	The single character used to delimit displayed date elements (M,D,Y). For example, a date can be displayed as: 12/22/2002.
ceDayHead	0–23	Start time hour (expressed as one of 24 hours in a day) for displaying calendar information.
ceDayTail	0–23	End time hour (expressed as one of 24 hours in a day) for displaying calendar information.
cdDefaultAgenda	unused	Not currently implemented.
cdDefaultAlarmEmail	email addresses separated by white space	Email Addresses event alarms sent to.
ceDefaultAlarmStart	P[unit count][unit type]	Amount of time before the event an alarm should be sent. Where unit count is any numeric value, and unit type is either M (minutes), H (hours), or D (days). For example: P10M
ceDefaultTZID	one of standard time zones For a list of time zones, see Standard Time Zones.	Time zone to use when a calendar does not have one assigned to it.
ceDefaultView	dayview weekview monthview yearview groupview	View to be presented at log in. If this parameter is not present, overview is used as the default. (groupview is the Comparison view on the user interface)
ceExludeSatSun	boolean (0, 1)	Calendars don't display if value=1. Default is value=0.

Table 3-3 Extended User Preferences *(Continued)*

Properties	Values	Description
ceFontFace	One of these values: 1) Times New Roman, Times, serif 2) Courier New, Courier, noon 3) PrimaSans BT, Verdana, sans-serif	Three choices of font face to be used in the user interface.
ceFontSizeDelta	pref_font_size_group_2 (normal) pref_font_size_group_1 (larger) pref_font_size_group_3 (smaller)	Defines three font sizes for the user interface. In the interface they are defined as: normal, larger, smaller.
ceGroupInviteAll	boolean (0, 1)	When creating an invitation while viewing a group, invite all calendars in the group when value=1; default is 1.
ceInterval	PT0H15M PT0H30M PT1H0M PT2H0M PT4H0M	Defines the time interval to be used when displaying calendar information. Intervals are: 15 min., 30 min., 1hour, 2 hours, 4 hours.
ceNotifyEmail	any valid RFC 822 email address	Email address notifications are mailed to when the calendar receives an invitation to an event.
ceNotifyEnable	0, 1	Enables/disables email notifications being sent when the calendar receives an invitation to an event. 0 = do not sent notifications 1 = send notifications
ceSingleCalendarTZID	any valid time zone For a list of valid time zones, see Standard Time Zones.	Lists the time zone assigned to this calendar. If the parameter is not sent, the default time zone is used. For example: America/Los_Angeles
ceToolImage	0, 1	Toggle for the user interface display of icon images on the toolbar. 0 = do not display icons, 1 = display icons (default)
ceToolText	0, 1	Toggle for the user interface display of icon text on the toolbar. 0 = do not display text with the icon 1 = display text with the icon (default)

NOTE Regarding `ceToolImage` and `ceToolText`: the user interface only allows three possibilities for the toolbar: icons and text (attributes values `1`, `1`), icons only (attributes values `1`, `0`), and text only (attributes values `0`, `1`). It does not allow the user to turn off both icons and text (attributes values `0`, `0`).

Example

```
icsextendeduserprefs: ceClock=12
icsextendeduserprefs: ceColorSet=pref_group_1
icsextendeduserprefs: ceDateOrder=D/M/Y
icsextendeduserprefs: ceDateSeparator=/
icsextendeduserprefs: ceDayHead=10
icsextendeduserprefs: ceDayTail=17
icsextendeduserprefs: ceDefaultAlarmEmail=jdoe@sesta.com
icsextendeduserprefs: ceDefaultAlarmStart=P30H
icsextendeduserprefs: ceDefaultTZID=America/New_York
icsextendeduserprefs: ceDefaultView=groupview
icsextendeduserprefs: ceFontFace=PrimaSans BT,Verdana,sans-serif
icsextendeduserprefs: ceFontSizeDelta=pref_font_size_group_3
icsextendeduserprefs: ceInterval=PT2H0M
icsextendeduserprefs: ceNotifyEmail=jdoe@sesta.com
icsextendeduserprefs: ceNotifyEnable=0
icsextendeduserprefs: ceSingleCalendarTZID=America/Los_Angeles
icsextendeduserprefs: ceToolText=1
icsextendeduserprefs: ceToolImage=1
```

OID

2.16.840.1.113730.3.1.742

icsFirstDay

Origin
Calendar Server

Syntax
cis, single-valued

Object Classes
icsCalendarUser

Definition
First day of the week to be displayed on user's calendar.

Range of values: 1–7, with 1 = Sunday, 2 = Monday, 3= Tuesday, 4 = Wednesday, 5 = Thursday, 6 = Friday, 7 = Saturday

Example
```
icsFirstDay: 1
```

OID
2.16.840.1.113730.3.1.743

icsFreeBusy

Origin
Not implemented.

Syntax
ces, single-valued

Object Classes

Definition
Reserved, not implemented.

Example

OID
2.16.840.1.113730.3.1.744

icsGeo

Origin
Not implemented.

Syntax
cis single-valued

Latitude; longitude

Object Classes

Definition
Reserved, not implemented.

Geographical location of user or resource.

Example
This class exists only for compliance with the RFC spec and is not used.

OID
2.16.840.1.113730.3.1.745

icsMandatorySubscribed

Origin
Calendar Server

Syntax
ces

Object Classes
icsCalendarDomain

Definition
The valid calendar IDs for mandatory subscribed calendars for all users in a domain.

Example
```
icsMandatorySubscribed: ConfRm1@sesta.com:meetings
```

OID
2.16.840.1.113730.3.1.746

icsMandatoryView

Origin
Calendar Server

Syntax
cis

Object Classes
`icsCalendarDomain`

Definition
The mandatory default view for all calendars in a domain. Views are: overview, day, week, month, year, comparison.

Example
```
icsMandatoryView: overview
```

OID
2.16.840.1.113730.3.1.747

icsPartition

Origin
Not implemented.

Syntax
cis, single-valued, ASCII

Object Classes
`icsCalendarResource`, `icsCalendarUser`

Definition
Reserved. not implemented.

The name of the partition that holds a calendar database. There is no default value.

Example
`icsPartition: partition1`

OID
1.3.6.1.4.1.42.2.27.9.1.4

icsPreferredHost

Origin
Not implemented.

Syntax
cis, single-valued

Object Classes

Definition
Reserved, not implemented.

Specifies the preferred host for this calendar. This attribute is used by clients to retrieve the front-end-host server name.

Example

OID
2.16.840.1.113730.3.1.749

icsQuota

Origin
Not implemented.

Syntax
int, single-valued

Object Classes

Definition
Reserved, not implemented.

Example

OID
2.16.840.1.113730.3.1.748

icsRecurrenceBound

Origin
Calendar Server

Syntax
int, single-valued

Object Classes
`icsCalendarDomain`

Definition
Maximum number of instances created for events and todos with infinite recurrence. The value is taken from the `ics.conf` setting `calstore.recurrence.bound`.

Example
```
icsRecurrenceBound: 60
```

OID
2.16.840.1.113730.3.1.750

icsRecurrenceDate

Origin
Calendar Server

Syntax
cis, single-valued

Object Classes
`icsCalendarDomain`

Definition
An ISO8601 date / time string specifying the maximum date for events and todos with infinite recurrence.

Example
`icsRecurrenceDate: 20300365T115959Z`

OID
2.16.840.1.113730.3.1.751

icsRegularExpressions

Origin
Calendar Server.1

Syntax
ces, multi-valued, UTF8

Object Classes
`icsCalendarDWPHost`

Definition
Stores regular expressions used to divide the LDAP database between servers.

Example
`icsRegularExpressions: A–F,G–L,M–T,U–Z`

A–F, G–L, M–T, U–Z are possible values for instances of this attribute and describe a database divided alphabetically between four servers.

OID
1.3.6.1.4.1.42.2.27.9.1.2

icsSessionTimeout

Origin
Calendar Server

Syntax
int, single-valued

Object Classes
icsCalendarDomain

Definition
Number of seconds of inactivity before a user session is timed out. Read from ics.conf setting service.http.idletimeout.

Example
icsSessionTimeout: 600

OID
2.16.840.1.113730.3.1.752

icsSet

Origin
Calendar Server

Syntax
cis, multi-valued

Object Classes
icsAnonymousSet,icsCalendarUser,icsDefaultAnonymousSet

Definition
Defines one group of calendars. End users create these groups for various tasks. Each group is represented by one icsSet attribute, that is, for every group the user creates there will be one icsSet attribute. For example, if the user has three groups defined, there will be three icsSet attributes.

The value for this attribute is a six-part string, with each part separated by a dollar sign ($).

The following table shows the six parts of this attribute's value:

Table 3-4 Six Parts of the Attribute Value

Part	Required?	Description
name	Required	The display name of this group.
calendars	Required	A semi-colon-separated list of calendar IDs (calid) that comprise this group.

Table 3-4 Six Parts of the Attribute Value *(Continued)*

Part	Required?	Description
`tzmode`	Required	Three possible values: `default`, `inherit`, `specify`. The value that tells where the time zone for this group comes from. `default` – take user's default time zone `inherit` – take the time zone of the first calendar in the group `specify` – take the time zone from the `tz` value that follows.
`tz`	Not Required, unless `tzmode = specify`	A valid time zone for this group. For a list of acceptable values, see Standard Time Zones. Value is optional unless `tzmode = specify`, then it is required.
`mergeInDayView`	Required	A boolean (TRUE/FALSE). The value tells whether to display this group in the Day view (TRUE) or the Comparison view (FALSE)
`description`	Not Required	Character string. Optional description of the calendar.

Example

The value of this attribute should all be on one line or if you wish to break a line, start the next line with a single space or tab.

```
icsSet: name=GroupName$calendars=calid1;calid2;calid3$
 tzmode=specify$tz=America/Los_Angeles$mergeInDayView=FALSE$
 description=Example group of calendars.
```

OID

2.16.840.1.113730.3.1.753

icsSourceHtml

Origin

Calendar Server

Syntax

ces, single-valued

Object Classes

`icsCalendarDomain`

Definition

The alternate location of all client HTML files. A directory path that is relative to the installed client HTML files. The default value comes from the `ics.conf` setting `service.http.uidir.path`.

Table 3-5 lists the values for this attribute.

Table 3-5 Alternate Locations for Client HTML files.

Parameters	Value	Definition
`sourceUrl`	directory	Directory relative to executable, where all URL references to files are stored.
`uiDirPath`	directory	Directory containing the default client. If only WCAP access is allowed, value is “”.
`calHostname`	hostname	HTTP host for retrieving HTML documents.

Example

```
icsSourceHtml: calHostname=calhost1
```

OID

2.16.840.1.113730.3.1.754

icsStatus

Origin

Calendar Server

Syntax

cis, single-valued

Object Classes

`inetDomain`

Definition

This attribute must be set when assigning calendar services to a domain. The attribute describes the status of this domain's calendar service. Calendar status, with one of the values specified in Table 3-6:

Table 3-6 Calendar Status Values

Status	Definition
`active`	Users and resources in this domain have access to calendar services.
`inactive`	No calendar services allowed for any users or resources in this domain, until the status is changed to `active` again. Calendars remain in the database and the LDAP entry remains.
`deleted`	No calendar service allowed for any users or resources in this domain. It is marked for deletion. Calendars will be removed from the database and the LDAP attributes that control the calendar's service will be removed. All the entries remain in the directory, but object classes having to do only with calendars for these users, resources and domains will be removed. For example, `icsCalendarUser`, `icsCalendarResource`, `icsCalendarDomain` will be removed. In addition all attributes with the `ics` prefix will be removed. For resources, it means that the resources associated with this object are to be removed from the calendar system, but the entry remains in the directory. For domains, all calendars associated with all the users and resources within that domain are to be removed.

If this attribute is not set, the icsAllowedServiceAccess attribute is checked. If present and the value of that attribute is `http`, then calendar services are disabled for the user (the user status is `inactive`). If icsAllowedServiceAccess has any other value, or if both attributes are missing, then the default user status is `active`.

Calendar services evaluate the following status attributes in order:`inetDomainStatus`, `icsStatus` (for `icsCalendarDomain`), either `inetResourceStatus` or `inetUserStatus`, and `icsStatus` (for either `icsCalendarResource` or `icsCalendarUser`).

The rule is: the first of these attributes that is set to something other than `active` takes precedence over all the others.

Example

```
icsStatus: active
```

OID

2.16.840.1.113730.3.1.755

icsSubscribed

Origin
Calendar Server

Syntax
ces, multi-valued

Object Classes
icsCalendarUser

Definition
List of calendars to which this user is subscribed. This includes all the calendars that the user owns, as well as any calendars owned by others to which the owner subscribes.

The value of this attribute is the calendar ID and optionally, the calendar name, with a dollar sign ($) between them, when present.

Example
```
icsSubscribed: jdoe$MyHomeCalendar
icsSubscribed: jsmith
```

OID
2.16.840.1.113730.3.1.756

icsTimezone

Origin
Calendar Server

Syntax
cis

Object Classes
icsCalendarResource, icsCalendarUser

Definition
The default time zone for this user or resource calendar if one is not explicitly assigned through their own user preferences (see `icsExtendedUserPrefs`). Specifically a valid time zone from the list found in "Standard Time Zones" on page 265. The value is taken from the `ics.conf` setting `calstore.default.timezoneID`.

Example
```
icsTimezone: America/Chicago
```

OID
2.16.840.1.113730.3.1.757

inetCanonicalDomainName

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetDomainAuthInfo`

Definition
Used both in LDAP Schema 1 and compatibility mode for LDAP Schema 2 (with a DC Tree). This attribute is a fully qualified domain name. For an explanation of native and compatibility mode LDAP structures, see the *Sun Java™ Enterprise System Installation Guide*.

In compatibility mode, if more than one DC node in a DC tree refers to the same organization node in the Organization tree, this attribute is used to specify the canonical domain name used by the mail processes to open users' mailboxes. (There can be only one canonical domain name per organization node, but there can be many DC nodes referring to the same organization node)

This attribute is not necessary if there is only one DC node referring to an organization node. If the attribute is missing, the DC node entry is taken for the canonical domain name.

If this attribute is missing and there are multiple DC nodes referring to the same organization node, the mail processes could possibly use the wrong domain name when trying to open users' mailboxes.

Using multiple domain nodes to point to the same organization node allows you to have different attribute settings (and therefore different routing) for each one. If you want to be sure the two domains have the same attribute settings (are routed identically), use `aliasedObjectName` on the duplicate node instead.

This attribute is not used for the LDAP Schema 2 native mode LDAP data model.

Example

For the corporation `sesta.com`, if two DC nodes exist, `dc=sesta` and `dc=sesta2`, both referring to the organization node `o=sesta`, then you must specify one of them in the attribute:

```
inetCanonicalDomainName: sesta.com
```

Thus:

```
dn: dc=sesta,dc=com,o=internet
inetDomainBaseDN: o=sesta.com
inetCanonicalDomainName: sesta.com

dn: dc=sesta2,dc=com,o=internet
inetDomainBaseDN: o=sesta.com
```

OID

2.16.840.1.113730.3.1.701

inetCoS

Origin

Messaging Server 5.0

Syntax

cis, single-valued

Object Classes

`ipUser`

Definition

(Organization tree domain) Specifies the name of the Class of Service (CoS) template supplying values for attributes in the user entry. The RDN of the CoS template is the value of this attribute. Attribute values provided by the template and any override rules are specified in the CoS definition. CoS definitions are

created by using the object class `cosDefinition`. The value of attribute `cosSpecifier` in CoS definition entry is set to `inetCoS`. Create CoS definitions and templates in the container `ou=CoS` in the subtree for that domain. See the *iPlanet Messaging Server 5.2 Provisioning Guide* for more information.

Example
`inetCoS: HallofFame`

OID
2.16.840.1.113730.3.1.706

inetDomainBaseDN

Origin
Messaging Server 5.0

Syntax
dn, single-valued

Object Classes
`inetDomain`

Definition
This attribute decorates domain nodes on the DC Tree when in compatibility mode. It is not used for native mode LDAP Schema 2.

The two domains, the alias and the referenced domain, can have different attribute values, such that routing will differ between the two. If you want to ensure routing is the same, the attribute values of both domains must be identical.

DN of the organization's subtree where all user/group entries are stored. This attribute points to a valid Organization subtree DN. Messaging Server components using the RFC 2247 search (compatibility mode) must resolve this DN in order to search for user and group entries that correspond to the hosted organization.

Example
`inetDomainBaseDN: o=sesta.com,o=siroe-isp.com`

OID
2.16.840.1.113730.3.1.690

inetDomainCertMap

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
inetDomainAuthInfo

Definition
Reserved.

Example
TBD

OID
2.16.840.1.113730.3.1.700

inetDomainSearchFilter

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetDomainAuthInfo

Definition
LDAP search filter to use in search templates when performing a native mode search. The compatibility mode RFC 2247 algorithm search requires this attribute, but ignores its value.

Used during authentication to map login name in that domain to an LDAP entry.

The following variables can be used in constructing the filter:

- %U–Name part of the login name (that is, everything before the login separator stored in the servers configuration).

- %V–Domain part of the login string .

If this attribute is missing, it is equivalent to:

```
(&(objectclass=inetOrgPerson)(uid=%U))
```

Namespaces where users are provisioned with compound uids, such as uid=john_siroe.com, where john is the userID and siroe.com is the domain, would use a search filter of uid=%U_%V. This maps a login string of john@siroe.com (where @ is the login separator for the service) into a search request by the service for an entry's namespace of siroe.com, where uid=john_siroe.com.

An alternate example of using this attribute would be for sites wanting to log people in based on their employee identification. Assuming the attribute empID in user entries stores employee identifications, the search filter would be:

```
(&(objectclass=inetOrgPerson)(empID=%U)).
```

This attribute must return a unique match for valid users within the inetDomainBaseDN subtree.

Example

```
inetDomainSearchFilter: uid=%U
```

OID

2.16.840.1.113730.3.1.699

inetDomainStatus

Origin

Messaging Server 5.0

Syntax

cis, single-valued

Object Classes

inetDomain

Definition

Applications using a DC Tree as their entry point (RFC 2247 compliant compatibility mode LDAP data model) may choose to respect application specific status attributes, but must consume and respect this attribute on the affiliated physical node (Organization Tree). In other words, for compatibility mode, both the DC Tree and the Organization Tree contain this attribute and if the two attribute's values differ, the one on the Organization Tree will take precedence.

Specifies the global status of a domain for all services. The intent of this attribute is to allow the administrator to temporarily suspend and then reactivate access, or to permanently remove access, by the domain and all its users to all the services enabled for that domain.

This attribute takes one of three values. Supported values are:

Table 3-7 Status Attribute Values

Value	Description
active	Domain is active and users in the domain may use services enabled by the overlay of service-specific object classes and the service state as indicated by the particular status attribute for that service.
inactive	Domain is inactive. The account may not use any services granted by service-specific object classes. This state overrides individual service status set using the service's status attributes.
deleted	Domain is marked as deleted. The account may remain in this state within the directory for some time (pending purging of deleted users). Service requests for all users in a domain marked as deleted will return permanent failures.

A missing value implies status is `active`. An illegal value is treated as `inactive`.

There are four status attributes that mail services look at and which are evaluated in this order: `inetDomainStatus`, `mailDomainStatus`, `inetUserStatus`, and `mailUserStatus`. The rule is: the first of these attributes that is set to something other than `active` takes precedence over all the others.

Similarly, this attribute is used for calendar services when evaluating status. The status attributes used are: `inetDomainStatus`, `icsStatus` (of `icsCalendarDomain`), either `inetResourceStatus` or `inetUserStatus`, and `icsStatus` (of either `icsCalendarResource` or `icsCalendarUser`).

In addition, in compatibility mode, when this attribute decorates both the DC Tree and the Organization Tree, both attributes should agree. Administrators are responsible for keeping the two synchronized. If the two attributes do not have the same value, Messaging Server will use the value found in the Organization Tree, while some other legacy application might be using the DC Tree attribute only. This could cause unpredictable results.

For more information on native and compatibility mode LDAP schemes, see the *Sun Java™ Enterprise System Installation Guide*.

Example

```
inetDomainStatus: active
```

OID

2.16.840.1.113730.3.1.691

inetMailGroupStatus

Origin

Messaging Server 5.0

Syntax

cis, single-valued

Object Classes

`inetMailGroup`

Definition

Current status of a mail group.

The following table lists the possible status values and gives a description of each:

`active`	Messages are delivered to the members of the mailing list.
`inactive`	Messages sent to the mailing list result in a transient failure.
`deleted`	Mailing list can be purged from the directory. Messages sent to the group return a permanent failure.

A missing value implies status is `active`. An illegal value is treated as `inactive`.

There are four status attributes that interact with each other: inetDomainStatus, mailDomainStatus, inetGroupStatus, and inetMailGroupStatus. These are considered in the order just given. The first one with a status of active takes precedence over the setting of all the others.

The MTA option LDAP_GROUP_STATUS can be used to specify a different attribute to be used for group status.

Example

```
inetMailGroupStatus: active
```

OID

2.16.840.1.113730.3.1.786

inetResourceStatus

Origin

Calendar Server

Syntax

cis, single-valued

Object Classes

inetResource

Definition

This is a global status for resources. It holds the current status of the resource: active, inactive, or deleted for all services. It is used by Identity Server to manage resources. Status changes can be made to a resource's status using the commcli interface, or by directly changing the LDAP entry for the group.

The following table lists the attribute's values and their meanings:

Table 3-8 Status Attribute Values

Value	Description
active	The resource is active and it may be used in services enabled by the overlay of service-specific object classes and the service state as indicated by the particular status attribute for that service.
inactive	Resource is inactive. The resource may not be used in any services granted by service-specific object classes. This state overrides individual service status set using the service's status attributes.

Table 3-8 Status Attribute Values

Value	Description
deleted	Resource is marked as deleted. The resource may remain in this state within the directory for some time (pending purging of deleted resources). Service requests for all resources marked as deleted will return permanent failures.

There are several status attributes that are evaluated to determine status. They are evaluated in this order: `inetDomainStatus`, `icsStatus` (for `icsCalendarDomain`), `inetResourceStatus`, `icsStatus` (for `icsCalendarResource`). These are considered in the order just given. The first one with a status of `active` takes precedence over the setting of all the others.

Example

```
inetResourceStatus: active
```

OID

2.16.840.1.113730.3.1.758

inetSubscriberAccountId

Origin

Messaging Server 5.0

Syntax

cis, multi-valued

Object Classes

`inetSubscriber`

Definition

A unique account ID used for billing purposes.

Example

```
inetSubscriberAccountId: A3560B0
```

OID

2.16.840.1.113730.3.1.694

inetSubscriberChallenge

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetSubscriber`

Definition
Attribute for storing the challenge phrase used to identify the subscriber. Used in conjunction with the `inetSubscriberResponse`.

Example
`inetSubscriberChallenge=Mother's Maiden Name`

OID
2.16.840.1.113730.3.1.695

inetSubscriberResponse

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetSubscriber`

Definition
Attribute for storing the response to the challenge phrase.

Example
`inetSubscriberResponse=Mamasita`

OID
2.16.840.1.113730.3.1.696

inetUserHttpURL

Origin
Messaging Server 5.0, deprecated in Messaging Server 6.0

Syntax
cis, single-valued

Object Classes
`inetUser`

Definition
This attribute is deprecated for the user class `inetUser` starting in Messaging Server 6.0 and is likely to be removed from the object class in future versions of the schema.

User's primary URL for publishing Web content. This is an informational attribute and may be used in phonebook-type applications. It is not intended to have any operational impact.

Example
```
inetUserHttpURL: http://www.siroe.com/theotis
```

OID
2.16.840.1.113730.3.1.693

inetUserStatus

Origin
Messaging Server 5.0, Calendar Server 5.1.1

Syntax
cis, single-valued

Object Classes
`inetUser`

Definition
Specifies the status of a user's account with regard to global server access.This attribute enables the administrator to temporarily suspend, reactivate, or permanently remove access to all services for a user account.

The following table lists the values for this attribute:

Table 3-9 Status Attribute Values

Values	Description
active	The user account is active and the user can use all services enabled by the overlay of service-specific object classes and the service state as indicated by the particular status attribute for that service. For example, a user can use the email system if both `mailUserStatus` and `inetDomainStatus` are set to `active`.
inactive	The user account is inactive. The account cannot use any services granted by service-specific object classes. This state overrides individual service status set using the service's status attributes.
deleted	The account is marked as deleted. The account can remain in this state within the directory for some time (pending purging of deleted users). Service requests for a user marked as deleted must return permanent failures.

A missing value implies status is `active`. An illegal value is treated as `inactive`.

There are four status attributes that mail services look at and which are evaluated in this order: `inetDomainStatus`, `mailDomainStatus`, `inetUserStatus`, and `mailUserStatus`. The rule is: the first of these attributes that is set to something other than `active` takes precedence over all the others.

For calendar services, the attributes evaluated are: `inetDomainStatus`, `icsStatus` (for `icsCalendarDomain`), `inetUserStatus`, `icsStatus` (for `icsCalendarUser`).

When this attribute applies to a static group, defined using the inetUser object class, inactivating (disabling) the group only applies to the group itself and not the users in the group.

To disable the users of a group, create a dynamic group by assigning roles to the users, and then disable the role (which disables all users assigned to that role). For more information about roles, see the *Sun Java™ System Directory Server Administrator's Guide.*

The MTA option `LDAP_USER_STATUS` can be used to specify a different attribute to be used for user status.

Example

```
inetUserStatus=inactive
```

OID

2.16.840.1.113730.3.1.692

mail

Origin
Messaging Server 5.0

Syntax
cis, single-valued (RFC 822 address)

Object Classes
`inetLocalMailRecipient`, `icsCalendarResource`, `icsCalendarUser`

Definition
Identifies a user's primary email address (the email address retrieved and displayed by white-pages lookup applications).

This attribute and `mailAlternateAddress`, are the default attributes used for reverse searches.

Example
`mail=jdoe@sesta.com`

OID
0.9.2342.19200300.100.1.3

mailAccessProxyPreAuth

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`mailDomain`

Definition
Attribute tells the MMP if the users in this domain have to be preauthenticated. Permitted values are `yes` or `no`.

Example
`mailAccessProxyPreAuth=yes`

OID
2.16.840.1.113730.3.1.769

mailAccessProxyReplay

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`mailDomain`

Definition
This attribute tells the Messaging Multiplexor how to reconstruct the login string when replaying the login sequence with the backend mail server. A missing attribute implies that the message access proxies construct the replay string based on the login name used by the client, the domain of the client, and the login separator used for this service. The `mailAccessProxyReplay` attribute overrides this default behavior when the message access proxy has a different backend server than Communications Services.

The syntax is that of a login string, with the following substitutions:

- `%U`: Login name. That is, the name part of the login string, if it is a {name,domain} compound.
- `%V`: Domain part of the login string.
- `%[attr]`: The value of the LDAP user attribute.

Examples

1. If the client logs in as `hugo` and the domain associated with the server IP address used is `yoyo.com`, and `mailAccessProxyReplay=%U@%V`, the replayed login string is `hugo@yoyo.com`.
2. If the client logs in as `hugo`, and the domain associated with the server IP address used is `yoyo.com`, and `mailAccessProxyReplay=%[surname]@%V`, the replayed login string is the value of the surname attribute of the client.
3. If the client logs in as `hugo+yoyo.com`, and the login separator for the service used is `+`, and `mailAccessProxyReplay=%U@%V`, the replayed login string is `hugo@yoyo.com`.

4. If the client logs in as `hugo`, and the domain associated with the server IP address used is `yoyo.com`, and `mailAccessProxyReplay` is not defined, and the login separator for the service used is `+`, the replayed login string is `hugo+yoyo.com`.

OID
2.16.840.1.113730.3.1.763

mailAdminRole

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailAdministrator`

Definition
Specifies the administrative role assigned to the members of the group. The only legal value for this attribute is `storeAdmin`. The object class that contains this attribute—`inetMailAdministrator`—is overlaid on a group entry to grant members of a group administrative privileges over part of the mail server. Currently the only privilege group members inherit are rights to perform proxy authentication for any user in the domain. These rights extend over users in the same domain as where the group is defined. To grant such privileges the attribute `mailAdminRole` must be set to the value `storeAdmin`.

Example
```
mailAdminRole: storeAdmin
```

OID
2.16.840.1.113730.3.1.780

mailAllowedServiceAccess

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailUser

Definition
Stores access filters (rules). If no rules are specified, then user is allowed access to all services from all clients. Rules are separated by a dollar sign ($). The rules are evaluated in this manner:

- Access is granted if the client information matches an allow filter for that service.
- Access is denied if the client information matches a deny filter for that service.
- If no match is made with any allow or deny filters, access is granted, except in the case where there are allow filters but no deny filters. In this case, a lack of match means access is denied.

For a full explanation of access filters and an alternate way to control access through the administration console or the `config` utility, see "Configuring Client Access to POP, IMAP, and HTTP Services" in the *Messaging Server Administration Guide*.

Rule Syntax

`"+" or "-"service_list":"client_list`

`+` (allow filter) means the services in the service list are being granted to the client list.

`-` (deny filter) means the services are being denied to the client list.

`service_list` is a comma separated list of services to which access is being granted or denied.

Legal service names are: `imap`, `imaps`, `pop`, `pops`, `smtp`, `smtps`, and `http`. Note that the MMP supports `imap`, `imaps`, `pop`, `pops`, and `smtp`. The backend supports `imap`, `pop`, `smtp`, and `http`.

`client_list` is a comma separated list of clients (domains) to which access is being granted or denied.

Wildcards can be substituted for the client list (domains). The following table shows the legal wildcards and gives a description of each:

Table 3-10 Wildcards

Wildcards	Description
ALL, *	The universal wildcard. Matches all names.
DNSSPOOFER	Matches any host whose DNS name does not match its own IP address.
KNOWN	Matches any host whose name and address are known. Use with care.
LOCAL	Matches any local host (one whose name does not contain a dot character). If your installation uses only canonical names, even local host names will contain dots and thus will not match this wildcard.
UNKNOWN	Matches any host whose name or address are unknown. Use this with care.

The following wildcards can be used for the service list: *, ALL.

Except Operator

The access control system supports a single operator, EXCEPT. You can use the EXCEPT operator to create exceptions to the patterns found in a rule's service list and client list. EXCEPT clauses can be nested. If there are multiple EXCEPT clauses in a rule, they are evaluated right to left.

The EXCEPT format is:

```
list1 EXCEPT list2
```

where `list1` is a comma separated list of services and `list2` is a comma separated lists of clients.

Example

This example shows a single rule with multiple services and a single wildcard for the client list.

```
mailAllowedServiceAccess: +imap,pop,http:*
```

This example shows multiple rules, but each rule is simplified to have only one service name and uses wildcards for the client list. (This is the most commonly used method of specifying access control in LDIF files.)

```
mailAllowedServiceAccess: +imap:ALL$+pop:ALL$+http:ALL
```

An example of how to disallow all services for a user is:

```
mailAllowedServiceAccess: -imap:*$-pop:*$-http:*
```

An example of a rule with an EXCEPT operator is:

```
mailAllowedServiceAccess: -ALL:ALL EXCEPT server1.sesta.com
```

This example denies access to all services for all clients except those on the host machine `server1.sesta.com`.

OID
2.16.840.1.113730.3.1.777

mailAlternateAddress

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`inetLocalMailRecipient`, `pabPerson`

Definition
Alternate RFC 822 email address of this recipient. If the MTA receives mail with a "from" header with this email address, it rewrites the header with the value of the `mail` attribute and routes the email to that inbox. The `mailEquivalentAddress` attribute works similarly to route the email, but does not rewrite the header.

The local part of the address may be omitted to designate a user/group as the catchall address. A catchall domain address is an address that will receive mail to a specified domain if the MTA does not find an exact user address match with that domain.

This attribute, along with `mail`, are the default attributes used for reverse searches.

Example

```
mailAlternateAddress: jdoe@sesta.com
```

```
mailAlternateAddress: @sesta.com (catchall domain address)
```

OID
2.16.840.1.113730.3.1.13

mailAntiUBEService

Origin
Messaging Server 5.2

Syntax
cis, multi-valued

Object Classes
inetMailUser, mailDomain

Definition
The string values given by this and other optin attributes are collected and passed to the filtering agent being used (for instance, Brightmail).

For Brightmail spam and virus checking, the interpretation of these strings is specified in the Brightmail configuration file. Brightmail uses the information from this attribute for its processing.

There are two Brightmail values:

- spam – When a spam message is found by the anti-UBE service, take the action specified in a system wide configuration option.
- virus - When a virus in a message is detected by the anti-UBE service, take the action specified in a system wide configuration option.

SpamAssasin, another filtering agent, does not use the actual value of the attribute; it can be set to anything.

While another attribute can be named in the option.dat setting for LDAP_OPTIN, it is not recommended. (For more information on Brightmail, see the *Messaging Server Administration Guide*.)

To use this attribute to specify per user optin values, set the following in the option.dat file:

```
LDAP_OPTIN=mailAntiUBEService
```

To use the attribute to specify domain level optin values, set the following in the option.dat file:

```
LDAP_DOMAIN_ATTR_OPTIN=mailAntiUBEService
```

Example

```
mailAntiUBEService: virus
```

```
mailAntiUBEService: spam
```

OID

mailAutoReplyMode

Origin
Messaging Server 5.0 (for reply mode), Messaging Server 5.2 patch 1 (for echo mode)

Syntax
cis, single-valued

Object Classes
`inetMailUser`

Definition
Specifies the autoreply mode for user mail account. This is one of several autoreply attributes used when autoreply is an active mail delivery option. The two modes for autoreply are:

- `echo` – Echo the original message with the added `mailAutoReplyText` or `mailAutoReplyTextInternal` to the original sender. This occurs only once a week per sender.

  If you want the message to be echoed for each message from every sender regardless of how recently a previous reply was sent, set the `mailAutoReplyTimeOut` to `0`, which will cause the reply message to be sent every time.

- `reply` – Send a fixed reply, contained in attributes `mailAutoReplyText` or `mailAutoReplyTextInternal`, to the original sender.

Example
```
mailAutoReplyMode: reply
```

OID
2.16.840.1.113730.3.1.14

mailAutoReplySubject

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailUser

Definition
Subject text of auto-reply response. $SUBJECT can be used to insert the subject of the original message into the response.

Example
```
mailAutoreplySubject: I am on vacation
```

OID
2.16.840.1.113730.3.1.772

mailAutoReplyText

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailUser

Definition
Auto-reply text sent to all senders except users in the recipient's domain. If not specified, external users receive no auto response.

Example
```
mailAutoreplyText: Please contact me later.
```

OID
2.16.840.1.113730.3.1.15

mailAutoReplyTextInternal

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailUser`

Definition
Auto-reply text sent to senders from the recipients domain. If not specified, then internal uses get the mail auto-reply text message.

Example
```
mailAutoreplyTextInternal: Please contact me later.
```

OID
2.16.840.1.113730.3.1.773

mailAutoReplyTimeOut

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
`inetMailUser`

Definition
Duration, in hours, for successive auto-reply responses to any given mail sender. Used only when `mailAutoReplyMode: reply`. If the value is set to `0` for `mailAutoReplyMode: echo` then a response is sent back every time a message is received. Auto-reply responses are sent out only if the recipient is listed in the “to” or “cc:” of the original message.

Example
```
mailAutoreplyTimeout: 48
```

OID
2.16.840.1.113730.3.1.771

mailClientAttachmentQuota

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
`mailDomain`

Definition
A positive integer value indicating the number of attachments the Messenger Express user can send per message in this domain. A value of `-1` means no limit on attachments.

Example
```
mailClientAttachmentQuota: 12
```

OID
2.16.840.1.113730.3.1.768

mailConversionTag

Origin
iPlanet Messaging Server 5.2

Syntax
cis, multi-valued (ASCII string)

Object Classes
`inetMailGroup, inetMailUser`

Definition
Method of specifying unique conversion behavior for a user or group entry. A message sent to this user or group will match any conversion file entries that require the specified value of the tag. (Any string value can be associated with this attribute.)

Tag-specific conversion actions are specified in the MTA configuration.

The MTA option used to override this attribute is `LDAP_CONVERSION_TAG`.

Example

OID

mailDeferProcessing

Origin
iPlanet Messaging Server 5.2

Syntax
cis, single-valued (ASCII string)

Object Classes
`inetMailGroup, inetMailUser`

Definition
Controls whether or not address expansion of the current user or group entry is performed immediately (value is “No”), or deferred (value is “Yes”).

NOTE A different attribute (other than `mailDeferProcessing`) can be designated for this purpose in the MTA option `LDAP_REPROCESS`.

Deferral takes place if the value is “Yes” and the current source channel isn’t the reprocess channel. Deferral is accomplished by directing the user or group’s address to the reprocess channel. That is, the expansion of the alias is aborted and the original address (user@domain) is queued to the reprocess channel.

If this attribute does not exist, the setting of the deferred processing flag associated with delivery options processing is checked. If it is set, processing is deferred.

If it is not set, the default for users is to process immediately (as if the value of this attribute were “No”).

The default for groups (such as mailing lists) is controlled by the MTA option DEFER_GROUP_PROCESSING, which defaults to 1 (yes).

Best Practices Suggestions for Duplicate Message Problem

Getting duplicate copies of messages can happen. For example, if a user sends an email to both addresseeA, and groupA that contains addresseeA, and DEFER_GROUP_PROCESSING=1 and this attribute is No, then the message immediately duplicates, such that addresseeA gets two copies, one that came directly, and one that took the deferred expansion hop through the reprocess channel for groupA to get expanded.

While disabling deferred group expansion would eliminate the duplicate, that's not a good idea if you have a lot of large groups. Using expandlimit 1 can potentially cause unnecessary overhead on general, non-group, multi-recipient messages.

To minimize the effect of this situation, the following two solutions are best practices:

- For installations with only a few small groups, setting the default DEFER_GROUP_PROCESSING=1, and this attribute to No, gives you duplicates but also gives you two major benefits:
  - You don't have to bother running the reprocess channel, which makes a bit less overhead and a bit faster delivery.
  - The potential for eliminating duplicate addresses is increased.
- If your installation has many small groups and only a few large groups, then set DEFER_GROUP_PROCESSING=0, and this attribute to Yes for the few large groups.

Example

The default for mail users:

```
mailDeferProcessing: No
```

The default for mailing lists:

```
mailDeferProcessing:Yes
```

OID

TBD

mailDeliveryFileURL

Origin
Messaging Server 5.0

Syntax
ces, single-valued

Object Classes
`inetMailGroup`

Definition
Fully qualified local path of file to which all messages sent to the mailing list are appended. Used in conjunction with `mailDeliveryOption: file`.

The MTA option used to override this attribute's value is `LDAP_PROGRAM_FILE`.

Example
```
mailDeliveryFileURL: /home/dreamteam/mail_archive
```

OID
2.16.840.1.113730.3.1.787

mailDeliveryOption

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`inetMailGroup`, `inetMailUser`

Definition
Specifies delivery options for the mail recipient. One or more values are permitted on a user or group entry, supporting multiple delivery paths for inbound messages. Values will apply differently depending on whether the attribute is used in `inetMailGroup` or `inetMailUser`.

Note, that the mailUserStatus attribute is processed before this attribute. If mailUserStatus is set to hold, an internal flag is set so that when mailDeliveryOption is processed, the mailUserStatus hold overrides whatever delivery options are specified with mailDeliveryOption.

For users, delivery addresses are generated for each valid delivery option value.

Valid values are:

For users only (inetMailUser):

- autoreply – Specifies autoreply is turned on for the user. Messages on which the recipient is listed in the "To:" or "Cc:" header fields of the message are sent to the autoreply channel where an autoreply message is generated and sent to the original sender.
- hold – A recipient is temporarily halted from receiving messages. Note that unlike mailUserStatus, hold for this attribute does not disallow POP, IMAP and WebMail access. For this attribute, hold only halts delivery to the recipient's mailbox, but access is still allowed.
- mailbox – Deliver messages to the user's IMAP / POP store.
- native or unix – Deliver messages to the user's /var/mail store INBOX. The store is in Berkeley mailbox format. Messaging Server does not support /var/mail access. Users must use UNIX tools to access mail from the /var/mail store.

For groups only (inetMailGroup):

- file – Messages are appended to the file specified in the attribute mailDeliveryFileURL.
- members – Messages are sent to members of the mailing list. If missing, default=members is assumed.
- members_offline – To defer processing for this group, set the attribute to this value, and set the option.dat file option DEFER_GROUP_PROCESSING to zero (0).

Both users and groups:

These values are handled the same for both users and groups.

- program – Messages are delivered to a program, which is on the approved list of programs (specified in MTA's configuration). The name of the program is specifed in the attribute mailProgramdeliveryInfo.

- `forward` – Specifies that messages will be forwarded. The forwarding address is specified in the attribute `mailForwardingAddress`. Note that when this value is set, `mailForwardingAddress` must be set to keep the mail system in sync.

The MTA option `DELIVERY_OPTIONS`, found in the *`msg_svr_base`*`/config/option.dat` file, defines how each of the previously listed values will be processed.

The MTA option used to override this attribute's value is `LDAP_DELIVERY_OPTION`.

Example
`mailDeliveryOption: mailbox`

OID
2.16.840.1.113730.3.1.16

mailDomainAllowedServiceAccess

Origin
Messaging Server 5.0

Syntax
cis, single valued

Object Classes
`mailDomain`

Definition
Stores access filters (rules). If no rules are specified, then domain is allowed access to all services from all clients. Rules are separated by a dollar sign ($). The rules are evaluated in this manner:

- Access is granted if the client information matches an allow filter for that service.
- Access is denied if the client information matches a deny filter for that service.
- If no match is made with any allow or deny filters, access is granted, except in the case where there are allow filters but no deny filters. In this case, a lack of match means access is denied.

For a full explanation of access filters and an alternate way to control access through the administration console or the `config` utility, see “Configuring Client Access to POP, IMAP, and HTTP Services” in the *Messaging Server Administration Guide*.

Rule Syntax

"+" or "-" `<service_list>":"<client_list>`

+ (allow filter) means the service list services are being granted to the client list.

- (deny filter) means the services are being denied to the client list.

`service_list` is a comma separated list of services to which access is being granted or denied.

Legal service names are: `imap, imaps, pop, pops, smtp, smtps,` and `http`. Note that the MMP supports `imap`, `imaps`, `pop`, `pops`, and `smtp`. The backend supports `imap`, `pop`, `smtp`, and `http`.

`client_list` is a comma separated list of clients (domains) to which access is being granted or denied.

Wildcards can be substituted for the client list (domains). The following table shows the allowed wildcards and describes each of them:

Table 3-11 Wildcards

Wildcards	Meanings
ALL, *	The universal wildcard. Matches all names.
DNSSPOOFER	Matches any host whose DNS name does not match its own IP address.
KNOWN	Matches any host whose name and address are known. Use with care.
LOCAL	Matches any local host (one whose name does not contain a dot character). If your installation uses only canonical names, even local host names will contain dots and thus will not match this wildcard.
UNKNOWN	Matches any host whose name or address are unknown. Use this with care.

The following wildcards can be used for the service list: *, `ALL`.

Except Operator

The access control system supports a single operator, EXCEPT. You can use the EXCEPT operator to create exceptions to the patterns found in a rule's service list and client list. EXCEPT clauses can be nested. If there are multiple EXCEPT clauses in a rule, they are evaluated right to left.

The EXCEPT format is:

```
list 1 EXCEPT list 2
```

A list is a comma separated list of services or clients.

Example

This example shows a single rule with multiple services and a single wildcard for the client list.

```
mailDomainAllowedServiceAccess: +imap,pop,http:*
```

This example shows multiple rules, but each rule is simplified to have only one service name and uses wildcards for the client list.

```
mailDomainAllowedServiceAccess:  +imap:ALL$+pop:ALL$+http:ALL
```

The second example is probably the most commonly used in Messaging Server LDIF files.

An example of a rule with an EXCEPT operator is:

```
mailDomainAllowedServiceAccess: -ALL:ALL EXCEPT server1.sesta.com
```

This example denies access to all services for all clients except those on the host machine `server1.sesta.com`.

OID

2.16.840.1.113730.3.1.764

mailDomainCatchallAddress

Origin

iPlanet Messaging Server 5.2

Syntax

cis, single-valued (RFC 822 mailbox)

Object Classes
mailDomain

Definition
Specifies an address to be substituted for any address in the domain that doesn't match any user or group in the domain.

The MTA option used to override this attribute's value is LDAP_DOMAIN_ATTR_CATCHALL_ADDRESS.

Example

OID
TBD

mailDomainConversionTag

Origin
iPlanet Messaging Server 5.2

Syntax
cis, multi-valued (ASCII string)

Object Classes
mailDomain

Definition
Method of specifying unique conversion behavior for any user in the domain. A message sent to a user in this domain will match any conversion file entries that require the specified value of the tag. (Any string value can be associated with this attribute.)

Tag-specific conversion actions are specified in the MTA configuration.

The MTA option used to override this attribute's value is LDAP_DOMAIN_ATTR_CONVERSION_TAG.

Example

OID
TBD

mailDomainDiskQuota

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
`mailDomain`

Definition
Disk quota, in bytes, for all users in the domain. If domain quota enforcement is activated, then domains exceeding this quota stop receiving more messages until the domain messages no longer exceed the quota. Domain quota enforcement is activated using the command `imquotacheck -f -d <domain>`.

A value of -1 specifies no limit. This is the default.

Example
`mailDomainDiskQuota: 50000000000`

OID
2.16.840.1.113730.3.1.766

mailDomainMsgMaxBlocks

Origin
iPlanet Messaging Server 5.2

Syntax
int, single-valued

Object Classes
`mailDomain`

Definition
Imposes a size limit in units of MTA blocks on all messages sent to addresses in this domain. This limit doesn't apply to messages sent by users from this domain.

The value of this attribute is overridden by the value of `mailMsgMaxBlocks`, if set.

The MTA option used to override this attribute's value is `LDAP_DOMAIN_ATTR_BLOCKLIMIT`.

Example

OID
TBD

mailDomainMsgQuota

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
`mailDomain`

Definition
Quota of number of messages permitted for all users in this domain. If domain quota enforcement is activated, then the domain exceeding this quota will stop receiving more messages until the messages no longer exceed the quota. Domain quota enforcement is activated using the command `imquotacheck -f -d <domain>`.

Example
`mailDomainMsgQuota: 2000000`

OID
2.16.840.1.113730.3.1.767

mailDomainReportAddress

Origin
iPlanet Messaging Server 5.2

Syntax
cis, single-valued (RFC 822 mailbox)

Object Classes
mailDomain

Definition
This value is used as the header From: address in DSNs reporting problems associated with recipient addresses in the domain. It is also used when reporting problems to users within the domain regarding errors associated with nonlocal addresses.

If this attribute is not set, the reporting address will default to "postmaster@domain."

The MTA option used to override this attribute's value is LDAP_DOMAIN_ATTR_REPORT_ADDRESS.

Example

OID
TBD

mailDomainSieveRuleSource

Origin
iPlanet Messaging Server 5.2

Syntax
cis, single-valued (RFC 3028 sieve filter)

Object Classes
mailDomain

Definition
SIEVE filters are not supported by iPlanet Delegated Administrator.

SIEVE filter for all users in the domain. There are two possible forms for the value of this attribute: a single value that contains the complete sieve script (RFC 3028 compliant), and multiple values, with each value containing a piece of the sieve script (not RFC 3028 compliant).

A script has the following form:

```
require ["fileinto", "reject"];
# $Rule Info: Order=(1-infinity, or 0 for disabled)
Template=(template-name) Name=(rule name)
if header :is "Sender" "owner-ietf-mta-filters@imc.org"
{ fileinto "filter"; # move to "filter" folder }
if header :is "Subject" "SPAM!"
{ delete }
```

Multi-valued Form

Multiple SIEVE scripts per user can be stored in LDAP. To enable the user interface to handle several smaller rules scripts, rather than one script containing all the domain's rules, this attribute takes multiple values (that is, multiple rules). The server looks at every rule in `mailSieveRuleSource`.

To provide ordering and possible user interface editing information, there is an optional SIEVE comment line in each rule. This line has the following format:

```
# $Rule Info: Order=(1-infinity, or 0 for disabled)
```

All rules that have a `Rule Info` line will be processed first by the Messaging Server. If `Order=0`, then this rule is not used in the SIEVE evaluation. Otherwise, the rules are processed in the order provided (`1` having highest priority). To accommodate SIEVE rules that might not have been entered using the `Rule Info` extension, any other rules found are run by the server, in order received from LDAP after all rules with corresponding order values have been processed.

MTA Override Option

The MTA option that overrides this attribute's value is `LDAP_DOMAIN_ATTR_FILTER`.

Example

The following example is correctly formed, but Messaging Server ignores discard and reject text, and does not send a reject or discard reply message.

```
mailSieveRuleSource:
require ["fileinto", "reject", "redirect", "discard"]
if header :contains "Subject" "New Rules Suggestion
    {redirect "rules@sesta.com" # Forward message }
if header :contains "Sender" "porn.com"
    {discard text:
Your message has been rejected. Please remove this address from your
mailing list.    # Reject message, send reply message.}
if size :over 1M
    { reject text:
Please do not send large attachments.
```

```
Put your file on a server and send the URL.
Thank you. # Discard message, send reply message.}
if header :contains "Sender" "domainadminstrator@sesta.com
    { fileinto complaints.refs # File message}
```

OID
TBD

mailDomainStatus

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`mailDomain`

Definition
Current status of the mail domain. Can be one of the following values: `active`, `inactive`, `deleted`, `hold`, or `overquota`. This attribute is the mail service domain status. Missing value implies status is `active`. An illegal value is treated as `inactive`.

The following table lists the status values:

Table 3-12 Status Values

Value	Description
`active`	Mail service is marked as active for all users in this domain and all users in the domain that are marked active (see inetUserStatus and mailUserStatus for more information). However, any restrictions specified in mailAllowedServiceAccess and mailDomainAllowedServiceAccess still apply.
`inactive`	Mail service for all users in the domain is marked inactive. All user login attempts are rejected and messages sent to them get transient failure messages.
`deleted`	Mail domain is marked as deleted and will be removed during cleanup by the purge utility after the grace period is over. Mailboxes and user's mail service object classes are included in cleanup.
`hold`	Messages sent to all users in the domain are redirected to the hold channel. This value is typically used when users in the domain are being moved from one server to another without having to bounce messages back to the sender during the move. In this state, mailboxes can be moved without fear of any lost messages as all incoming messages are sent to the hold channel. Once the move is complete and the state has been changed from hold to active the messages are drained from the hold channel and sent to the MTAs where the user mailboxes now reside.

Table 3-12 Status Values

Value	Description
overquota	The MTA will not accept new messages for any users in the domain until this value is changed back to active.

There are four status attributes that mail services look at and which are evaluated in this order: inetDomainStatus, mailDomainStatus, inetUserStatus, and mailUserStatus. The rule is: the first of these attributes that is set to something other than active takes precedence over all the others.

The MTA option that overrides this attribute's values is LDAP_DOMAIN_ATTR_STATUS. The LDAP_DOMAIN_ATTR_STATUS option does not affect the message store or Identity Server commadmin utility, which only recognize and use the current value of mailDomainStatus.

Example

```
mailDomainStatus: active
```

OID

2.16.840.1.113730.3.1.770

mailDomainWelcomeMessage

Origin

Messaging Server 6.0

Syntax

cis, single-valued

Object Classes

mailDomain

Definition

Welcome message sent to new users added to this domain. '$$' is a carriage return. BNF syntax of this attribute is:

```
value:: <subjectline>'$'[<opt_headers>]'$$'<body>
subjectline:: 'Subject:'[<TEXT>]
opt_headers::<header_line>'$'[<opt_headers>]
header_line:: <header_name>':'<TEXT>
```

```
header_name:: <TEXT>
body:: [<lines>]
lines:: <line>’$’[<lines>]
line:: <TEXT>
```

Example

```
mailDomainWelcomeMessage: Subject: Welcome!!$X-Endorsement: We’re
good. $$Welcome to the mail system.
```

OID

2.16.840.1.113730.3.1.765

mailEquivalentAddress

Origin

iPlanet Messaging Server 5.2

Syntax

cis, multi-valued (RFC 822 addr-spec)

Object Classes

`inetMailGroup, inetMailUser`

Definition

Equivalent to `mailAlternateAddress` in regard to mail routing, except with this attribute, the header doesn’t get rewritten.

Note that `mailEquivalentAddress` is searched for when the system is deciding where to deliver messages, but it is not one of the attributes searched for when doing `REVERSE_URL` address reversal.

This attribute works only for direct LDAP mode, not with the deprecated `imsimta dirsync` option.

Example

```
mailEquivalentAddress: jdoe@sesta.com
```

```
mailEquvalentAddress: @sesta.com (catchall domain address)
```

OID

TBD

mailFolderName

Origin
Sun ONE Messaging Server 6.0

Syntax
cis, single-valued

Object Classes
`mailDomain`, `mailPublicFolder`

Definition
This attribute specifies the name of a public folder.

Example
`mailFolderName: Announcements`

OID

mailForwardingAddress

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`inetMailUser`

Definition
This attribute stores one or more forwarding addresses for inbound messages. Addresses are specified in RFC 822 format. Messages are forwarded to the listed address when `mailDeliveryOption: forward` is set.

Note that both `mailDeiveryOption` and this attribute must be set in order to keep the mail system in sync.

Example
`mailForwardingAddress: kokomo@sesta.com`

OID
2.16.840.1.113730.3.1.17

mailHost

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetLocalMailRecipient`

Definition
For a user or group entry, the fully qualified host name of the MTA that is the final destination of messages sent to this recipient. To be deemed local, the user entry must have this attribute, and it must match either the local.hostname configutil attribute, or one of the names specified by the local.imta.hostnamealiases configutil attribute. Otherwise, a new source routed address is generated in the form: `@mailhost:`*`user@domain`* and will be processed through the rewrite rules.

If a user entry does not have this attribute, the generated address will use the `mailRoutingSmartHost` hostname associated with the domain `@smarthost:`*`user@domain`*. If the domain has no `mailRoutingSmartHost` attribute, the address is discarded and a `5xx` error is reported.

If a group entry does not have this attribute, the group is processed locally.

The MTA option that overrides this attribute's value is `LDAP_MAILHOST`.

Example
```
mailHost: mail.siroe.com
```

OID
2.16.840.1.113730.3.1.18

mailMessageStore

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailUser`

Definition
Specifies the message store partition name for the user. The mapping between the partition name and the file system location of the store is kept in the message store configuration. If not specified, the default store partition specified in the server configuration is used.

Example
```
mailMessageStore: secondary
```

OID
2.16.840.1.113730.3.1.19

mailMsgMaxBlocks

Origin
iPlanet Messaging Server 5.2

Syntax
int, single-valued

Object Classes
`inetMailGroup, inetMailUser`

Definition
The size in units of MTA blocks of the largest message that can be sent to this user or group. The limit doesn't apply to messages sent by the user.

If this attribute is set, it overrides the value of `mailDomainMsgMaxBlocks`.

The MTA option that overrides the attribute's value is `LDAP_BLOCKLIMIT`.

Example

OID
TBD

mailMsgQuota

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
`inetMailUser`

Definition
Maximum number of messages permitted for a user is set with `mailMsgQuota`. This is a cumulative count for all folders in the store. Table 3-13 shows the special values and their meanings:

Table 3-13 mailMsgQuota Special Values

Value	Meaning
`0`	No mail messages allowed
`-1`	No limit on number of messages allowed
`-2`	Use system default quota (use of this value is being deprecated)

If this attribute is missing, the system default quota is used. This is defined by the `configutil` parameter `store.defaultmessagequota`.

During server configuration, quota enforcement must be turned on for `mailMsgQuota` to take effect. Both soft and hard quotas can be set. (See the *Sun Java System Messaging Server Administration Guide*.)

The MTA option override is `LDAP_MESSAGE_QUOTA`.

Example
```
mailMsgQuota: 2000
```

OID
2.16.840.1.113730.3.1.774

mailProgramDeliveryInfo

Origin
Messaging Server 5.0

Syntax
ces, multi-valued

Object Classes
`inetMailGroup`, `inetMailUser`

Definition
Specifies one or more programs used for program delivery. These programs have to be on the approved list of programs that the messaging server is permitted to execute for a domain. The attribute value specifies a reference to a program. That reference is resolved from the approved list of programs. The resolved reference also provides the program parameters and execution permissions. Used in conjunction with the `mailDeliveryOption: program`.

The value of this attribute should be used as the value for the method name (-m value) when running `imsimta program`.

The program approval process is documented further in the *Messaging Server Administrator's Guide*.

The MTA option used to name a different attribute for this function is `LDAP_PROGRAM_INFO`.

Example
```
mailProgramDeliveryInfo: procmail
```

OID
2.16.840.1.113730.3.1.20

mailPublicFolderDefaultRights

Origin
Sun ONE Messaging Server 6.0

Syntax
cis, multi-valued

Object Classes

mailPublicFolder

Definition

Specifies the access control rights granted for this public folder. Each value of this attribute consists of two parts separated by a space. The two parts are: an identifier, as specified in RFC 2086, and a list of access rights (mod_rights) as follows in Table 3-14.

Table 3-14 Access Rights for a Public Folder

Allowed Characters	Name	Actions Permitted
l	lookup	Mailbox is visible to LIST/LSUB commands.
r	read	SELECT the mailbox, perform CHECK, FETCH, PARTIAL, SEARCH, COPY from mailbox.
s	seen	Keep seen/unseen information across sessions. (STORE SEEN flag)
w	write	STORE flags other than SEEN and DELETED.
i	insert	Perform APPEND, COPY into mailbox.
p	post	Send mail to submission address for mailbox (not enforced by IMAP 4 itself).
c	create	CREATE new sub-maiboxes in any implementation-defined hierarchy.
d	delete	STORE DELETED flag, perform EXPUNGE.
a	administer	Perform SETACL.

Messaging Server's IMAP ACL implementation also defines the following new identifier:

anyone@*domain*

where *domain* is a valid domain.

If the attribute is missing, the default rights specified in the mailPublicFolderDefaultRights attribute from the mailDomain object class will be applied. If mailDomain does not contain this attribute, the following default ACL is set when a public folder is first created:

anyone@*domain* lrs

where *domain* is a valid domain.

Group identifiers start with the prefix “group=”. Do not put the group identifier prefix on a userid. The message store’s user creation code checks for this.

Examples

```
mailPublicFolderDefaultRights: anyone@sesta.com lrs
mailPublicFolderDefaultRights: group: sales@sesta.com lrs
mailPublicFolderDefaultRights: john@sesta.com lrswid
```

OID

mailQuota

Origin

Messaging Server 5.0

Syntax

int, single-valued

Object Classes

`inetMailUser`, `mailDomain`

Definition

Specifies, in bytes, the amount of disk space allowed for the user’s mailbox. The numeric portion of the value is limited to 4294966272. For values approaching of exceeding four gigabytes, use the `G` suffix instead of specifying the full value as a number. Other valid suffixes are: `K` for kilobytes, `M` for megabytes, and `G` for gigabytes.

Table 3-15 shows the special values for this attribute.

Table 3-15 mailQuota Special Values

Value	Meaning
`0`	No space allowed for user’s mailbox
`-1`	No limit on space usage allowed
`-2`	Use system default quota (use of this value is being deprecated)

The quota value is limited to `4096G` because the message store uses a 32 bit unsigned integer to store the quota value.

If the attribute is not specified, the system default quota is used.The system default is specified in the server configuration parameter `store.defaultmailboxquota`. Setting the configuration parameter `store.quotaenforcement` to 'on' causes the message store to enforce the quota.

NOTE `LDAP_DISK_QUOTA` is the MTA option used to specify a different attribute name for this function.

Example

```
mailQuota: 4G
```

or for the system default quota:

```
mailQuota:
```

OID

2.16.840.1.113730.3.1.21

mailRejectText

Origin

Messaging Server 5.2

Syntax

ces, multi-valued

Object Classes

`inetMailGroup`

Definition

The first line of text stored in the first value of this attribute is saved. This text is returned if any of the authentication attributes cause the message to be rejected. Since text can appear in SMTP responses, the value is limited to US-ASCII characters in order to comply with messaging standards.

NOTE `LDAP_REJECT_TEXT` is the MTA option used to specify a different attribute name for this function.

Example

OID
TBD

mailRoutingAddress

Origin
Messaging Server 5.0

Syntax
cis, single valued

Object Classes
`inetLocalMailRecipient`

Definition
Used together with `mailHost` to determine whether or not the address should be acted upon at this time or forwarded to another system.

NOTE `LDAP_ROUTING_ADDRESS` is the MTA option used to specify a different attribute name for this function.

Example

OID
2.16.840.1.113730.3.1.24

mailRoutingHosts

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`mailDomain`

Definition

Fully qualified host name of the MTA responsible for making routing decisions for users in this (and all contained) domain(s). Unspecified attribute implies all MTAs must route messages for the users / groups of this (and contained) domain(s).

When a domain is found to be nonlocal, the use of this attribute depends on the value of the MTA option `ROUTE_TO_ROUTING_HOST`:

- If the value is zero (`0`), which is the default setting, the attribute was checked as part of the $* rewrite rule. With a nonlocal domain, the $* rewrite rule fails and no further use is made of this attribute's values. The remaining rewrite rules determine the handling of the domain.
- If the value of the option is one (`1`), then the first value of this attribute that the MTA receives is installed as the source route in the address. And, all addresses associated with the domain are routed to that host.

Since this attribute is multi-valued and the first value the MTA "sees" will be chosen when the option is set to `1`, it might be tempting to assume that you can direct the order in which these mail hosts will be used; that is, you might assume you can do a sort of load balancing by ordering the various values of this attribute. But, LDAP does not guarantee that attribute value ordering is preserved, so the first value seen by the MTA might be any of the attribute's values, not necessarily the first one in the LDAP entry.

You can implement load balancing with a set of MX records for each of the routing host names. Do not attempt to do it with the ordering of this attribute's values.

`LDAP_DOMAIN_AATR_ROUTING_HOSTS` is the MTA option used to specify a different attribute name for this function.

Example

```
mailRoutingHosts: mail.siroe.com
```

OID

2.16.840.1.113730.3.1.759

mailRoutingSmartHost

Origin

Messaging Server 5.0

Syntax

cis, single-valued

Object Classes
mailDomain

Definition
Fully qualified host name, or domain-literal IP address, of a mail server responsible for handling mail for users not found in the local directory. Messages sent to users not found in the messaging server's directory are forwarded to the mail server specified in this attribute. This is useful when making a transition from one mail system to another and all users have not yet been moved over to the messaging server directory. An empty or missing attribute implies the local MTA is responsible for routing and delivering all messages for users in that domain.

This attribute is used by the system only if the domain it cares about is listed in the attribute, otherwise, it is ignored.

NOTE LDAP_DOMAIN_ATTR_SMARTHOST is the MTA option used to specify a different attribute name for this function.

Example
```
mailRoutingSmartHost: mail.siroe.com
mailRoutingSmartHost: 129.148.12.141
```

OID
2.16.840.1.113730.3.1.760

mailSieveRuleSource

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
inetMailUser

Definition
SIEVE filters are not supported with iPlanet Delegated Administrator for Messaging. Use this with LDAP Schema 2 and Identity Server.

The attribute contains a SIEVE rule (RFC 3028 compliant) used to create a message filter script for a user entry. This attribute can be either single-valued, with the rule containing the complete SIEVE script, or multi-valued, with each rule containing an independently valid piece of the SIEVE script. When there are multiple values, the Web filter construction interface combines the rules into a single SIEVE script using an ordering parameter (`Order`) found in a `#Rule Info:` comment.

NOTE Note that when the value of `Order` is a negative number, the value is ignored, and the rule is processed with other unordered SIEVE rules for this entry, but when the value of `Order` is zero, the rule is disabled and not processed at all.

The script is applied when a message is ready to be enqueued to the delivery channel. Though the SIEVE script is created while the MTA is expanding aliases, it is not used until after the resulting delivery addresses have been expanded and are being sent to the `ims-ms`, `native`, `autoreply` or `pipe` channels.

A script has the following form:

```
require ["fileinto", "reject"];
# $Rule Info: Order=(1-infinity, or 0 for disabled)
Template=(template-name) Name=(rule name)
if header :is "Sender" "owner-ietf-mta-filters@imc.org"
{ fileinto "filter"; # move to "filter" folder }
if header :is "Subject" "SPAM!"
{ delete }
```

MTA Option

The MTA option used to name a different attribute for this function is `LDAP_FILTER`.

Example

```
mailSieveRuleSource:
require ["fileinto", "reject", "redirect", "discard]
if header :contains "Subject" "New Rules Suggestion
    {redirect "rules@sesta.com" # Forward message }
if header :contains "Sender" "porn.com"
    {discard text:
Your message has been rejected. Please remove this address from your
mailing list.    # Reject message, send reply message.}
if size :over 1M
    { reject text:
Please do not send me large attachments.
```

```
Put your file on a server and send me the URL.
Thank you. # Discard message, send reply message.}
if header :contains "Sender" "barkley@sesta.com
    { fileinto complaints.refs # File message}
```

OID

2.16.840.1.113730.3.1.775

mailSMTPSubmitChannel

Origin

Messaging Server 5.0

Syntax

cis, single-valued

Object Classes

inetMailUser

Definition

Most commonly, this attribute is a factor involved in setting up guaranteed message delivery, or in setting up other special classes of service. When defined, this attribute tells the MTA to consider the channel named by this attribute to be the effective submission channel, if the SMTP AUTH is successful.

Example

```
mailSMTPSubmitChannel: tcp_tas
```

OID

2.16.840.1.113730.3.1.776

mailUserStatus

Origin

Messaging Server 5.0

Syntax

cis, single-valued

Object Classes
inetMailUser

Definition
Current status of the mail user. Can be one of the following values: active, inactive, deleted, hold, overquota, or removed.

A missing value implies status is active. An illegal value is treated as inactive.

Table 3-16 Mail User Status

Status Value	Description
active	Normal state. If inetUserStatus is also active, then mail is processed as per the values stored in other user attributes (such as mailDeliveryOption, mailSieveRuleSource, and so on). If not set to active, the status from inetUserStatus takes precedence. Other status attributes taken into consideration are inetDomainStatus and mailDomainStatus. If the combination of inetDomainStatus and mailDomainStatus permits mail delivery and access for the domain, the user state is determined from inetUserStatus and mailUserStatus.
inactive	The user's mail account is inactive. A transient failure is returned to the sending MTA.
deleted	The user's mail account is marked to be deleted from the message store. A permanent failure is returned to the sending MTA and the user's mail account is a candidate for cleanup by the msuser purge utility. User access to the mailbox is blocked. After msuser purge deletes the mail account from the message store, it sets the value of mailUserStatus to removed.
removed	The user entry is marked to be deleted from the LDAP directory. A permanent failure is returned to the sending MTA. User access to the mailbox is blocked. This setting allows the Identity Server commadmin domain purge command to delete the user entry from the LDAP directory.
hold	User's mail is sent to the hold queue and access to the mailbox over IMAP, POP, and HTTP is disallowed. MTA and Message Access Servers on the store server must comply with this requirement. This setting overrides any other mailDeliveryOption settings.
overquota	The MTA will not deliver mail to a mailbox with this status.

There are four status attributes that mail services look at and which are evaluated in this order: inetDomainStatus, mailDomainStatus, inetUserStatus, and mailUserStatus. The rule is: the first of these attributes that is set to something other than active takes precedence over all the others.

NOTE LDAP_USER_STATUS is the MTA option that overrides the mailUserStatus attribute. The LDAP_USER_STATUS option does not affect the message store or Identity Server commadmin utility, which only recognize and use the current value of mailUserStatus.

Example
`mailUserStatus: active`

OID
2.16.840.1.113730.3.1.778

maxPabEntries

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
`ipUser`

Definition
Specifies the maximum number of personal address book entries users are permitted to have in their personal address book store. A value of `-1` implies there is no limit. If this attribute is not present then the system default specified in the personal address book configuration is used.

Example
`maxPabEntries: 1000`

OID
2.16.840.1.113730.3.1.705

memberOf

Origin
Messaging Server 5.0, deprecated in Messaging Server 6.0 for `inetUser`; Identity Server

Syntax
dn, multi-valued

Object Classes
inetAdmin, inetUser

Definition
For LDAP Schema 2, this attribute decorates inetAdmin, and specifies the DN of an assignable dynamic group to which a user belongs. It is used as the default well-known filtered attribute used in conjunction with mgrpDeliverTo to search for assignable dynamic group members.

This attribute is deprecated for inetUser in Messaging Server 6.0 and is likely to be removed from the inetUser object class in future versions of the schema.

For LDAP Schema 1, this attribute specifies the DN of a mailing list to which a user belongs, indicating static group membership as a backpointer.

Example
memberOf: cn=Administrators,ou=groups o=sesta.com,o=*basedn*

OID
1.2.840.113556.1.2.102

memberOfPAB

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
pabPerson, pabGroup

Definition
The unique name (un) of the personal address book(s) in which this entry belongs.

Example
memberOfPAB:addressbook122FA7

OID
2.16.840.1.113730.3.1.718

memberOfPABGroup

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
pabPerson

Definition
Unique name of the personal group(s) in which this user belongs.

Example
memberOfPabGroup:testgroup15577F2D

OID
2.16.840.1.113730.3.1.719

memberURL

Origin
Messaging Server 5.2

Syntax
ces, multi-valued

Object Classes
inetMailGroup

Definition
A list of URLs, which, when expanded, provides a list of mailing list member addresses.

This is the preferred way to specify a dynamic mailing list. Alternately, you can use mgrpDeliverTo.

The MTA option used to override this attribute's value is LDAP_GROUP_URL2.

Example
memberURL:ldap://cn=jdoes, o=sesta.com

OID
2.16.840.1.113730.3.1.198

mgrpAddHeader

Origin
Netscape Messaging Server

Syntax
ces, multi-valued

Object Classes
`inetMailGroup`

Definition
Each attribute value specifies a header field that is to be added to the message header if it is present.

For the MTA, the values of these attributes are headers, which are used to set header-trimming ADD options.

NOTE `LDAP_ADD_HEADER` is the MTA option used to specify a different attribute name for this function.

Example
```
mgrpAddHeader:Reply-To: thisgroup@sesta.com
```

OID
2.16.840.1.113730.3.1.781

mgrpAllowedBroadcaster

Origin
Messaging Server 5.0

Syntax
ces, multi-valued

Object Classes
inetMailGroup

Definition
Identifies mail users allowed to send messages to the mail group. The Messaging Server expects this attribute to contain either a distinguished name or an RFC822address using an LDAP URI or a mailto address (see example). If a distinguished name is used, it must represent a mailable entry or entries of type group or groupOfUniqueNames. (That is, the group entry must contain an email address in one of the following attributes: mail, mailAlternateAddress, mailEquivalentAddress.) If no instances of this attribute exist on the inetMailGroup entry, then there are no restrictions on who can send messages to the mail group unless the mgrpAllowedDomain and mgrpDisallowedDomain attributes are used.

If multi-valued, each URL is expanded into a list of addresses and each address is checked against the current envelope “from” address. The message is allowed if there is a match.

To specify that only the members of this group can post to the group, use the group name as the value of the attribute.

If none of the attribute values is a valid URL, or none of the members of the group specified in the attribute value have a valid URL, then the message will bounce.

NOTE LDAP_AUTH_URL is the MTA option used to specify a different attribute name for this function.

Example
```
mgrpAllowedBroadcaster: ldap:///uid=bjensen,o=siroe.com

mgrpAllowedBroadcaster:mailto:group1@siroe.com
```

OID
2.16.840.1.113730.3.1.22

mgrpAllowedDomain

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
inetMailGroup

Definition
Identifies domains (including subdomains) from which users are allowed to send messages to the mail group. If no instances of this attribute exist on the inetMailGroup entry, then there are no restrictions on who can send messages to the mail group unless the mgrpAllowedBroadcaster, mgrpDisallowedBroadcaster, and mgrpDisallowedDomain attributes are used.

NOTE LDAP_AUTH_DOMAIN is the MTA option used to specify a different attribute name for this function.

Example
mgrpAllowedDomain:siroe.com

This matches any user sending from *.siroe.com.

OID
2.16.840.1.113730.3.1.23

mgrpAuthPassword

Origin
Messaging Server 5.0

Syntax
ces, single-valued

Object Classes
inetMailGroup

Definition
Specifies a password needed to post to the list.

The presence of this attribute forces a reprocessing pass. As the message is enqueued to the reprocessing channel, the password is taken from the header and placed in the envelope. Then, while reprocessing, the password is taken from the envelope and checked against this attribute. Only passwords that are actually used are removed from the header field.

This allows for routing to the moderator in the event of a password failure.

NOTE LDAP_AUTH_PASSWORD is the MTA option used to specify a different attribute name for this function.

Example

OID
2.16.840.1.113730.3.1.783

mgrpBroadcasterPolicy

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailGroup

Definition
Policy for determining allowed broadcaster. It specifies the level of authentication required to access the list of broadcaster addresses. The allowed values are:

- AUTH_REQ, SMTP_AUTH_REQUIRED

  In order to post to the list, the sender must be authenticated using the SMTP AUTH command.

- PASSWORD_REQUIRED, PASSWD_REQUIRED, PASSWD_REQ

  All values mean the password to the broadcaster list, specified by the mgrpAuthPassword attribute, must appear in an Approved: header field in the message.

- NO_REQUIREMENTS

  This value means no special requirements apply.

NOTE LDAP_AUTH_POLICY is the MTA option used to specify a different attribute name for this function.

Example
mgrpBroadcasterPolicy:AUTH_REQ

OID
2.16.840.1.113730.3.1.3

mgrpDeliverTo

Origin
Messaging Server 5.0

Syntax
ces, multi-valued

Object Classes
inetMailGroup

Definition
Used as an alternative method of specifying mail group membership. This can be used to create a dynamic mailing list.

The preferred attribute to use for specifying dynamic mail group is memberURL.

The values of this attribute are a list of URLs, which, when expanded, provides mailing list member addresses.

Messaging Server expects this attribute to contain an LDAP URL using the format described in RFC 1959. Any entries returned by the resulting LDAP search are members of the mailing group. There is a hard limit on the length of the search filter of 1024 bytes.

NOTE LDAP_GROUP_URL1 is the MTA option used to specify a different attribute name for this function.

Example

This example returns all users in the United States Accounting department for Sesta corporation.

```
mgrpDeliverTo: ldap:///ou=Accounting,o=Sesta,c=US??sub?
(&(objectClass=inetMailUser)(objectClass=inetOrgPerson))
```

OID

2.16.840.1.113730.3.1.25

mgrpDisallowedBroadcaster

Origin

Messaging Server 5.0

Syntax

ces, multi-valued

Object Classes

inetMailGroup

Definition

Identifies mail users not allowed to send messages to the mail group. If no instances of this attribute exist on the inetMailGroup entry, then there are no restrictions on who can send messages to the mail group unless the mgrpAllowedDomain and mgrpDisallowedDomain attributes are used.

Messaging Server expects this attribute to contain either a distinguished name or an RFC822address. If a distinguished name is used, it must represent a mailable entry or entries of type group or groupOfUniqueNames. (That is, the group entry must contain an email address in one of the following attributes: mail, mailAlternateAddress, mailEquivalentAddress.) The distinguished name must be represented in the form of an LDAP URL as described in RFC 1959.

If multi-valued, each URL is expanded into a list of addresses and each address is checked against the current envelope “from” address. The message is disallowed if there is a match.

NOTE LDAP_CANT_URL is the MTA option used to specify a different attribute name for this function.

Example

```
mgrpDisallowedBroadcaster: ldap:///uid=bjensen, o=sesta.com
mgrpDisallowedBroadcaster: mailto:sys50@sesta.com
```

OID

2.16.840.1.113730.3.1.785

mgrpDisallowedDomain

Origin

Messaging Server 5.0

Syntax

cis, multi-valued

Object Classes

`inetMailGroup`

Definition

Identifies domains from which users are not allowed to send messages to the mail group. This attribute is a private extension used by Messaging Server to manage mailing lists. If this attribute exists, then messages from listed domains are rejected. If no instances of this attribute exist on the `inetMailGroup` entry, then there are no restrictions on who can send messages to the mail group unless the `mgrpAllowedBroadcaster`, `mgrpDisallowedBroadcaster`, and `mgrpAllowedDomain` attributes are used.

NOTE `LDAP_CANT_DOMAIN` is the MTA option used to specify a different attribute name for this function.

Example

```
mgrpDisallowedDomain:sesta.com
```

OID

2.16.840.1.113730.3.1.784

mgrpErrorsTo

Origin
Messaging Server 5.0

Syntax
ces, single-valued

Object Classes
`inetMailGroup`

Definition
Recipient of error messages generated when messages are submitted to this list. Recipient's address can be specified using the `mailto` syntax, which includes an RFC 822 email address preceded by the keyword "`mailto:`" or simply an RFC 822 email address. Also supports LDAP URL syntax. However, if an LDAP URL is used, it must be one that produces a single address.

The envelope originator (`MAIL FROM`) address is set to the value of this attribute.

NOTE `LDAP_ERRORS_TO` is the MTA option used to specify a different attribute name for this function.

Examples:

```
Example 1: mgrpErrorsTo:mailto:jordan@siroe.com
Example 2: mgrpErrorsTo:
ldap:///uid=ofanning,ou=people,o=siroe.com,o=isp
```

OID
2.16.840.1.113730.3.1.26

mgrpModerator

Origin
Messaging Server 5.0

Syntax
ces, multi-valued

Object Classes
inetMailGroup

Definition
LDAP URI or mailto URL identifying the moderators allowed to submit messages to this list. Only those messages that are submitted by the moderator are sent to the members of this list. Messages submitted by others are forwarded to the moderators for approval and resubmitting.

The URLs given as the value of this attribute are expanded into a series of addresses, and then compared with the envelope "from" address. If there is a match, group processing continues. If there is no match, the value of this attribute becomes the group URL, any list of RFC 822 addresses or DNs associated with the group is cleared, the delivery options for the group are set to "members," and there is no further group processing for the failed URL (subsequent group attributes are ignored).

NOTE LDAP_MODERATOR_URL is the MTA option used to specify a different attribute name for this function.

Example
```
mgrpModerator: mailto:jordan@sesta.com
```

OID
2.16.840.1.113730.3.1.33

mgrpMsgMaxSize

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailGroup

Definition
Maximum message size in bytes that can be sent to the group. Messaging Server expects zero or one instance of this attribute to exist for every mailGroup entry. If no entry exists, then no size limit is imposed on mail to the group.

This attribute is obsolete, but still supported for backwards compatibility. Use `mailMsgMaxBlocks` instead.

NOTE `LDAP_ATTR_MAXIMUM_MESSAGE_SIZE` is the MTA option used to specify a different attribute name for this function.

Example
`mgrpMsgMaxSize:8000`

OID
2.16.840.1.113730.3.1.3

mgrpMsgPrefixText

Origin
Not implemented.

Syntax
UTF-8 text, single-valued

Object Classes
`inetMailGroup`

Definition
Specifies the text to be added to the beginning of the message text. You must supply the formatting. That is, you must insert CRLF where they belong in the text.

NOTE `LDAP_PREFIX_TEXT` is the MTA option used to specify a different attribute name for this function.

Example

OID
TBD

mgrpMsgRejectAction

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailGroup

Definition
Identifies the action to be taken when a email sent to a mail group is rejected. The Messaging Server may reject mail for the following reasons:

- It is received from an unauthorized domain (as defined by the mgrpAllowedDomain attribute).
- It is received from an mail address that is not a member of the mgrpAllowedBroadcaster attribute.
- It is larger than the size permitted on mgrpMsgMaxSize.

This attribute takes two values: reply and toModerator:

reply – The system produces an SMTP error, which is also the default if the attribute is not set. The text of the failure notice is stored in the mgrpMsgRejectText attribute.

toModerator – The mail is forwarded to the moderator for processing. The moderator is identified by the mgrpModerator attribute.

NOTE LDAP_REJECT_ACTION is the MTA option used to specify a different attribute name for this function.

Example
```
mgrpMsgRejectAction: reply
```

OID
2.16.840.1.113730.3.1.28

mgrpMsgRejectText

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailGroup`

Definition
Specifies the error text to use int he event of a group access failure. Because this text may appear in SMTP responses, this restricts the text to a single line of US-ASCII. This is implemented by reading only the first line of text in this attribute and using it only if it contains no 8-bit characters. (This is a limitation of the SMTP protocol.)

Example

OID
2.16.840.1.113730.3.1.29

mgrpMsgSuffixText

Origin
Not implemented.

Syntax
UTF-8 text, single valued

Object Classes
`inetMailGroup`

Definition
Specifies the text to be appended to the text message. You must supply the formatting. That is, you must insert any CRLFs (carriage return, line feeds) that belong in the text.

NOTE `LDAP_SUFFIX_TEXT` is the MTA option used to specify a different attribute name for this function.

Example

OID
TBD

mgrpNoDuplicateChecks

Origin
Messaging Server 5.0, not implemented going forward for Messaging Server 5.2

Syntax
cis, single-valued

Object Classes
`inetMailGroup`

Definition
This attribute is no longer supported. Duplicate checking is controlled by characteristics of the lists themselves. Some lists combine and some lists don't.

Old definition: Prevents Messaging Server from checking for duplicate delivery to members of the mail group. Prevents multiple deliveries if a user is on multiple lists. `No` means the system checks for duplicate delivery. `Yes` means the system does not check for duplicate delivery.

Example
```
mgrpNoDuplicateChecks: yes
```

OID
2.16.840.1.113730.3.1.789

mgrpRemoveHeader

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
inetMailGroup

Definition
Each attribute value specifies a header field that is to be removed from the message header, if present.

Turns the headers specified into header trimming MAXLINES=-1 options.

NOTE LDAP_REMOVE_HEADER is the MTA option used to specify a different attribute name for this function.

Example

OID
2.16.840.1.113730.3.1.801

mgrpRequestTo

This attribute has been removed from the schema. It is no longer supported. It only worked for dirsync mode, which was deprecated in Messaging Server 5.2.

mgrpRFC822MailMember

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
inetMailGroup

Definition

Identifies recipients of mail sent to mail group. Mail sent to both this attribute and `uniqueMember` attributes are not members of the mixed-in `groupOfUniqueNames`. This attribute represents mail recipients that cannot be expressed as distinguished names, or who are to be sent mail from this group but who do not have the full privileges of a unique group member. Messaging Server expects this attribute to contain RFC 822 mail addresses. Generally used for group members who are not in the local directory.

For backwards compatibility, `rfc822MailMember` is also supported. You can use either one or the other of these attributes in any given group, but not both.

NOTE `LDAP_GROUP_RFC822` is the MTA option used to specify a different attribute name for this function.

Example

```
mgrpRFC822MailMember:bjensen@siroe.com
```

OID

2.16.840.1.113730.3.1.30

msgVanityDomain

Origin

Messaging Server 5.0

Syntax

cis, single-valued

Object Classes

`msgVanityDomainUser`

Definition

This attribute and the object class using it are deprecated in the current release, and may not be supported in future releases. Sites should stop using this feature and consider migrating current vanity domains to hosted domains.

Example

OID

2.16.840.1.113730.3.1.799

multiLineDescription

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailUser`

Definition
Detailed description of the distribution list. A dollar sign (“$”) creates a new line.

Example
```
multiLineDescription:People who like cats. $And are ambivalent
about people.
```

OID
1.3.6.1.4.1.250.1.2

nickName

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`pabPerson`, `pabGroup`

Definition
Identifies the short name used to locate a `pabPerson` or a `pabGroup` entry.

Example
```
nickname:Nick
```

OID
2.16.840.1.113730.3.1.720

nswcalDisallowAccess

Origin
Netscape™ Calendar Hosting Server

Syntax
cis, single

Object Classes
`icsCalendarUser`

Definition
Lists the calendar protocols not allowed to be used by this user.

Example

OID
2.16.840.1.113730.3.1.539

nswmExtendedUserPrefs

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`inetMailUser`

Definition
This attribute holds the pairs that define Messenger Express preferences such as sort order, Mail From address, and so on. Each instance of this attribute is the tuple *pref_name=pref_value*. This is a proprietary syntax and the example below is for illustrative purposes only.

Example

```
Example 1: nswmExtendedUserPrefs: meColorSet=4
Example 2: nswmExtendedUserPrefs: meSort=r
Example 3: nswmExtendedUserPrefs: meAutoSign=True
Example 4: nswmExtendedUserPrefs: meSignature=Otis
Fanning$ofanning@sesta.com
Example 5: nswmExtendedUserPrefs: meDraftFolder=Drafts
```

OID

2.16.840.1.113730.3.1.520

o

Origin

Messaging Server 5.0

Syntax

cis, single valued

Object Classes

pabPerson

Definition

Name of the user's company or organization. Abbreviation of `organizationName`.

Example

```
organizationName:Company22 Incorporated
```

or

```
o:Company22 Incorporated
```

OID

2.5.4.10

objectClass

Origin

Messaging Server 5.0

Syntax
cis

Object Classes
inetAdmin, organization

Definition
Specifies the objects for this object class.

Example
objectClass:person

OID
2.5.4.0

organizationName (see o)

organizationUnitName (see ou)

ou

Origin
Messaging Server 5.0

Syntax
cis, single valued

Object Classes
organizationalUnit,pabPerson

Definition
Name of the organization unit to which the user belongs. Abbreviation for organizationUnitName.

Example
organizationUnitName:docs

or

`ou:docs`

OID
2.16.840.1.113730.3.1.722

owner

Origin
Messaging Server 5.0

Syntax
dn, single-valued

Object Classes
`inetOrgPerson`

Definition
Identifies the distinguished name (DN) of the person or group with administrative privileges over the entry.

Example
`owner: cn=John Smith,o=Sesta,c=US`

OID
2.5.4.32

pabURI

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`ipUser`

Definition
LDAP URI specifying the container of the personal address book entries for this user. It takes the following form: `ldap://`*`server`*`:`*`port`*`/`*`container_dn`*, where:

- *server* – Host name of the personal address book LDAP server.
- *port* – Port of the personal address book LDAP server.
- *container_dn* – DN of the subtree where all PAB entries for the user are created.

Example
```
pabURI:
ldap://ldap.siroe.com:389/ou=ed,ou=people,o=sesta.com,o=isp,o=pab
```

OID
2.16.840.1.113730.3.1.703

parentOrganization

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, single-valued

Object Classes
`sunManagedSubOrganization`

Definition
Specifies the logical parent of a suborganization. The value of this is the DN of the parent organization or parent suborganization.

Example
`parentOrganization:o=sesta,o=com,o=internet`

OID

postalAddress

Origin
LDAP

Syntax
cis

Object Classes
`icsCalendarResource`, `organization`, `organizationalUnit`

Definition
Identifies the entry's mailing address. This field is intended to include multiple lines. When represented in LDIF format, each line should be separated by a dollar sign ($).

To represent an actual dollar sign ("$") or back slash ("\") within this text, use the escaped hex values, \24 and \5c respectively. For example, to represent the string:

```
The dollar ($) value can be found
in the c:\cost file.
```

provide the string:

The dollar(\24) value can be found$in the c:\5ccost file.

Example
```
postalAddress:123 Oak Street$Anytown, CA$90101
```

OID
2.5.4.16

preferredLanguage

Origin
Messaging Server 5.0, Calendar Server, Directory Server

Syntax
RFC 2798, cis, single-valued

Object Classes

icsCalendarUser, inetMailGroup, inetOrgPerson, iPlanetPreferences, mailDomain

Definition

Preferred written or spoken language for a person. The value for this attribute should conform to the syntax for HTTP Accept-Language header values.

Messaging Server uses this attribute to figure the locale. It does not use the locale specified with iPlanetPreferences.

Also used by Identity Server in user LDAP entries to store a user's preferred language. Note that only Identity Server uses the iPlanetPreferences object class to host this attribute.

Table 3-17 lists the supported language strings:

Table 3-17 Language Strings for preferredLanguage Attribute

Language String	Language
de	German
en	English
es	Spanish
fr	French
ja	Japanese
ko	Korean
zh-CN	Chinese - People's Republic of China
zh-TW	Chinese - Taiwan

Example

preferredLanguage:en

OID

2.16.840.1.113730.3.1.39

preferredMailHost

Origin

Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
mailDomain

Definition
Used by Messaging Server Delegated Administrator with LDAP Schema 1 only.

Used to set the mailHost attribute of newly created users and groups in this mail domain.

Example
preferredMailHost:mail.siroe.com

OID
2.16.840.1.113730.3.1.761

preferredMailMessageStore

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
mailDomain

Definition
Used by Messaging Server Delegated Administrator for LDAP Schema 1 only.

Used to set the mailMessageStore attribute of newly created users. If missing, Delegate Administrator leaves the mailMessageStore attribute empty and the access server assumes that the user's mailbox is in the default partition of the server instance.

Example
preferredMailMessageStore: primary

OID
2.16.840.1.113730.3.1.762

seeAlso

Origin
LDAP

Syntax
dn

Object Classes
groupOfUniqueNames, organization, organizationalUnit

Definition
Identifies another LDAP entry that may contain information related to this entry.

Example
```
seeAlso: cn=Quality Control
Inspectors,ou=manufacturing,o=Company22, c=US
```

OID
2.5.4.34

sn

Origin
LDAP

Syntax
cis

Object Classes
icsCalendarUser

Definition
Identifies the entry's surname, also referred to as last name or family name.

Example
```
surname:jones
```

OID
2.5.4.4

telephoneNumber

Origin
LDAP

Syntax
tel

Object Classes
`domain`, `organization`, `organizationalUnit`

Definition
Identifies the entry's phone number.

Example
`telephoneNumber:800-555-1212`

OID
2.5.4.20

uid

Origin
Calendar Server 5.0, Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`icsCalendarResource`, `icsCalendarUser`

Definition
Identifies the unique identifier for this user or resource within its relative namespace. All valid user and resource entries must have a `uid` attribute. Group entries may have a `uid`.

For Messaging Server, the `uid` is used to generate the user address to pass to the delivery channel. If a user entry does not have a `uid` attribute, the entry is ignored. If multiple `uid` attributes exist in an entry, only the first one is used. The MTA used to override this attribute's value is `LDAP_UID`.

Example
`uid:jdoe`

OID
0.9.2342.19200300.100.1.1

un

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`pabPerson`, `pabGroup`, `pab`

Definition
Unique name assigned to PAB entry. This is also the naming attribute for entries created by this object class and is used to form the DN of all PAB entries, irrespective of the type (`pab`, `pabPerson`, or `pabGroup`).

Example
`un:Nick`

OID
2.16.840.1.113730.3.1.717

uniqueMember

Origin
Messaging Server 5.0

Syntax
dn, multi-valued

Object Classes
`groupOfUniqueNames`

Definition
Identifies a member of a static group. Each member of the group is listed in the group's LDAP entry using this attribute.

Example
`uniqueMember: uid=jdoe,ou=People,o=sesta.com,o=`*basedn*
`uniqueMember: uid=rsmith,ou=People,o=sesta.com,o=`*basedn*

OID
2.5.4.50

userId (see uid)

userPassword

Origin
Messaging Server 5.0

Syntax
bin, single-valued

Even though RFC 2256 defines this attribute as multi-valued, for Sun Java™ System products, only one value is allowed.

Object Classes
`inetUser`, `domain`, `organization`, `organizationalUnit`

Definition
This attribute identifies the entry's password and encryption method in the following format:

{*encryption method*}`encrypted password`

Transfer of cleartext passwords is strongly discouraged where the underlying transport service cannot guarantee confidentiality. Transfer of cleartext may result in disclosure of the password to unauthorized parties.

Example
`userPassword:{sha}FTSLQhxXpA05`

OID
2.5.4.35

vacationEndDate

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`userPresenceProfile`

Definition
Vacation end date and time. Date is in the following format: `YYYYMMDDHHMMSSZ`; where `YYYY` is the four digit year, `MM` is the two digit month, `DD` is the two digit day, `HH` is the two digit hour, and `SS` is the two digit second. Time is normalized to GMT. `Z` is the character `Z`.

When the current date falls outside the range of dates specified by the attributes `vacationStartDate` and `vacationEndDate`, then any delivery options (in the DELIVERY_OPTIONS list) prefixed with "^" are removed from the active set of options. For example, if one of the DELIVERY_OPTIONS is "^*autoreply" and today's date falls outside the vacation date range, then the option is removed from the active options list. Otherwise, the autoreply delivery option is activated.

Example
`vacationEndDate:20000220000000Z`

OID
2.16.840.1.113730.3.1.708

vacationStartDate

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
userPresenceProfile

Definition
Vacation start date and time. Date is in the following format: YYYYMMDDHHMMSSZ; where YYYY is the four digit year, MM is the two digit month, DD is the two digit day, HH is the two digit hour, and SS is the two digit second. Time is normalized to GMT. Z is the character Z.

Example
vacationStartDate:20000215000000Z

OID
2.16.840.1.113730.3.1.707

Chapter 4

Sun Java™ System Identity Server Classes and Attributes

This chapter describes LDAP object classes and attributes for Sun Java™ System Identity Server implementing LDAP Schema 2. The objects and attributes are listed alphabetically.

Note that the Identity Server schema is subject to change. To understand provisioning considerations, see the *Sun Java™ Enterprise System Installation Guide*.

The chapter is divided into two sections:

Object Classes

This section describes the following Identity Server object classes:

iplanet-am-managed-assignable-group

Supported by
Identity Server

Definition
Specifies a dynamic group with a well-known attribute in the search filter. For Messaging Server, the well-known attribute is `memberOf`. The search filter is contained in the `mgrpDeliverTo` attribute.

Superior Class
`iplanet-am-managed-group`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.182

Required Attributes
N / A

Allowed Attributes
Inherits attributes from superior class.

iplanet-am-managed-filtered-group

Supported by
Identity Server

Definition
Specifies a dynamic group which can be filtered on any attribute. The search filter is set in the `mgrpDeliverTo` attribute.

This group is not subscribable. Do not use `iplanet-am-group-subscribable` for a filtered dynamic group.

Superior Class
`iplanet-am-managed-group`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.181

Required Attributes
N / A

Allowed Attributes
Inherits attributes from superior class. Note that since this group can not be subscribed to, the `mail` attribute should not be used with it. If present, it will be ignored.

iplanet-am-managed-filtered-role

Supported by
Identity Server

Definition
Specifies the attributes necessary to define administrator roles and their ACIs. The list of all users assigned this role is a dynamic list; that is, the list can be retrieved only by performing a search filtered by the role name. For further information on roles, see the Identity Server documentation at:

`http://docs.sun.com`

Superior Class
iplanet-am-managed-role

Object Class Type
auxiliary

OID
1.3.6.1.4.1.42.2.27.9.2.74

Required Attributes
N / A

Allowed Attributes
This class inherits the attributes of its superior class, see iplanet-am-managed-role.

iplanet-am-managed-group

Supported by
Identity Server

Definition
This is the superior class for the various types of groups: static, assignable dynamic, and filtered dynamic. (See iplanet-am-managed-assignable-group, iplanet-am-managed-filtered-group, iplanet-am-managed-static-group.)

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.180

Required Attributes
N / A

Allowed Attributes
mail, inetGroupStatus

iplanet-am-managed-group-container

Supported by
Identity Server

Definition
The Identity Server class that defines the groups container under each Messaging Server hosted domain.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.189

Required Attributes
N / A

Allowed Attributes
N / A

iplanet-am-managed-org-unit

Supported by
Identity Server

Definition
This class is used by Identity Server to manage organizational units. It uses the same attributes as `sunManagedOrganization` and for all intents and purposes functions as any other organization managed by Identity Server.

Do not use this class for the domain organizations, or people and group containers in Messaging Server. Even though the attribute that holds the container name is organizational unit (`ou`), the proper Identity Server class to use is either `iplanet-am-managed-group-container`, or `iplanet-am-managed-people-container`.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.186

Required Attributes
N / A

Allowed Attributes
businessCategory, iplanet-am-service-status, telephoneNumber, sunOverrideTemplates, sunPreferredDomain, seeAlso

iplanet-am-managed-people-container

Supported by
Identity Server

Definition
The Identity Server class that defines the people container under each Messaging Server hosted domain.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.187

Required Attributes
N / A

Allowed Attributes
N / A

iplanet-am-managed-person

Supported by
Identity Server

Definition
Specifies Identity Server attributes used to manage users.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.184

Required Attributes
N/A

Allowed Attributes
`iplanet-am-modifiable-by`, `iplanet-am-role-aci-description`, `iplanet-am-static-group-dn`, `iplanet-am-user-account-life`

iplanet-am-managed-role

Supported by
Identity Server

Definition
Specifies the attributes necessary to define administrator roles and their ACIs. This is the superior class for `iplanet-am-managed-filtered-role`.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.179

Required Attributes
N / A

Allowed Attributes
iplanet-am-role-aci-description, iplanet-am-role-aci-list, iplanet-am-role-any-options, iplanet-am-role-description, iplanet-am-role-managed-container-dn, iplanet-am-role-service-options, iplanet-am-role-type

iplanet-am-managed-static-group

Supported by
Identity Server

Definition
Defines a group in which there are members identified with the `uniqueMember` attribute. Each user named in those attributes has the `memberOf` attribute in their LDAP user entry.

Note that static groups can have dynamic members. In this case, the LDAP entry must also contain the `iplanet-am-managed-assignable-group` object class.

Superior Class
`iplanet-am-managed-group`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.183

Required Attributes
N / A

Allowed Attributes
N / A (inherits from `iplanet-am-managed-group`)

iplanet-am-user-service

Supported by
Identity Server

Definition
This class contains the Identity Server attributes necessary to manage user accounts.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.176

Required Attributes
N / A

Allowed Attributes
`iplanet-am-user-account-life`, `iplanet-am-user-admin-start-dn`, `iplanet-am-user-alias-list`, `iplanet-am-user-auth-config`, `iplanet-am-user-auth-modules`, `iplanet-am-user-failure-url`, `iplanet-am-user-federation-info`, `iplanet-am-user-federation-info-key`, `iplanet-am-user-login-status`, `iplanet-am-user-password-reset-force-reset`, `iplanet-am-user-password-reset-options`, `iplanet-am-user-password-reset-question-answer`, `iplanet-am-user-service-status`, `iplanet-am-user-success-url`

iPlanetPreferences

Supported by
Directory Server

Definition
Used by Identity Server. While Messaging Server does not use this object class, it is necessary for Identity Server.

Attributes for this object class hold certain preferences for this user. Specifically, the preferred language, preferred locale, and preferred time zone.

Note: The Messaging Server does not use this object class to define the preferred language. In addition, it does not use an attribute for locale; it infers the locale from the language. Messaging Server holds the `preferredLanguage` attribute in `inetOrgPerson`.

Superior Class
`top`

Object Class Type
auxiliary

OID

Required Attributes
N / A

Allowed Attributes
`preferredLanguage`, `preferredLocale`, `preferredTimeZone`

sunISManagedOrganization

Supported by
Calendar Server 6.0, Messaging Server 6.0

Definition
For LDAP Schema 2, this is a core class for both Messaging and Calendar products doing authentication with SSO. Every physical node must contain this class, including the root suffix.

The attribute holds the fully qualified login host name.

Superior Class
`top`

Object Class Type
auxiliary

OID

Required Attributes
N / A

Allowed Attributes
sunOrganizationAlias

sunManagedOrganization

Supported by
Calendar Server 6.0, Messaging Server 6.0

Definition
This is a core class for both Messaging and Calendar products. Every physical node must contain this class.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.185

Required Attributes
inetDomainStatus

Allowed Attributes
sunPreferredDomain, businessCategory, sunPreferredOrganization, telephoneNumber, sunOverrideTemplates

sunNameSpace

Supported by
Identity Server

Definition

Used for LDAP Schema 2 only. Required to be present at the root of a subtree representing a namespace. Identity Server enforces the uniqueness attribute for namespaces.

Any organization or its subtree nodes can be designated as a namespace by extending the organization LDAP entry with this object class. Namespaces based on different unique attributes may overlap. That is, a subtree of a node designated as a namespace could also be its own namespace if the unique attributes are different. For example, the parent node could use `uid` to enforce uniqueness, while the child node uses the employee number.

This is a different paradigm than was used in LDAP Schema 1, in which every domain was considered a unique namespace (using `uid` as the default unique attribute). For LDAP Schema 2, all namespaces must be explicitly declared using this object class.

NOTE After Identity Server is installed, the root-suffix node contains this object class, but not its corresponding attribute. If you want to provision more than one unique namespace for your Messaging Server or Calendar Server installation, do not add `sunNameSpaceUniqueAttrs` to the root-suffix node.

For more information about namespaces, see the *Sun Java™ Enterprise System Installation Guide*.

Superior Class

`top`

Object Class Type

auxiliary

OID

1.3.6.1.4.1.42.2.27.9.2.29

Required Attributes

N / A

Allowed Attributes

`sunNameSpaceUniqueAttrs`

sunServiceComponent

Supported by
Calendar Server 6.0, Messaging Server 6.0

Definition
Templates are LDAP entries of this object class. Search templates are used to describe how applications should construct searches to send to the directory server in order to locate entries in the DIT.

The entry is named by its required ou attribute.

Superior Class
top

Object Class Type
auxiliary

OID
1.3.6.1.4.1.42.2.27.9.2.27

Required Attributes
organizationalUnitName (ou)

Allowed Attributes
description, sunKeyValue, sunServiceId, sunSmsPriority, sunXmlKeyValue

userPresenceProfile

Supported by
Messaging Server 5.0

Definition
Used to store the presence information for a user.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.136

Required Attributes
N / A

Allowed Attributes
`vacationEndDate`, `vacationStartDate`

Attributes

This section describes the following Identity Server attributes:

associatedDomain

Origin
LDAP Schema 2

Syntax
dn, multi-valued

Object Classes
`inetDomain, sunManagedOrganization`

Definition
Specifies the DNS domain name aliases used to lookup an organization entry.

Used when a domain subtree is being referenced by domain names in addition to the one specified in the attribute `sunPreferredDomain`.

Example
`associatedDomain:qa.sesta.com`

`associatedDomain:eng.sesta.com`

OID

inetGroupStatus

Origin
Identity Server

Syntax
cis, single-valued

Object Classes
`iplanet-am-managed-group`

Definition
This is a global status for groups and overrides the status found in `inetMailGroupStatus`. It holds the current status of the group: `active`, `inactive`, or `deleted` for all services. It is used by Identity Server to manage groups. Status changes can be made to a group's status using the `commcli` interface, or by directly changing the LDAP entry for the group.

The following table lists the attribute's values and their meanings:

Table 4-1 Status Attribute Values

Value	Description
active	The group is active and its users may use services enabled by the overlay of service-specific object classes and the service state as indicated by the particular status attribute for that service.
inactive	Group is inactive. The group users may not use any services granted by service-specific object classes. This state overrides individual service status set using the service's status attributes.
deleted	Group is marked as deleted. The group may remain in this state within the directory for some time (pending purging of deleted groups). Service requests for all groups marked as deleted will return permanent failures.

A missing value implies status is `active`. An illegal value is treated as `inactive`.

Example
`inetGroupStatus: active`

OID
1.3.6.1.4.1.42.2.27.9.1.588

iplanet-am-group-subscribable

Origin
Identity Server

Syntax
boolean, single-valued

Object Classes
iplanet-am-managed-group

Definition
Specifies if users can subscribe to the group. Boolean value: `true`, `false`. Default setting is `true`.

If the value is `true`, the group can be seen, searched for and subscribed to by end users. If the value is `false`, the group can be seen and searched for but can not be subscribed to by end users.

Filtered groups can not be subscribed to; this attribute is ignored if found on a filtered group.

Example
`iplanet-am-group-subscribable: true`

OID
2.16.840.1.113730.3.1.1085

iplanet-am-modifiable-by

Origin
Identity Server

Syntax
dn, multi-valued

Object Classes
iplanet-am-managed-person

Definition
This attribute lists the role-dn of the administrator who has access rights to modify this user entry. By default, the value is set to the role-dn of the administrator who created the account.

Example
For native mode (with domain nodes on the organization tree):

```
iplanet-am-modifiable-by: cn:Top-level Admin Role, o=sesta.com
```

For compatibility mode (with domain nodes on the DC Tree):

```
iplanet-am-modifiable-by: cn=Top-level Admin Role, dc=sesta, dc=com
```

OID
2.16.840.1.113730.3.1.1094

iplanet-am-role-aci-description

Origin
Identity Server

Syntax
string, multi-valued

Object Classes
iplanet-am-managed-person

Definition
Description of the ACI that belongs to this role.

Example

OID
2.16.840.1.113730.3.1.1081

iplanet-am-role-aci-list

Origin
Identity Server

Syntax
string, multi-valued

Object Classes
iplanet-am-managed-role

Definition
The set of ACIs associated with this role. The format is a DN:ACI pair, where the DN of the entry is specified with its ACI. When deleting a role, this attribute allows for the ACIs associated with this role to be located and cleaned up properly.

Example
For native mode (with domain nodes on the organization tree):

```
iplanet-am-role-aci-list: o=sesta.com,o=basedn:aci:
(target="ldap:///o=sesta.com,o=basedn")(targetfilter=(!(|(nsroledn=cn=Top-le
vel Admin Role,o=sesta.com,o=basedn)(nsroledn=cn=Top-level Help Desk Admin
Role,o=sesta.com,o=basedn))))(targetattr != "nsroledn")(version 3.0; acl
"Organization Admin access allow"; allow (all) roledn =
"ldap:///cn=myrole,o=sesta.com,o=basedn";)
```

For compatibility mode (with domain nodes on a DC Tree):

```
iplanet-am-role-aci-list: dc=sesta,dc=com:aci:
(target="ldap:///dc=sesta,dc=com")(targetfilter=(!(|(nsroledn=cn=Top-level
Admin Role,dc=sesta,dc=com)(nsroledn=cn=Top-level Help Desk Admin
Role,dc=sesta,dc=com))))(targetattr != "nsroledn")(version 3.0; acl
"Organization Admin access allow"; allow (all) roledn =
"ldap:///cn=myrole,dc=sesta,dc=com";)
```

OID
2.16.840.1.113730.3.1.1082

iplanet-am-role-any-options

Origin
Identity Server

Syntax
string, multi-valued

Object Classes
iplanet-am-managed-role

Definition
Not currently used.

Example

OID
2.16.840.1.113730.3.1.1084

iplanet-am-role-description

Origin
Identity Server

Syntax
cis, multi-valued

Object Classes
iplanet-am-managed-role

Definition
An optional description of the role being defined.

Example
`iplanet-am-role-description: Top Level Admin Role`

OID
2.16.840.1.113730.3.1.1080

iplanet-am-role-managed-container-dn

Origin
Identity Server

Syntax
dn, multi-valued

Object Classes
iplanet-am-managed-role

Definition
Defines the container this role resides in.

Example
For example, if the role being defined administers the domain organization `east`:

`iplanet-am-role-managed-container-dn: ou=east,o=sesta.com,o=`*basedn*

OID
2.16.840.1.113730.3.1.977

iplanet-am-role-service-options

Origin
Identity Server

Syntax
string, multi-valued

Object Classes
iplanet-am-managed-role

Definition
Not currently used.

Example

OID
2.16.840.1.113730.3.1.1083

iplanet-am-role-type

Origin
Identity Server

Syntax
string, multi-valued

Object Classes
iplanet-am-managed-role

Definition
Defines the type of role. There are three values, as shown in the following table:

Role Value	Role Names
1	Top Level Admin Role
2	General Admin Role
3	User Role

Even though this attribute is defined as multi-valued string, it is implemented in Messaging Server as if it were a single-valued integer.

Example
```
iplanet-am-role-type: 1
```

OID
2.16.840.1.113730.3.1.1079

iplanet-am-service-status

This attribute is aliased to sunRegisteredServiceName. Use that attribute instead.

iplanet-am-static-group-dn

Origin
Identity Server

Syntax
dn, multi-valued

Object Classes
iplanet-am-managed-group

Definition
Defines the DNs for the static groups this user belongs to.

Example
For native mode (with domain nodes on the organization tree):

```
iplanet-am-static-group-dn: cn=mygroup, ou=groups, o=sesta.com
```

For compatibility mode (with domain nodes on the DC Tree):

```
iplanet-am-static-group-dn: cn=mygroup, ou=groups, dc=sesta, dc=com
```

OID
2.16.840.1.113730.3.1.1094

iplanet-am-user-account-life

Origin
Identity Server

Syntax
date string, single-valued

Object Classes
iplanet-am-user-service

Definition
Specifies the account expiration date in the following format:

yyyy/mm/dd hh:mm:ss

where the first mm is for month, dd is for day, yyyy for full year (for example, 2005), hh is for the time stamp hour, the final mm is for the timestamp minutes, and ss is for the timestamp seconds.

If this attribute is present, the authentication service will disallow login if the current date has passed the specified account expiration date.

Example
iplanet-am-user-account-life: 2040/12/31 23:59:59

OID
2.16.840.1.113730.3.1.976

iplanet-am-user-admin-start-dn

Origin
Identity Server

Syntax
dn, single-valued

Object Classes
iplanet-am-user-service

Definition
Specifies the starting point node (DN) displayed in the starting view of the IS Console when this administrator logs in.

Example
iplanet-am-user-admin-start-dn: ou=people, o=sesta.com, o=*basedn*

OID
2.16.840.1.113730.3.1.1072

iplanet-am-user-alias-list

Origin
Identity Server

Syntax
string, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Defines a list of aliases for the user.

Example
User `jdoe` could have an alias of `jd`, `johnd`, or `jd123456`.

```
iplanet-am-user-alias-list: jd
iplanet-am-user-alias-list: johnd
iplanet-am-user-alias-list: jd123456
```

OID
1.3.6.1.4.1.42.2.27.9.1.59

iplanet-am-user-auth-config

Origin
Identity Server

Syntax
string, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Specifies the user authentication configuration method in an XML string. There is no default value.

Example

```
<AttributeValuePair><Value>com.sun.identity.authentication.modules.ldap.LD
AP REQUIRED </Value></AttributeValuePair>
```

OID

1.3.6.1.4.1.42.2.27.9.1.58

iplanet-am-user-auth-modules

Origin

Identity Server

Syntax

string, multi-valued

Object Classes

iplanet-am-user-service

Definition

Not currently used.

Example

OID

2.16.840.1.113730.3.1.1071

iplanet-am-user-failure-url

Origin

Identity Server

Syntax

string, single-valued

Object Classes

iplanet-am-user-service

Definition
Defines the routing taken (URL user is redirected to) if the login fails. Any valid URL can be used.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.71

iplanet-am-user-federation-info

Origin
Identity Server

Syntax
string, single-valued

Object Classes
`iplanet-am-user-service`

Definition
For Identity Server internal use only. Do not use.

Specifies the user account's Federation specific information. This is managed internally by Identity Server's Federation Management module to store user account's Federation related information, and should not be modified outside of that module.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.74

iplanet-am-user-federation-info-key

Origin
Identity Server

Syntax
string, single-valued

Object Classes
iplanet-am-user-service

Definition
For Identity Server internal use only. Do not use.

Specifies the user account's Federation information key. This is managed internally by Identity Server's Federation Management module to store the user account's Federation information key, and should not be modified outside of that module.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.73

iplanet-am-user-login-status

Origin
Identity Server

Syntax
string, single-valued

Object Classes
iplanet-am-user-service

Definition
Specifies the user status. It takes two values:

- `Active` - The user is allowed to authenticate through the Identity Server.
- `Inactive` - The user is not allowed to authenticate through the Identity Server.

Example

OID
2.16.840.1.113730.3.1.1074

iplanet-am-user-password-reset-force-reset

Origin
Identity Server

Syntax
boolean, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Not currently used.

Specifies whether password will be forced to be reset. Values: `true`, `false`. Defaults to `false`.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.591

iplanet-am-user-password-reset-options

Origin
Identity Server

Syntax
string, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Used internally by Identity Server's password reset module. Do not use. Any values assigned to this attribute will be ignored.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.589

iplanet-am-user-password-reset-passwordChanged

Origin
Identity Server

Syntax
string, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Not used.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.592

iplanet-am-user-password-reset-question-answer

Origin
Identity Server

Syntax
string, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Password question and answer used to prompt user who has forgotten their password. The format is `question answer`.

Example

```
iplanet-am-user-password-reset-question-answer:
favorite restaurant Outback
```

OID
1.3.6.1.4.1.42.2.27.9.1.590

iplanet-am-user-service-status

Origin
Identity Server

Syntax
dn, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Specifies the status of the user for various services.

Example

OID
2.16.840.1.113730.3.1.1073

iplanet-am-user-success-url

Origin
Identity Server

Syntax
dn, single-valued

Object Classes
`iplanet-am-user-service`

Definition
Defines the routing taken (URL the user is directed) if the login succeeds. Any valid URL can be used.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.71

preferredLocale

Origin
Directory Server

Syntax
cis, single-valued

Object Classes
`iPlanetPreferences`

Definition
Used by Identity Server to store user preference for locale. The values accepted by this attribute are described in the *Sun Java™ System Identity Server Administrator's Guide*, chapter 18. Some additional information on locales is located in the *Sun Java™ System Directory Server Reference Manual*.

Example
`preferredLocale:en-US`

OID
2.16.840.1.113730.3.1.39

preferredTimeZone

Origin
Directory Server

Syntax
cis, single-valued

Object Classes
`iPlanetPreferences`

Definition
Used by Identity Server to store user preference for time zone. Supported time zone names can be found in the appendix under "Standard Time Zones" on page 265.

Example
`preferredTimeZone: America/Los Angeles`

OID
TBD

sunAdditionalTemplates

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, multi-valued

Object Classes
`inetDomain, sunManagedOrganization`

Definition
Specifies relative DN (RDN) sequences, that is DNs that are relative to the organization entry. Values identify entries in the configuration templates part of the `ou=services` tree below this organization. These are additional templates beyond those specified in the global configuration templates. These are used to specify operations private to an organization.

This attribute must appear in the top entry for this organization.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.76

sunKeyValue

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, multi-valued

Object Classes
`sunServiceComponent`

Definition

Each value is a “key=value” pair, where the key is the name of the XML element. table lists the keys for search templates.

Table 4-2 Search Template Keys

Key	Description
`attrs`	Attribute to retrieve from LDAP entry.
`rfc2247Flag`	Boolean (`ture`, `false`) that tells applications to use the RFC2247 algorithm for constructing the DN of the LDAP entry, instead of performing an LDAP search using the filter specified in the `inetDomainSearchFilter` attribute.
`baseDN`	If `rfc2247Flag` is set to `true`, and if this key is present, then it must be appended to the algorithmically constructed DN in order to get the DN of the target entry.

For more information on templates and the native and compatibility mode LDAP data models, see Chapter 1, “Overview”.

Example

The following sunKeyValue attributes appear in the default search template for the native mode LDAP data model:

```
sunKeyValue: attrs=objectclass
sunKeyValue: attrs=ou
sunKeyValue: attrs=inetDomainStatus
```

The following sunKeyValue attributes appear in the default search template for compatibility mode (uses the RFC 2247 algorithm for constructing the search DN):

```
sunKeyValue: attrs=objectclass
sunKeyValue: attrs=ou
sunKeyValue: attrs=inetDomainStatus
sunKeyValue: rfc2247=true
sunKeyValue: baseDN=o=internet
```

OID

1.3.6.1.4.1.42.2.27.9.1.83

sunNameSpaceUniqueAttrs

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, multi-valued

Object Classes
sunNameSpace

Definition
Stores the name of an attribute required to be unique across all entries in the subtree.

This attribute allows namespace uniqueness to be enforced. For further explanation of namespaces, see the *Sun Java™ Enterprise System Installation Guide* and the object class description for sunNameSpace.

Example
sunNameSpaceUniqueAttrs:uid

sunNameSpaceUniqueAttrs:c

OID
1.3.6.1.4.1.42.2.27.9.1.85

sunOrganizationAlias

Origin
Identity Server

Syntax
cis, single-valued

Object Classes
userPresenceProfile

Definition
Identity Server uses this attribute for authentication. It holds the fully qualified host name for the server the user is logging into.

The format is: *server.domain*.

Example
`sunOrganizationAlias: seaside.siroe.com`

OID
TBD

sunOverrideTemplates

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, multi-valued

Object Classes
`inetDomain`, `sunManagedOrganization`

Definition
Specifies relative DN (RDN) sequences, that is DNs that are relative to the organization entry. Values identify entries in the configuration templates part of the `ou=services` tree below this organization. These templates override global configuration templates for searches and other operations within this organization.

This attribute must appear in the top entry for this organization.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.77

sunPreferredDomain

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, single-valued

Object Classes
iplanet-am-managed-org-unit, sunManagedOrganization

Definition
Specifies the DNS domain name used to lookup an organization entry when a unique matching organization is required.

When a value for this is available, provisioners should set it so as to enable applications to look up organizations using a domain name.

The domain name value of this attribute must be unique across all organizations in the directory, including the domains named in associatedDomain.

This attribute is for use with native mode data model LDAPs only; it must not be used in DC Tree nodes.

In the native mode LDAP data model, this attribute serves the same function as inetCanonicalDomainName used to in compatibility mode. If you are running in compatibility mode, do not use this attribute.

Example
sunPreferredDomain:sesta.com

OID
2.16.840.1.113730.3.1.1086

sunPreferredOrganization

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, single-valued

Object Classes
iplanet-am-managed-org-unit, sunManagedOrganization

Definition
Specifies the DNS name used to lookup an organization entry when a unique matching organization is required.

When a value for this is available, provisioners should set it so as to enable applications to look up organizations using the organization's name.

This attribute is for use with native mode data model LDAPs only; it must not be used in DC Tree nodes.

Example
`sunPreferredOrganization:sesta.com`

OID
1.3.6.1.4.1.42.2.27.9.1.75

sunRegisteredServiceName

Origin
Identity Server

Syntax
string, multi-valued

Object Classes
`iplanet-am-managed-org-unit`, `sunManagedOrganization`

Definition
Defines the set of names of the registered services. The following services are defined for Messaging Server and Calendar Server:

Service Name	Description
DomainMailService	Mail service definition for domains.
DomainCalendarService	Calendar service definition for domains.
UserMailService	Mail service definition for users.
UserCalendarService	Calendar service definition for users.
GroupMailService	Mail service definition for groups.

For informational purposes: The following services are used by Identity Server for authentication with SSO (Single Sign-On). These services must be registered to the root suffix node. This step is done by Identity Server as part of its installation process. The services are:

- `PlanetAMAuthService`
- `iPlanetAMAuthLDAPService`

- iPlanetAMPolicyConfigService
- iPlanetAMAuthenticationDomainConfigService
- iPlanetAMProviderConfigService

Any one can create a new service and load it into Identity Server. For information on how to do this, see the Identity Server documentation at:

http://docs.sun.com/

Example
sunRegisterdServiceName: DomainMailService

OID
1.3.6.1.4.1.42.2.27.9.1.593

sunServiceId

Origin
Messaging Server 6.0, Calendar Server 6.0

Syntax
cis, single valued

Object Classes
sunServiceComponent

Definition
The kind of template being created. For search templates, the value is StuctureUmsObjects. (At this time search templates are the only publicly defined template.)

Example
sunServiceId:StructureUmsObjects

OID
1.3.6.1.4.1.42.2.27.9.1.79

sunSmsPriority

Origin
Identity Server

Syntax
cis, single valued

Object Classes
sunServiceComponent

Definition
Stores the priority of the service with respect to its siblings.

Example
sunSmsPriority:

OID
1.3.6.1.4.1.42.2.27.9.1.81

sunXmlKeyValue

Origin
Identity Server

Syntax
cis, single valued

Object Classes
sunServiceComponent

Definition
Not currently used.

Example

OID
1.3.6.1.4.1.42.2.27.9.1.84

iPlanet Delegated Administrator for Messaging Classes and Attributes

This chapter describes LDAP object classes and attributes for iPlanet Delegated Administrator for Messaging implementing LDAP Schema 1. The objects and attributes are listed alphabetically.

The chapter is divided into two sections:

Object Classes

This chapter describes the following object classes used by Delegated Administrator and those object classes only used in LDAP Schema 1.

- "nsManagedOrgUnit" on page 238
- "nsManagedPerson" on page 238
- "nsUniquenessDomain" on page 239

inetDomainOrg

Supported by
Messaging Server 5.0

Definition
Used for LDAP Schema 1. Auxiliary class for supporting a Delegated Manager for Messaging managed domain organization.

This object class is used in conjunction with the structural class `organization` to define a domain organization. A domain organization is usually created as a way of introducing hierarchy beneath a customer subtree and assigning administrators for that domain organization. To create a suborganization beneath the parent tree and designate a set of administrators for that suborganization, you would create a domain organization node by using `organizationalUnit` and `inetDomainOrg` object classes. For example, `siroe.com` could have a customer subtree with the DN:

`ou=east,o=siroe.com,o=`*basedn*`.`

How to provision a domain organization for LDAP Schema 1 is described in the *iPlanet Messaging Server 5.2 Provisioning Guide.*

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.132

Required Attributes
N / A

Allowed Attributes
`domOrgMaxUsers`, `domOrgNumUsers`

inetMailGroupManagement

Supported by
Messaging Server 5.0

Definition
Used for LDAP Schema 1 only. Used to extend the base entry created by `groupOfUniqueNames`. `inetMailGroupManagement` is used to store attributes for managing a distribution list by using Delegated Administrator for Messaging. This object class is used in conjunction with `inetMailGroup` and `inetLocalMailRecipient`. The attributes in this object class have no operational impact on the messaging server's MTA or message access / message store.

Superior Class
`top`

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.149

Required Attributes
N / A

Allowed Attributes
`mgrpAddHeader`, `mgmanDenySubscribe`, `mgmanGoodbyeText`, `mgmanHidden`, `mgmanIntroText`, `mgmanJoinability`, `mgmanMemberVisibility`, `mgmanVisibility`, `multiLineDescription`

inetManagedGroup

Supported by
Messaging Server 5.0

Definition
Used to define a managed group. If a managed group is just a department or family group, then the structural class to use is `top`, but it can also be used to make a statically defined group (from `groupOfUniqueNames`) and make that a managed group.

Superior Class
top

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.137

Required Attributes
cn

Allowed Attributes
description, mnggrpAdditionPolicy, mnggrpBillableUser, mnggrpCurrentUsers, mnggrpDeletionPolicy, mnggrpMailQuota, mnggrpMaxUsers, mnggrpStatus, mnggrpUserClassOfServices, nsdaModifiableBy, owner

nsManagedDept

Supported by
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Stores information for a non-administrator group.

Superior Class
groupOfUniqueNames

Object Class Type
auxiliary

OID
2.16.840.1.113730.3.2.88

Required Attributes
N/A

Allowed Attributes
nsMaxDepts, nsMaxUsers, nsNumDepts, nsNumUsers, nsdaModifiableBy, owner

nsManagedDeptAdminGroup

Supported by
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Stores information for a group of administrators for iPlanet Delegated Administrator.

Superior Class
top

Object Class Type

OID
2.16.840.1.113730.3.2.111

Required Attributes
objectClass

Allowed Attributes
N/A

nsManagedDomain

Supported by
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Used only for versions of Messaging Server using iPlanet Delegated Administrator. It contains information necessary to administer domains.

Superior Class
top

Object Class Type

OID
2.16.840.1.113730.3.2.86

Required Attributes
objectClass

Allowed Attributes
nswcalDisallowAccess, nsMaxDepts, nsMaxDomains, nsMaxMailLists, nsMaxUsers, nsNumDepts, nsNumDomains, nsNumMailLists, nsNumUsers, nsdaModifiableBy, owner

nsManagedFamilyGroup

Supported by
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Stores information for a family group managed by a delegated administrator. The family group is like a Group, with a few differences. It was added primarily to support Delegated Administrator deployments using Sun Internet Message Service (SIMS) 4.0.

Superior Class
top

OID
2.16.840.1.113730.3.2.89

Required Attribute
objectClass

Allowed Attributes
nsMaxUsers, nsNumUsers, nsdaModifiableBy, owner

nsManagedISP

Supported by
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Tracks the number of sub-organizations that can be created under this object.

Superior Class
top

OID
2.16.840.1.113730.3.2.85

Required Attribute
objectClass

Allowed Attributes
nsNumDomains

nsManagedMailList

Supported by
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Stores information for a mail list created by enabled users. A mail list must contain this object class in order to be managed by Delegated Administrator.

Superior Class
top

Object Class Type

OID
2.16.840.1.113730.3.2.90

Required Attributes
objectClass

Allowed Attributes
nsMaxUsers, nsNumUsers, nsdaModifiableBy, owner

nsManagedOrgUnit

Supported by
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Stores information for a Delegated Administrator managed organizational unit.

Superior Class
top

OID
2.16.840.1.113730.3.2.87

Required Attributes
objectClass

Allowed Attributes
nsdaModifiableBy, owner

nsManagedPerson

Supported by
Messaging Server 5.0; deprecated for Messaging Server 6.0 with LDAP Schema 2

Definition
This object class is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Stores information about a user. A user entry must contain this object class in order to be managed by Delegated Administrator.

Superior Class
top

Object Class Type

OID
2.16.840.1.113730.3.2.91

Required Attributes
`objectClass`

Allowed Attributes
`memberOf`, `nsdaCapability`, `nsdaDomain`, `nsSearchFilter`, `nsdaModifiableBy`, `owner`

nsUniquenessDomain

Supported by
Messaging Server 5.0; deprecated for Messaging Server 6.0 with LDAP Schema 2

Definition
LDAP Schema 1 object class in support of Delegated Administrator for Messaging. If you are still using LDAP Schema 1, then this object is still valid; otherwise it is deprecated.

This object class is a marker to identify the subtree where the uniqueness of `uid` should be enforced. The `uid` uniqueness plugin used this to determine the scope or sphere of influence for enforcing uniqueness.

Superior Class
top

OID
2.16.840.1.113730.3.2.115

Required Attributes
`objectClass`

Allowed Attributes
N / A

Attributes

domainUidSeparator

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetDomainOrg`

Definition
This attribute is used only for LDAP Schema 1.

This attribute is used by the messaging server to override the default mailbox (MB) home. When present, this attribute specifies that compound user identifications (UIDs) are used in this domain and this attribute specifies the separator. For instance, if + is the separator, the mailbox names in this domain are obtained by replacing the right most occurrence of + in the uid with @. To map an internal mailbox name to the UID, the right most occurrence of @ is replaced with a + in the mailbox name.

While substitution of an @ for the UID separator is sufficient to generate a mailbox name, this may not be the same as any of the user's actual email addresses.

NOTE	Format of internal mailbox names is `uid@domain`, where "domain" is DNS domain mapping to the namespace. The only exception to this rule is mailbox names for users in default domain where only the `uid` is used to construct internal mailbox names. See `inetCanonicalDomainName` on how the default value of domain name used can be overridden in specific cases.

The MTA option used to override this attribute's value is `LDAP_DOMAIN_ATTR_UID_SEPARATOR`.

Example
`domainUIDSeparator: #`

OID
2.16.840.1.113730.3.1.702

domOrgMaxUsers

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetDomainOrg`

Definition
This attribute is used only for LDAP Schema 1.

Maximum number of user entries in a domain organization.

Example
`domOrgMaxUser: 500`

OID
2.16.840.1.113730.3.1.697

domOrgNumUsers

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetDomainOrg

Definition
Number of current user entries in a domain organization.

Example
```
domOrgNumUsers: 345
```

OID
2.16.840.1.113730.3.1.698

memberOfManagedGroup

Origin
Messaging Server 5.0

Syntax
dn, single-valued

Object Classes
ipUser

Definition
Family accounts are not supported in LDAP Schema 2. Use this only if you are using LDAP Schema 1.

Specifies the DN of the family account of which this user is a member.

Example
```
memberOfManagedGroup: cn=Addams Family, ou=groups,o=sesta.com,o=isp
```

OID
2.16.840.1.113730.3.1.704

mgmanAllowSubscribe

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`inetMailGroupManagement`

Definition
Domain name(s) or email addresses of users allowed to subscribe to this mailing list.

Example
`mgmanAllowSubscribe:sesta.com` (Every user at `sesta.com` would be able to subscribe to the list.)

OID
2.16.840.1.113730.3.1.790

mgmanDenySubscribe

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`inetMailGroupManagement`

Definition
Domain name(s) or email addresses of users not allowed to subscribe to this list. The `mgmanDenySubscribe` attribute takes precedence over `mgmanAllowSubscribe`.

Example
`mgmanDenySubscribe:siroe.com`

OID
2.16.840.1.113730.3.1.791

mgmanGoodbyeText

Origin
Messaging Server 5.0

Syntax
cis, single valued

Object Classes
`inetMailGroupManagement`

Definition
Reserved.

Example
TBD.

OID
2.16.840.1.113730.3.1.797

mgmanHidden

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailGroupManagement

Definition
Used with iPlanet Delegated Administrator for Messaging only.

A boolean flag specifying whether or not the group should appear in lists that are requested by people other than the group owners. A value of `true` corresponds with a hidden group, that is, the list is not visible. A value of `false` means that the list is visible. A missing value is the same as a value of `false`.

Example
`mgmanHidden:true`

OID
2.16.840.1.113730.3.1.792

mgmanIntroText

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
inetMailGroupManagement

Definition
Reserved.

Example
TBD.

OID
2.16.840.1.113730.3.1.796

mgmanJoinability

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailGroupManagement`

Definition
Used for LDAP Schema 1 only. Specifies who can subscribe to the group. The allowed values are `ANYONE`, `ALL`, and `NONE` (If this attribute is not specified, the default is `NONE`):

- `ANYONE` – Enables anyone to subscribe.
- `ALL` – Enables anyone authenticated to the directory (or Sun ONE Delegated Adminstrator for Messaging) to subscribe.
- `NONE` – Only owner can add members to a closed distribution list.

Example
`mgmanJoinability:All`

OID
2.16.840.1.113730.3.1.793

mgmanMemberVisibility

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailGroupManagement`

Definition
Only used in LDAP Schema 1 with iPlanet Delegated Administrator for Messaging.

Defines who has rights to view the group membership list (expand the group). This attribute has the keyword values: none, `all`, `true` , anyone. No matter what the setting of this attribute, group owners always retain the right to view (and modify) membership.

However, if this attribute is checked in the case of group expansion as part of an SMTP EXPN command (that is, not as part of an administrative tool that can easily identify whether or not the client is the group owner), then a value of none ends up operating as if the list is unconditionally disabled. This is because SMTP doesn't provided a means of establishing a client's identity, such as "owner".

The following table lists the keywords and gives a description of each:

Table 5-1 Rights Keywords

Rights	Description
anyone	Enables anyone to expand the group (see the members in the mailing list). Also, the MTA returns the addresses of members when an EXPN is performed.
`all or true`	The user has to successfully authenticate to the directory (or iPlanet Delegated Administrator for Messaging) before expansion is allowed.
none	Expansion is not allowed.

Unrecognized values are interpreted as none.

If the attribute is not present, the MTA option EXPANDABLE_DEFAULT controls whether the expansion is allowed.

NOTE LDAP_EXPANDABLE is the MTA option used to specify a different attribute name for this function.

Example
`mgmanMemberVisibility:all`

OID
2.16.840.1.113730.3.1.795

mgmanVisibility

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetMailGroupManagement`

Definition

Example

OID
2.16.840.1.113730.3.1.794

mnggrpAdditionPolicy

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetOrgPerson`

Definition
Reserved.

Example
TBD.

OID
2.16.840.1.113730.3.1.710

mnggrpBillableUser

Origin
Messaging Server 5.0

Syntax
dn, single-valued

Object Classes
inetOrgPerson

Definition
DN of the user who is responsible for paying the bills for this family account or group of users.

Example
```
mnggrpBillableUser: uid=John,ou=people,o=sesta.com,o=isp
```

OID
2.16.840.1.113730.3.1.711

mnggrpCurrentUsers

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
inetOrgPerson

Definition
Current number of users allowed in the managed group. Intended for reporting purposes only. No operational impact.

Example
```
mnggrpCurrentUsers: 20
```

OID
2.16.840.1.113730.3.1.714

mnggrpDeletionPolicy

Origin
Messaging Server 5.0

Syntax
cis, single valued

Object Classes
inetOrgPerson

Definition
Reserved.

Example
TBD.

OID
2.16.840.1.113730.3.1.709

mnggrpMailQuota

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
inetOrgPerson

Definition
Cumulative disk quota allowed for all users in the managed group. A value of -1 specifies that there is no limit on space used by users in the managed group. Intended for reporting purposes only. No operational impact.

Example
mnggrpMailQuota:-1

OID
2.16.840.1.113730.3.1.715

mnggrpMaxUsers

Origin
Messaging Server 5.0

Syntax
int, single-valued

Object Classes
`inetOrgPerson`

Definition
Maximum number of users allowed in the managed group.

Example
30

OID
2.16.840.1.113730.3.1.713

mnggrpStatus

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`inetOrgPerson`

Definition
Reserved.

Example
TBD.

OID
2.16.840.1.113730.3.1.712

mnggrpUserClassOfServices

Origin
Messaging Server 5.0

Syntax
cis, multi-valued

Object Classes
`inetOrgPerson`

Definition
Reserved.

Example
TBD.

OID
2.16.840.1.113730.3.1.716

nsDefaultMaxDeptSize

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
`nsManagedDomain`

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Specifies the default size (in number of users) of a newly created department managed by Delegated Administrator.

Example
`nsDefaultMaxDeptSize:20`

OID
2.16.840.1.113730.3.1.562

nsMaxDepts

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
`organization`, `nsManagedDomain`

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Used with Delegated Administrator. Specifies the maximum number of group entries that can be created under this object.

Example
`nsMaxDepts:200`

OID
2.16.840.1.113730.3.1.557

nsMaxDomains

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
`nsManagedDomain`

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

For use with Delegated Administrator. Specifies the maximum number of suborganizations allowed to be created under this object.

Example
`nsMaxDomains:50`

OID
2.16.840.1.113730.3.1.561

nsMaxMailLists

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single valued

Object Classes
`nsManagedDomain`

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

For use with Delegated Administrator. Specifies the maximum number of mailing lists that can be created under this entry.

Example
`nsMaxMailLists:200`

OID
2.16.840.1.113730.3.1.559

nsMaxUsers

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
`organization`

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

For use with Delegated Administrator. Specifies the maximum number of users that can be created under this entry.

Example
`nsMaxUsers:750`

OID
2.16.840.1.113730.3.1.555

nsNumDepts

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
`organization`, `nsManagedDomain`

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

For use with Delegated Administrator. Tracks the number of nested departments that exist under this object.

Example
nsNumDepts:35

OID
2.16.840.1.113730.3.1.556

nsNumDomains

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
nsManagedDomain

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Used by Delegated Administrator. Tracks the number of suborganizations that exist under this object.

Example
nsNumDomains:5

OID
2.16.840.1.113730.3.1.560

nsNumMailLists

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
nsManagedDomain

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Used by Delegated Administrator. Tracks the number of mail lists that exist under this object.

Example
`nsNumMailLists:200`

OID
2.16.840.1.113730.3.1.558

nsNumUsers

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
int, single-valued

Object Classes
`organization`, `nsManagedDomain`

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Tracks the number of users that can be created under this object.

Example
`nsNumUsers:2000`

OID
2.16.840.1.113730.3.1.554

nsSearchFilter

Origin
Not currently used; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
cis, single-valued

Object Classes
nsManagedPerson

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Reserved for future development for Delegated Administrator.

Example

OID
2.16.840.1.113730.3.1.564

nsdaCapability

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
cis, single-valued

Object Classes
nsManagedPerson

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Specifies whether a user can create a mail list. Supports Delegated Administrator.

Example

OID
2.16.840.1.113730.3.1.563

nsdaDomain

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
cis, single

Object Classes
nsManagedPerson

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Specifies the user's organization, for Delegated Administrator.

Example

OID
2.16.840.113730.3.1.600

nsdaModifiableBy

Origin
Messaging Server 5.0; deprecated in Messaging Server 6.0 with LDAP Schema 2.

Syntax
dn, single-valued

Object Classes
inetOrgPerson

Definition
This attribute is deprecated for LDAP Schema 2, it is supported only for LDAP Schema 1.

Used by Delegated Administrator. Specifies who has modify access to the object in which this attribute appears. DN of the administrator's group used with ACIs to grant rights to manage other groups.

Example
`nsdaModifiableBy: cn=service administrators,ou=group,o=isp`

OID
2.16.840.1.113730.3.1.565

preferredMailMessageStore

Origin
Messaging Server 5.0

Syntax
cis, single-valued

Object Classes
`mailDomain`

Definition
Used by Messaging Server Delegated Administrator for LDAP Schema 1 only.

Used to set the `mailMessageStore` attribute of newly created users. If missing, Delegate Administrator leaves the `mailMessageStore` attribute empty and the access server assumes that the user's mailbox is in the default partition of the server instance.

Example
preferredMailMessageStore: primary

OID
2.16.840.1.113730.3.1.762

Appendix A

General Information

This appendix covers the following topics:

LDAP Overview

Messaging Server and Calendar Server products include object classes and attributes defined by the Lightweight Directory Access Protocol (LDAP) and extensions to the standard LDAP schema that extend the basic functionality of LDAP.

Initially developed at the University of Michigan, LDAP is a lightweight version of the X.500 Directory Access Protocol. LDAP has become an Internet standard for directory services running over TCP/IP.

One or more LDAP servers contain the data that make up the LDAP directory. An LDAP directory stores information in object-oriented hierarchies of entries. Each entry is uniquely identified by a distinguished name, or DN. The DN consists of the comma-separated sequence of attributes and values that specify the unique location of an entry within the directory information tree. This provides a path of names tracing the entry back to the top of the directory hierarchy.

Attribute Syntax

Directory data is represented as attribute-value pairs. Any specific piece of information is associated with a descriptive attribute.

Each attribute has a corresponding syntax definition. The syntax definition describes the type of information provided by the attribute.

Table A-1 Syntax Types

Syntax Method	Abbreviation	Definition
Binary	`bin`	Attribute values are binary
Boolean	`boolean`	Two values possible: Yes or No, True or False, On or Off
Case Exact String	`ces`	Values are case sensitive
Case Ignore String	`cis`	Values are not case sensitive
Telephone	`tel`	Telephone numbers (identical to cis, but blanks and dashes (-) are ignored
Distinguished Name	`dn`	Indicates values are DNs
Integer	`int`	Values are numbers
Operational	`operational`	Not displayed in search results

Required and allowed attributes for each object class are included in the object class listing.

Unless otherwise noted, attributes are assumed to be multi-valued, that is, more than one instance of the attribute can be specified. Attributes that are single-valued, that is, only one instance of the attribute can be specified, are noted as such in the Syntax heading, found in each attribute definition.

Object Identifiers

To meet LDAP and X.500 standards, all attributes and objects should have been assigned Object identifiers (OIDs). An OID is a sequence of integers, typically written as a dot-separated string. The OID identifies who first filed the name of the object or attribute with the standards committee.

In some cases, objects and attributes listed in this document do not have an OID assigned to them yet.

Standard Time Zones

The following two tables lists the time zones recognized by Calendar and Messaging Servers first in alphabetical order, and then by offset from Universal Time Constant (UTC).

Note that in some countries, like Israel, day-light savings time is not always observed every year. The decision is made year-by-year. Also, some individual states in the United States do not observe day-light savings time.

This means that some time offsets will not be accurate unless the definitions are updated as needed in the respective systems (see individual product documentation for information about adjusting time zone offsets).

The following table lists the time zones in alphabetical order.

Time Zone Name	Offset
Africa/Amman	+0300
Africa/Cairo	+0300
Africa/Casablanca	-0000
Africa/Johannesburg	+0200
Africa/Lagos	+0100
Africa/Tripoli	+0100
Africa/Windhoek	+0300
America/Adak	-0900
America/Anchorage	-0800
America/Buenos_Aires	-0300
America/Caracas	-0300
America/Chicago	-0500
America/Costa_Rica	-0600
America/Cuiaba	-0300
America/Denver	-0600
America/Godthab	-0200
America/Grand_Turk	-0400
America/Halifax	-0300
America/Havana	-0400
America/Indianapolis	-0500

Time Zone Name	Offset
America/Los_Angeles	-0700
America/Miquelon	-0200
America/New_York	-0400
America/Phoenix	-0700
America/Port-au-Prince	-0400
America/Santiago	-0300
America/Sao_Paulo	-0200
America/St_Johns	-0230
Asia/Alma-Ata	+0700
Asia/Anandyr	+1400
Asia/Aqtau	+0500
Asia/Aqtobe	+0600
Asia/Baku	+0500
Asia/Bangkok	+0700
Asia/Beirut	+0300
Asia/Bishkek	+0600
Asia/Calcutta	+0530
Asia/Dacca	+0600
Asia/Irkutsk	+0900
Asia/Jerusalem	+0300
Asia/Kabul	+0430
Asia/Kamchatka	+1300
Asia/Karachi	+0500
Asia/Katmandu	+0545
Asia/Krasnoyarsk	+0800
Asia/Magadan	+1200
Asia/Novosibirsk	+0700
Asia/Rangoon	+0630
Asia/Riyadh	+0300
Asia/Shanghai	+0800
Asia/Taipei	+0800

Time Zone Name	Offset
Asia/Tehran	+0400
Asia/Tokyo	+0900
Asia/Ulan_Bator	+0800
Asia/Vladivostok	+1100
Asia/Yakutsk	+1000
Asia/Yekaterinburg	+0600
Asia/Yerevan	+0400
Atlantic/Azores	-0000
Atlantic/Cape_Verde	-0100
Atlantic/South_Georgia	-0200
Atlantic/Stanley	-0300
Australia/Adelaide	+1030
Australia/Brisbane	+1000
Australia/Darwin	+0930
Australia/Hobart	+1100
Australia/Lord_Howe	+1100
Australia/Perth	+0800
Australia/Sydney	+1100
Europe/Bucharest	+0300
Europe/Istanbul	+0300
Europe/London	+0100
Europe/Minsk	+0300
Europe/Moscow	+0400
Europe/Paris	+0200
Europe/Riga	+0300
Europe/Samara	+0500
Europe/Simferopol	+0400
Europe/Warsaw	+0200
Pacific/Apia	-1100
Pacific/Auckland	+1300
Pacific/Chatham	+1345

Time Zone Name	Offset
Pacific/Easter	-0500
Pacific/Fiji	+1200
Pacific/Gambier	-0900
Pacific/Guadalcanal	+1100
Pacific/Honolulu	-1000
Pacific/Kiritimati	+1400
Pacific/Marquesas	-0930
Pacific/Norfolk	+1130
Pacific/Noumea	+1200
Pacific/Pitcairn	-0830
Pacific/Rarotonga	-0930
Pacific/Tongatapu	+1300

The following table lists the time zones by standard-time offset.

Offset	Time Zone Name
-1100	Pacific/Apia
-1000	Pacific/Honolulu
-0900	America/Adak
-0930	Pacific/Rarotonga
-0930	Pacific/Marquesas
-0900	Pacific/Gambier
-0830	Pacific/Pitcairn
-0800	America/Anchorage
-0700	America/Los_Angeles
-0700	America/Phoenix
-0600	America/Denver
-0600	America/Costa_Rica
-0500	America/Chicago
-0500	Pacific/Easter
-0500	America/Indianapolis

Offset	Time Zone Name
-0400	America/New_York
-0400	America/Havana
-0400	America/Port-au-Prince
-0400	America/Grand_Turk
-0300	America/Caracas
-0300	America/Cuiaba
-0300	America/Halifax
-0300	America/Santiago
-0300	Atlantic/Stanley
-0300	America/Buenos_Aires
-0230	America/St_Johns
-0200	America/Sao_Paulo
-0200	America/Miquelon
-0200	America/Godthab
-0200	Atlantic/South_Georgia
-0100	Atlantic/Cape_Verde
-0000	Atlantic/Azores
-0000	Africa/Casablanca
+0100	Europe/London
+0100	Africa/Lagos
+0100	Africa/Tripoli
+0200	Europe/Paris
+0200	Europe/Warsaw
+0200	Africa/Johannesburg
+0300	Europe/Bucharest
+0300	Europe/Istanbul
+0300	Africa/Cairo
+0300	Africa/Amman
+0300	Europe/Riga
+0300	Asia/Beirut
+0300	Africa/Windhoek

Offset	Time Zone Name
+0300	Europe/Minsk
+0300	Asia/Jerusalem
+0300	Asia/Riyadh
+0400	Europe/Simferopol
+0400	Europe/Moscow
+0400	Asia/Yerevan
+0400	Asia/Tehran
+0430	Asia/Kabul
+0500	Asia/Aqtau
+0500	Asia/Baku
+0500	Europe/Samara
+0500	Asia/Karachi
+0530	Asia/Calcutta
+0545	Asia/Katmandu
+0600	Asia/Aqtobe
+0600	Asia/Bishkek
+0600	Asia/Yekaterinburg
+0600	Asia/Dacca
+0630	Asia/Rangoon
+0700	Asia/Alma-Ata
+0700	Asia/Novosibirsk
+0700	Asia/Bangkok
+0800	Asia/Krasnoyarsk
+0800	Asia/Shanghai
+0800	Australia/Perth
+0800	Asia/Taipei
+0800	Asia/Ulan_Bator
+0900	Asia/Irkutsk
+0900	Asia/Tokyo
+0930	Australia/Darwin
+1000	Asia/Yakutsk

Offset	Time Zone Name
+1000	Australia/Brisbane
+1030	Australia/Adelaide
+1100	Australia/Sydney
+1100	Australia/Hobart
+1100	Asia/Vladivostok
+1100	Australia/Lord_Howe
+1100	Pacific/Guadalcanal
+1130	Pacific/Norfolk
+1200	Pacific/Noumea
+1200	Asia/Magadan
+1200	Pacific/Fiji
+1300	Pacific/Auckland
+1300	Asia/Kamchatka
+1300	Pacific/Tongatapu
+1345	Pacific/Chatham
+1400	Asia/Anandyr
+1400	Pacific/Kiritimati

Glossary

Refer to the *Java Enterprise System Glossary* (http://docs.sun.com/doc/816-6873) for a complete list of terms that are used in this documentation set.

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W