Oracle® Communications Unifed Communications Suite Schema Reference

Release 8.1

F17047-01

March 2019

ORACLE®

Oracle® Communications Unifed Communications Suite Schema Reference

Release 8.1.0

F17047-01

Contents

Chapter 1 LDAP Attributes

1.1 abBookType Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piLocalBook

OID   2.16.840.1.113894.1009.1.107.1.1118.1.1

Definition

An address book can either be user-defined or set up from a system-defined type. Currently three system-defined categories are supported, namely, favorites, subscribed, and user-defined. The category display name is stored in the `displayName` attribute of the `piTypeBook` object class. Only user defined `abBookType` can be deleted by users.

1.2 abEventNotificationDestination Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.107.1.1140.1.1

1.3 aclGroupAddr Attribute

Origin   Sun ONE Messaging Server

Syntax   directory string (UTF-8)

Object Classes   inetMailUser

OID   2.16.840.1.113894.1009.1.101.0.1197.1.1

Definition

Indicates that the user is a member of the specified group. This type of group is used for message store folder permissions (ACLs), which you should not confuse with mailing lists,

group objects in LDAP, or LDAP ACLs. (You could construct a dynamic group/mailing list by using an LDAP URL that finds users who have this attribute with a specific value. If you do that, be sure this attribute is indexed properly for that usage.) Used by Calendar Server 6 but not Calendar Server 7.

1.4 alarmflag Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piEntry
OID	2.16.840.1.113894.1009.1.107.1.1129.1.1
Definition	

Specifies whether the alarm is set.

1.5 alarmstatus Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piEntry
OID	2.16.840.1.113894.1009.1.107.1.1130.1.1
Definition	

Specifies whether the status is completed, where 1 represents completed and 0 represents that the activity is not yet started.

1.6 alarmtime Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1131.1.1
Definition	

Specifies the UTC formatted date/time

1.7 alarmtopic Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1132.1.1
Definition	

Specifies the follow up status.

1.8 anniversary Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1058.1.1
Definition	

Specifies the anniversary date.

1.9 assistantName Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1124.1.1
Definition	

Specifies the name of the assistant

1.10 attachment Attribute

Syntax	directory string (UTF-8)
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1135.1.1
Definition	

Specifies the URL information.

1.11 building Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1099.1.1
Definition	

Specifies the building location.

1.12 campus Attribute

Syntax	IA5 string (ASCII), single-valued

Object Classes piTypePerson

OID 2.16.840.1.113894.1009.1.107.1.1096.1.1

Definition

Specifies the physical location of the person.

1.13 category Attribute

Syntax directory string (UTF-8)

Object Classes piEntry

OID 2.16.840.1.113894.1009.1.107.1.1136.1.1

Definition

Specifies that the contact belongs to categories like friends, colleagues etc.

1.14 company Attribute

Syntax directory string (UTF-8), single-valued

Object Classes piTypePerson

OID 2.16.840.1.113894.1009.1.107.1.1033.1.1

Definition

Specifies the contact's company.

1.15 contact Attribute

Syntax directory string (UTF-8)

Object Classes piTypePerson

OID 2.16.840.1.113894.1009.1.107.1.1120.1.1

Definition

Specifies the Contact

1.16 contactPerson Attribute

Syntax directory string (UTF-8), single-valued

Object Classes piTypeABConferenceRoom

OID 2.16.840.1.113894.1009.1.107.1.1119.1.1

Definition

Specifies who needs to be contacted to use the resource (typically a conference room)

1.17 corpDirectoryUrl Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.108.0.1005.1.1

Definition

Enables a domain to point to a different corporate directory, or enables support for multiple corporate directories within that domain. The value of this attribute must be one or more valid corporate directory LDAP URLs.

1.18 dataSource Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1049.1.1

Definition

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

Example

```
dataSource:1.0
```

The postmaster group of the default messaging domain:

```
datasource: Messaging Server Initial Configuration
```

1.19 dateOfBirth Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   pabPerson piTypePerson

OID   2.16.840.1.113894.1009.1.101.0.1050.1.1

Definition

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

Example

```
dateOfBirth: 19740404
```

(date of birth on April 6, 1974.)

1.20 davStore Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.102.1.1004.1.1

Definition

Logical back-end ID. Used only if you have multiple Calendar Server back-end hosts.

Example

```
davStore: backend1
```

1.21 davUniqueId Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.102.1.1001.1.1

Definition

This attribute can be used to specify a globally unique ID for any LDAP entry. The attribute is recommended to be used as the value for the Calendar Server `davcore.uriinfo.permanentuniqueid` configuration parameter. The `populate-davuniqueid` tool sets this attribute. For more information on setting the `davUniqueId` value, see `populate-davuniqueid` Usage.

In the Calendar Server data base, the unique identifier value is case sensitive. If you need to move or recreate the corresponding LDAP entry, make sure to retain the case of the value as is. However, because the value is considered as case insensitive for LDAP comparisons, do not create a unique identifier value for another user or resource entry by just changing the case of the value.

Example

```
davUniqueId: 426dfa81-3ec811e0-808bb160-e71a5247
```

1.22 deleted Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1133.1.1

Definition

Specifies the deletion flag.

1.23 department Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1128.1.1
Definition	

Specifies the contact's work department

1.24 description Attribute

Syntax	directory string (UTF-8)
Object Classes	inetManagedGroup
OID	2.5.4.13

1.25 domainUidSeparator Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1051.1.1
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 (UID's) 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: #
```

1.26 externalAuthPostUrlTemplate Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.102.1.1003.1.1

Definition

This attribute is used for finding the internal Directory Server entry for a user who has authenticated against an external Directory Server. It sets the LDAP URL that must be used to map the user who has authenticated against the external Directory Server to a user in the internal Directory. It is used in conjunction with the `externalAuthPreUrlTemplate` attribute and must be added to each domain entry associated with that external directory.

The attribute value is an LDAP URL of the form:

```
ldap:///<search base DN>?<attributes>?<scope>?<earch filter>
```

where:

- `search base DN`: Specifies the search base DN from which to perform searches. It can be a template or a fixed DN.

- `attributes`: Specifies the list of attributes to be retrieved. It must include the `mail` attribute.

- `scope`: Should be `base`, `one`, or `sub`.

- `search filter`: Specifies either a template or a fixed filter.

Note: No server name is used in this LDAP URL (it must be empty), because the lookup is performed against the internal Directory Server.

Both the search base DN and search filter can be templates containing the following patterns:

- `%o` (full login id)

- `%U` (user part of login id)

- `%V` (domain part of login id)

- `%A[attributename]` (value of attribute specified)

Note: The % character in %o, %U, %V, and %A needs to be encoded as per the general URI definition. That is, the % character becomes %25.

Example

Consider the following LDAP URL:

```
ldap:///uid=%25A[ucsUid],ou=people,o=example.com?mail?base?(objectclass=*)
```

In this example, a search is constructed against the internal User/Group directory with the following values:

- base DN:`uid=jdoe,ou=people,o=example.com`

- scope: `base search`

- filter: `(objectClass=*)`

- attributes to retrieve:`mail`

1.27 externalAuthPreUrlTemplate Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.102.1.1002.1.1

Definition

This attribute is used to authenticate against external Directory Servers. It is used to set the LDAP URL that defines how users must be searched for in the external Directory Server against which authentication is performed. You must add this attribute to each domain entry associated with that external directory. The attribute value is an LDAP URL of the form:

`ldap://<server name>/<search base DN>?<attributes>?<scope>?<search filter>`

where:

- `server name`: Specifies the LDAP pool identifier, defined in the Calendar Server configuration for that specific external directory server. See the `davadmin ldappool create` command for more information on how to configure the LDAP pool.

- `search base DN`: Specifies either a template or fixed DN.

- `attributes`: Specifies a list of attributes to be retrieved that are required to perform external authentication and mapping to the internal Communications Suite directory.

- `scope`: Should be `base`, `one`, or `sub`.

- `search filter`: Specifies either a template or a fixed filter.

Both the search base DN and search filter can be templates containing the following patterns:

- %o (original login ID, as provided by the user over protocol)

- %U (user part of login ID)

- %V (domain part of login ID)

Note: The % character in %o, %U, and %V needs to be encoded as per the general URI definition. That is, the % character becomes %25.

Examples

Consider the following LDAP URL:

```
ldap://examplepool/ou=people,o=example.com?mail?sub?(uid=%25o)
```

In this example, for a user with login ID `john@example.com`, the following subtree search is issued:

- basedn: `ou=people,o=example.com`

- filter: `(uid=john@example.com)`

Consider the following LDAP URL where example.com is the default domain:

```
ldap://examplepool/cn=%U,ou=people,o=example.com?mail?base?(objectclass=*)
```

In this example, for a user with a login ID of John Doe, the following search is issued:

- basedn: `cn=John Doe,ou=people,o=example.com`

- filter: `(objectClass=*)`

If more than one entry matches the search, the authentication is rejected.

1.28 floor Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypeABConferenceRoom piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1050.1.1
Definition	

Specifies the floor of the building.

1.29 fullname Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1057.1.1
Definition	

Specifies the person's full name.

1.30 gender Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1121.1.1

Definition

Specifies the gender.

1.31 groupid Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	icsCalendarGroup
OID	2.16.840.1.113894.1009.1.101.0.1052.1.1

Definition

Identifies the unique name used to create the group calendar. The `groupid` must be unique among all `uid` and `groupid` attributes in its relative namespace. All valid Calendar group entries must have a `groupid` attribute.

Example

```
groupid:calendar1
```

1.32 homeCity Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1003.1.1

Definition

Specifies the contact's city

1.33 homeCountry Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1115.1.1

Definition

Specifies the contact's home country

1.34 homeDomDelivery Attribute

Syntax	boolean (TRUE or FALSE), single-valued
Object Classes	piTypePerson

    OID   2.16.840.1.113894.1009.1.107.1.1141.1.1

    Definition

    Specifies whether the contact's home address will be used as domestic delivery address

1.35 homeIntlDelivery Attribute

    Syntax   boolean (TRUE or FALSE), single-valued

    Object Classes   piTypePerson

    OID   2.16.840.1.113894.1009.1.107.1.1142.1.1

    Definition

    Specifies whether the contact's home address will be used as international delivery address

1.36 homeParcelDelivery Attribute

    Syntax   boolean (TRUE or FALSE), single-valued

    Object Classes   piTypePerson

    OID   2.16.840.1.113894.1009.1.107.1.1144.1.1

    Definition

    Specifies whether the contact's home address will be used as parcel delivery address

1.37 homePOBox Attribute

    Syntax   directory string (UTF-8), single-valued

    Object Classes   piTypePerson

    OID   2.16.840.1.113894.1009.1.107.1.1143.1.1

    Definition

    Specifies the contact's home PO BOX

1.38 homePostalCode Attribute

    Syntax   directory string (UTF-8), single-valued

    Object Classes   piTypePerson

    OID   2.16.840.1.113894.1009.1.107.1.1070.1.1

    Definition

    Specifies the home postal code of the contact

1.39 homePostalDelivery Attribute

Syntax   boolean (TRUE or FALSE), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1145.1.1

Definition

Specifies whether the contact's home address will be used as postal delivery address

1.40 homeState Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1098.1.1

Definition

Specifies the contact's state

1.41 icsAutoaccept Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.102.1.1005.1.1

Definition

When a group receives an invitation, this attribute indicates whether the invitation is marked automatically as accepted. When enabled, the attribute causes the scheduled event to be marked as busy on the group calendar without any member taking any action.

For a Calendar resource, this attribute allows the resource to accept invitations automatically.

The `icsAutoaccept` attribute can have a value of 1, which allows automatic acceptance of invitations, or 0, which prohibits automatic acceptance.

For a group calendar, the default value is 0 (prohibit automatic acceptance of events). For a Calendar resource, the default value is 1 (allow automatic acceptance of events).

Example

```
icsAutoaccept:0
icsAutoaccept:1
```

1.42 icsCalendar Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes	icsCalendarGroup icsCalendarResource icsCalendarUser
OID	2.16.840.1.113894.1009.1.104.1.1020.1.1

Definition

The calendar ID (`calid`) of the default calendar for a user, group, or resource. Required attribute. It is a policy of Calendar Server to construct the `calid` based on the user's uid or the group's `groupid`, since it is guaranteed to be unique. Used by Calendar Server 6 but not Calendar Server 7.

Example

```
icsCalendar: jdoe
```

1.43 icsDomainAcl Attribute

Syntax	IA5 string (ASCII), single-valued
OID	2.16.840.1.113894.1009.1.102.1.1006.1.1

Definition

For use with cross-domain access.

Example

```
icsDomainAcl: @a.com:w
```

For more examples, see Managing Domain Access Controls.

1.44 icsDomainNames Attribute

Syntax	IA5 string (ASCII)
OID	2.16.840.1.113894.1009.1.102.1.1007.1.1

Definition

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

Example

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

1.45 icsDoublebooking Attribute

Syntax	IA5 string (ASCII), single-valued
OID	2.16.840.1.113894.1009.1.102.1.1008.1.1

Definition

Indicates whether a group allows double-booking of events in the group's calendar. When enabled,double-booking allows two events to be scheduled and displayed on the calendar at the same time.

For a Calendar resource, this attribute allows the resource to be booked for two events at the same time.

The `icsDoublebooking` attribute can have a value of 1, which allows double-booking, or 0, which prohibits double-booking.

For a group calendar, the default value is 1 (allow double-booking). For a Calendar resource, the default value is 0 (prohibit double-booking).

Example

```
icsDoublebooking:1
icsDoublebooking:0
```

1.46 icsDWPHost Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	icsCalendarGroup icsCalendarResource icsCalendarUser
OID	2.16.840.1.113894.1009.1.104.1.1021.1.1

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 the back-end server hosting the user, group, or resource. Each user's, group's, or resource's entire calendar will be on a single back---end server. Required if using the Calendar Lookup Database (CLD). Used by Calendar Server 6 but not Calendar Server 7.

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
```

1.47 icsExtendedUserPrefs Attribute

Syntax	directory string (UTF-8)
Object Classes	icsCalendarUser sunUCPreferences

OID   2.16.840.1.113894.1009.1.106.1.1001.1.1

Definition

Extensions for calendar user preferences. The attribute value is a property-value pair. The following are the properties and their values. Primarily used in Calendar Express. Used by Calendar Server 6 but not Calendar Server 7.

Table 1.1 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.
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 the display order of the three date elements: month (M), day (D), and year (Y) .
ceDateSeparator	Any single printable character. For example: / or -	The single character used to delimit displayed date elements. For example, a date can be delimited with a /, such as 12/22/2002, or with a -, such 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.
ceDefaultAgenda	unused	Not currently implemented.
ceDefaultAlarmEmail	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.
ceExludeSatSun	boolean (0, 1)	Calendars don't display if the value is set to 1. Default is the value set to 0.
ceFontFace	One of these values:	Three choices of font face to be used in the user interface.

	1. Times New Roman, Times, serif 2. Courier New, Courier, noon 3. PrimaSans BT, Verdana, sans-serif	
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 the value is set to 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., 1 hour, 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 send 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
```

1.48 icsFirstDay Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.106.1.1002.1.1

Definition

First day of the week to be displayed on user's calendar. Used by Calendar Server 6 but not Calendar Server 7.

Range of values: 1--7, with the values assigned as follows:

Table 1.2 icsFirstDay Values

1	Sunday
2	Monday
3	Tuesday
4	Wednesday
5	Thursday
6	Friday
7	Saturday

Example

```
icsFirstDay: 1
```

1.49 icsSecondaryowners Attribute

Syntax   distinguished name (DN)

Object Classes   icsCalendarGroup icsCalendarResource

OID   2.16.840.1.113894.1009.1.104.1.1022.1.1

Definition

Identifies the distinguished names (DNs) of co-owners of a group Calendar or Calendar resource. Like the primary owner, the users identified with `icsSecondaryowners` have administrative privileges over the Calendar group or Calendar resource entry. Used by Calendar Server 6 but not Calendar Server 7.

The co-owners must be Calendar users in the same domain as the group or resource. That is, Calendar service must be assigned to the co-owners as well as to the Calendar group or resource.

Example

```
icsSecondaryowners:cn=John Smith,o=Sesta,c=US
```

1.50 icsStatus Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.102.1.1009.1.1

Definition

If this attribute is used with icsCalendarDomain, the attribute must be set to active when assigning calendar services to a domain. The attribute describes the status of this domain's calendar service with one of the values specified in icsStatus.

If the attribute is set for a user (icsCalendarUser), group (icsCalendarGroup), or resource (icsCalendarResource), the value of icsStatus affects the availability of the calendar for that individual entry.

See Calendar Status Values for definitions of the attribute's values.

Note: The following information applies only to Calendar Server 6. 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 or group (the user or group status is `inactive`). If icsAllowedServiceAccess has any other value, or if both attributes are missing, then the default user or group status is `active`. Calendar services evaluate the following status attributes in order: `inetDomainStatus`, `icsStatus` (for `icsCalendarDomain`), either `inetResourceStatus` or `inetUserStatus`, and `icsStatus` (for `icsCalendarResource`, `icsCalendarUser`, or `icsCalendarGroup`). The rule is: the first of these attributes that is set to something other than `active` takes precedence over all the others. When this attribute is set for a domain, the following status values apply to all users, groups, and resources in the domain. When this attribute is set for a user, group, or resource, the following status values apply only to that individual entry.

Table 1.3   Calendar Status Values

Status	Definition
active	The user, group, or resource, or all users, groups, and resources in this domain, have access to calendar services.
inactive	Calendar services are blocked for this user, group, or resource, or for any users, groups, or resources in this domain, until the status is changed to active again. Calendars remain in the database and the LDAP entry remains.

deleted	This user, group, or resource entry is marked for deletion. Calendar service is blocked for the user, group, or resource, or for any users, groups, or resources in this domain. Calendars are removed from the database and the LDAP attributes that control the calendar's service are removed. For Calendar Server 7, see To Remove Calendar Users. For Calendar Server 6, the entry is a candidate for cleanup by the csclean utility. After csclean removes the calendar, it sets the value of icsStatus to removed. All the entries remain in the directory, but object classes having to do only with calendars for these users, resources and domains are removed. For example, icsCalendarUser, icsCalendarResource, icsCalendarDomain are removed. In addition, all attributes with the ics prefix are 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.
removed	Indicates that the resource (calendar) associated with this entry has been removed. In addition, the entry itself is marked to be purged from the LDAP directory. If `icsStatus` is set at the domain level, all entries with calendar service in the domain are set to be removed. All calendar service is blocked for the entry (or entries). This setting allows the Delegated Administrator `commadmin domain purge` command to remove the entry (or entries) from the LDAP directory.

Note: A missing or unknown value for the `icsStatus` attribute implies the status is `active`.

Example

```
icsStatus: active
```

1.51 icsTimezone Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   icsCalendarDomain icsCalendarGroup icsCalendarResource icsCalendarUser

OID   2.16.840.1.113894.1009.1.104.1.1023.1.1

Definition

The default time zone for this user, group, or resource calendar. Specifically, a valid time zone from the list found in `Standard Time Zones`. The value is taken from the `ics.conf` setting `calstore.default.timezoneID`. Used by Calendar Server 6 but not Calendar Server 7.

For a user, a time zone can be assigned explicitly through the user preferences attribute (see `icsExtendedUserPrefs`), which overrides the domain-level default.

Example

```
icsTimezone: America/Chicago
```

1.52 inetCalendar Attribute

Syntax	IA5 string (ASCII)
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1025.1.1

Definition

Specifies the URL of the person. The format of this URL is: ics:///?calid=<calid\>

For a group, this attribute specifies the URL used to invite the group. If this is not specified, all members of the group are sent invitations to meetings by default. The format of this URL is: ics:///<uid>[@<domain>]: [<opt_cal_name>]

1.53 inetCanonicalDomainName Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1053.1.1

Definition

For Messaging Server, this attribute specifies the canonical domain name used to map a user entry to the correct organization entry when more than one organization entry exists.

The mail processes use information stored in the organization entry to locate a user's mailbox in the message store. If a user has multiple identities in different domains (associated with the different organization entries), the mail processes need to determine which organization entry to use to find the correct mailbox. The inetCanonicalDomainName attribute points to this canonical organization. If inetCanonicalDomainName were not used, a user with multiple user IDs (in multiple domains) would have a different mailbox for each domain.

Typically, the value of inetCanonicalDomainName is a fully qualified domain name, although this is not an absolute requirement.

The inetCanonicalDomainName attribute is used in LDAP Schema 2 and LDAP Schema 1. For an explanation of Schema 1 and Schema 2 LDAP structures, see the Sun Java Communications Suite Deployment Planning Guide and Sun Java Communications Suite Schema Migration Guide.

Schema 2

In Schema 2, the directory can have two types of organization nodes: base and index. Base nodes appear at the root of the directory tree and contain the organization's data (users and groups).

Typically, index nodes for the organization are created if a deployment involves more than one logical grouping of the same physical data. An index node can appear anywhere in the directory.

Moreover, some LDAP administrators need to create a directory structure in which one organization node is placed above another, and the user data exists below both organization nodes. (You might have to do this to maintain the structure of a legacy user directory or to merge an existing user domain with a recently acquired domain.)

If the directory contains multiple index nodes for the organization or nested organization nodes, a user entry can "belong" logically to more than one organization node. An application such as Messaging Server must determine which organization is the canonical one in order to resolve a domain search and correctly identify the user's mailbox.

In this situation, you must decorate all the non-canonical organization entries with the `inetCanonicalDomainName` attribute, which specifies the domain name of the organization's base node. Its value must be the same as that of the `sunPreferredDomain` attribute in the organization's base node.

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

Note that it serves no purpose to decorate the canonical domain entry itself with the `inetCanonicalDomainName` attribute. If you do, it must have the same value as `sunPreferredDomain`.

If you want multiple domains to have the same attribute settings, you should not create multiple organization nodes. Instead, add `associatedDomain` to the organization's base node to specify the DNS domain name aliases. (Add one instance of `associatedDomain` for each domain name alias.) If the organization's base node is not the canonical domain, then it must contain the `sunPreferredDomain` attribute.

Schema 1

In Schema 1, the `inetCanonicalDomainName` attribute is used for the same purpose as in Schema 2, but it is used with DC nodes in the DC tree.

This attribute is used when more than one DC node in a DC tree refers to the same base node of a user/group tree for a particular domain in the Organization tree. (There can be only one canonical domain name for a domain's user/group base node in the Organization tree, but there can be many DC nodes referring to the same user/group base node.)

In Schema 1, this attribute is not necessary if there is only one DC node referring to a domain's user/group base 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 user/group base 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 user/group base node allows you to have different attribute settings (for example, to achieve different routing) for each one. If you want to be sure the two domains have the same attribute settings (for example, to ensure that they are routed identically), use `aliasedObjectName` on the duplicate node instead.

Example 1 - Schema 2

Suppose the directory contains a base node, `o=sesta`, to store a corporation's user data. In addition, there is an index node, `o=sesta2`, which points to an overlapping subset of users. In this example, `sesta.com` is the canonical domain name.

To identify the actual organization node, you must decorate the non-canonical organization entry (the index node) with the value of the canonical organization node, `inetCanonicalDomainName:sesta.com`:

```
dn:o=sesta,o=rootsuffix
sunPreferredDomain:sesta.com



dn:o=sesta2,o=sesta,o=rootsuffix
inetDomainBaseDN:o=sesta,o=rootsuffix
inetCanonicalDomainName:sesta.com
```

Example 2 - User Login with inetCanonicalDomainName

Assume the two organization nodes, o=sesta and o=sesta2, are decorated as shown in Example 1. The user jdoe logs in to Messaging Server with the following user ID: jdoe@sesta2.com

In this example, there can be only one LDAP entry for the user jdoe.

In this case, Messaging Server performs one or more lookups to determine jdoe's canonical user ID, which consists of the user's uid followed by @ and the user's canonical domain name.

Messaging Server looks up the value of the inetCanonicalDomainName attribute in the sesta2 organization entry. It then replaces the original domain name in the login ID, sesta2, with the canonical domain name, sesta.

Using the canonical user ID, Messaging Server opens jdoe's correct mailbox, which displays all of jdoe's messages, including messages sent to jdoe@sesta2.com, to jdoe@sesta.com, and to any other domain or alias domain associated with jdoe.

Example 3 - User Login without inetCanonicalDomainName

Assume the same directory tree layout as is shown in Example 1, but now inetCanonicalDomainName is not used. The user jdoe logs in to Messaging Server with the following user ID: jdoe@sesta2.com

As in Example 2 (shown above), there can be only one LDAP entry for the user jdoe.

In this case, Messaging Server performs the same lookups it performs in Example 2.

However, because the sesta2 organization entry does not contain the inetCanonicalDomainName attribute, Messaging Server uses the user ID <uid>@sesta2.com to determine which mailbox to open. A second mailbox associated with the sesta2 domain is created (or, if it already exists, opened).

In this mailbox, the user jdoe sees only messages sent to the sesta2 domain; jdoe has no access to any other messages. All other messages are contained in the mailbox associated with the canonical domain.

Example 4 - Schema 1

In a Schema 1 scenario, if two DC Tree nodes exist, dc=sesta and dc=sesta2, both referring to the user/group base node o=sesta, then you must specify the canonical domain name as follows:

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


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

1.54 inetCOS Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.104.1.1024.1.1

Definition

The inetCOS entries are the Delegated Administrator Service Packages assigned to a user or group.

In Delegated Admin 6.4, the Service Packages are stored under the default domain's dn: in the o=cosTemplates subtree. For example (below), the Class of Service referenced by the package is found in:

Example

```
inetCoS: earth
```

1.55 inetDomainBaseDN Attribute

Syntax   distinguished name (DN), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1054.1.1

Definition

In Schema 2, this attribute decorates index nodes configured to support multiple logical groupings that point to the same physical data. In Schema 1, the attribute decorates domain nodes on the DC Tree when in compatibility mode.

1.55.1 Schema 2

When your deployment comprises multiple logical groupings pointing to the same physical data, the directory may be configured to contain index nodes. Each index node must include the attribute inetDomainBaseDN; the attribute's value must point to the physical node under which the physical data is contained. The physical node must be decorated with the `sunManagedOrganization` object class.

1.55.2 Schema 1

Any 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.

1.55.3 Example

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

1.56 inetDomainSearchFilter Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1055.1.1

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

• %o--Original login ID entered by the user

If this attribute is missing, it is equivalent to:

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

Namespaces where users are provisioned with compound userIDs, 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
```

1.57 inetDomainStatus Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1056.1.1

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 1.4   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
```

1.58 inetFreeBusy Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1030.1.1
Definition	

Specifies the URL usually used to see the calendar free-busy time for a user

1.59 inetgroupstatus Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	iplanet-am-managed-group inetGroup
OID	2.16.840.1.113894.1009.1.104.1.1027.1.1
Definition	

This is a status for groups only in Delegated Administrator, and does not apply to Messaging Server or Calendar Server. It holds the current status of the group: `active`, `inactive`, or `deleted` for all services. It is used by Access Manager 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 MTA does not consider inetGroupStatus by default. If you want to have inetGroupStatus checked, you need to add to the MTA options something like:

```
LDAP_USER_STATUS=inetUserStatus
```

```
LDAP_GROUP_STATUS=inetGroupStatus
LDAP_USER_MAIL_STATUS=mailUserStatus
LDAP_GROUP_MAIL_STATUS=inetMailGroupStatus
```

You only need to specify `LDAP_GROUP_STATUS`, but if you are changing one of these settings from the default, it is worthwhile noting them all.

Example

```
inetGroupStatus: active
```

1.60 inetMailGroupStatus Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1057.1.1

Definition

Current status of a mail group. The following table lists the possible status values and gives a description of each:

Table 1.5 inetMailGroupStatus Values

active	Messages are delivered to the members of the mailing list.
inactive	Messages sent to the mailing list result in a transient failure.
disabled	Mailing list is disabled. Messages sent to the mailing list result in a permanent failure returned to the sending MTA with text specified by the ERROR_TEXT_DISABLED_GROUP MTA option. If option is not set, the message "group disabled; cannot receive new mail" will be used.
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 rule is: the first of these attributes that is set to something other than active takes precedence over all the others.

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

The MTA does not consider `inetGroupStatus` by default. If you want to have `inetGroupStatus` checked, you need to add to the MTA options something like:

```
LDAP_USER_STATUS=inetUserStatus
LDAP_GROUP_STATUS=inetGroupStatus
LDAP_USER_MAIL_STATUS=mailUserStatus
LDAP_GROUP_MAIL_STATUS=inetMailGroupStatus
```

You only need to specify `LDAP_GROUP_STATUS`, but if you are changing one of these settings from the default, it is worthwhile noting them all.

Example

```
inetMailGroupStatus:active
```

1.61 inetResourceStatus Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetResource

OID   2.16.840.1.113894.1009.1.104.1.1025.1.1

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 Access Manager 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 1.6   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.
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`). The rule is: the first of these attributes that is set to something other than `active` takes precedence over all the others.

Example

`inetResourceStatus: active`

1.62 inetSubscriberAccountId Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.104.1.1026.1.1

Definition

A unique account ID used for billing purposes.

Example

`inetSubscriberAccountId: A3560B0`

1.63 inetSubscriberChallenge Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   inetSubscriber

OID   2.16.840.1.113894.1009.1.101.0.1058.1.2

Definition

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

Example

`inetSubscriberChallenge:Mother's Maiden Name`

1.64 inetSubscriberResponse Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   inetSubscriber

OID   2.16.840.1.113894.1009.1.101.0.1059.1.2

Definition

Attribute for storing the response to the challenge phrase.

Example

```
inetSubscriberResponse: Mamasita
```

1.65 inetUserHttpURL Attribute

Syntax	IA5 string (ASCII)
Object Classes	inetUser
OID	2.16.840.1.113894.1009.1.101.0.1060.1.1

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
```

1.66 inetUserStatus Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1061.1.1

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 1.7 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.

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

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.

Example

```
inetUserStatus: inactive
```

1.67 iplanet-am-user-account-life Attribute

Syntax   directory string (UTF-8)

Object Classes iplanet-am-managed-person

OID   2.16.840.1.113894.1009.1.101.0.1062.1.1

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
```

1.68 jobTitle Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1072.1.1

Definition

Specifies the contact's job title.

1.69 label Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1146.1.1

Definition

Specifies the formatted text corresponding to delivery address of the contact

1.70 lastPurgeDate Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1134.1.1

Definition

Species the last purge cycle date.

1.71 latitude Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1147.1.1

Definition

Specifies the contact's latitude coordinate

1.72 location Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1126.1.1

Definition

Specifies the contact location.

1.73 logoURL Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1148.1.1

Definition

Specifies the URL that points to a logo of contact's company

1.74 longitude Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1149.1.1

Definition

Specifies the contact's longitude coordinate

1.75 mail rfc822mailbox Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1069.1.1

Definition

Identifies the primary email address for a user, Calendar group, or Calendar resource. This is 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
```

1.76 mailAccessProxyPreAuth Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1070.1.1

Definition

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

Example

```
mailAccessProxyPreAuth: yes
```

1.77 mailAccessProxyReplay Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1072.1.1

Definition

This attribute tells the Messaging Multiplexor how to reconstruct the login string when replaying the login sequence with the back-end 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 back-end server than Communications Suite.

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.

- %A[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=%A[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`.

1.78 mailAdminRole Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1073.1.1

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
```

1.79 mailAllowedServiceAccess Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1074.1.1

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.

Note the effect of the preceding rule:

- If no rule is specified for mailAllowedServiceAccess, users are allowed access to all services from all clients.

- If an allow filter is explicitly specified for any service, users are denied access to all other services that are not specified.

For example, suppose you want to enable S/MIME for a domain. If you do not specify any allow filters or deny filters for mailAllowedServiceAccess, S/MIME is enabled.

Now suppose you specify an allow filter for the pop service. In this case, S/MIME is disabled until you also specify an allow filter for the smime service.

For a full explanation of access filters and an alternate way to control access through the administration console or the configutil utility, see Configuring Client Access to POP, IMAP, and HTTP Services.

1.79.1 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`, `http`, and `smime`. Note that the MMP supports `imap`, `imaps`, `pop`, `pops`, and `smtp`, and `smime`. The back-end supports `imap`, `pop`, `smtp`, `http`, and `smime`.

client_list is a comma separated list of clients (domains) to which access is being granted or denied. The following wild cards can be used for the service list: *, ALL. Wild cards can be substituted for the client list (domains). The following table shows the legal wild cards and gives a description of each:

Table 1.8 Wild cards

Wild cards	Description
ALL, *	The universal wild card. 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 wild card.
UNKNOWN	Matches any host whose name or address are unknown. Use this with care.

1.79.2 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.

1.79.3 Example

This example shows a single rule with multiple services and a single wild card 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 wild cards 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.

The following example shows how to restrict user access to SSL-encrypted POP and IMAP access only:

```
mailAllowedServiceAccess: +imaps,pops:*$+imap,pop:MMP IP address
```

In the preceding example, note that the back-end servers do not recognize the pops and imaps service names, so it is necessary to grant the MMP IP address(es) pop and imap service access. Otherwise, connections for that user between the MMP and the back-end servers will be rejected.

1.80 mailAlternateAddress Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1075.1.1

Definition

Alternate RFC 822 email address of this recipient. If the MTA receives mail with a "to" header with this email address, it rewrites the header with the value of the mail attribute and routes the email to that inbox. The reverse-pointing addresses are rewritten from the value of any of

a user's `mailAlternateAddress` attributes to the value of the user's mail attribute. (That is, the MTA will rewrite the following headers, if they match this attribute, to the value of the user's `mail` attribute.)

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
```

To specify a mail catchall address:

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

1.81 mailAntiUBEService Attribute

Syntax	directory string (UTF-8)
Object Classes	inetMailUser
OID	2.16.840.1.113894.1009.1.101.0.1076.1.1

Definition

The string values given by this and other opt in 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 opt in values, set the following in the `option.dat` file:

```
LDAP_OPTIN=mailAntiUBEService
```

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

```
LDAP_DOMAIN_ATTR_OPTIN=mailAntiUBEService
```

Example

```
mailAntiUBEService: virus
mailAntiUBEService: spam
```

1.82 mailApplyHOHControls Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   inetMailUser inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1023.1.1

1.83 mailAutoReplyAddresses Attribute

Syntax   directory string (UTF-8)

Object Classes   inetMailUser inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1030.1.1

1.84 mailAutoReplyMode Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1077.1.1

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 (`mailDeliveryOption: autoreply`). The two modes for autoreply are:

- echo-- Echo the original message with the added mailAutoReplyText or mailAutoReplyTextInternal to the original sender. echo mode replies are sent unconditionally.

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

NOTE: The two modes support different attributes for composing mail.

Example

```
mailAutoReplyMode: reply
mailAutoReplyMode: echo
```

1.85 mailAutoReplySubject Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1078.1.1

Definition

Subject text of autoreply response. $SUBJECT can be used to insert the subject of the original message into the response.

Example

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

1.86 mailAutoReplyText Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1079.1.1

Definition

Autoreply 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.
```

1.87 mailAutoReplyTextInternal Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1080.1.1

Definition

Autoreply text sent to senders from the recipients domain. If not specified, then internal uses get the mail autoreply text message.

Example

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

1.88 mailAutoReplyTimeout Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1081.1.1

Definition

This value is only used with "mailAutoReplyMode: reply"

Interval, in hours, for successive autoreply responses to any given mail sender. If the value is set to 0 *and* the `mailAutoReplyMode: reply`, then a response is sent back every time a message is received. Autoreply responses are sent out only if the recipient is listed in the `To:` or `Cc:` of the original message.

Example

```
mailAutoreplyTimeout: 48
```

1.89 mailCaptureAddress Attribute

Syntax   directory string (UTF-8)

Object Classes   inetMailGroup inetMailUser inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1198.1.1

1.90 mailClientAttachmentQuota Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1082.1.1

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
```

1.91 mailConversionTag Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1083.1.1

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.

1.92 mailDeferProcessing Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1084.1.1

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).

1.92.1 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.

1.92.2 Example

The default for mail users:

```
mailDeferProcessing: No
```

The default for mailing lists:

```
mailDeferProcessing:Yes
```

1.93 mailDeliveryFileURL Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1085.1.1

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
```

1.94 mailDeliveryOption Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1086.1.1

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. See `mailUserStatus`, `hold`. 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.

- `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 specified 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.

Defaults

The default for users is the first item in the DELVERY_OPTIONS MTA option (normally `mailbox`); the default for groups is the second item (normally `members`).

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 to override the name of the attribute used for this is LDAP_DELIVERY_OPTION.

Note: Because the default behavior if the attribute is not present is usually `mailbox` for user objects and `members` for group objects, it is possible that the object might not have a `mailDeliveryOption` attribute. Ensure that when setting this attribute that you do not

replace all values with only your new value, or that if there was no attribute, you also add the appropriate value to maintain the default behavior along with the behavior you intend to add.

In other words, if a user object does not have a `mailDeliveryOption` attribute, then the default is to deliver mail to the user. If you then set `maildeliveryoption: forward` (or `autoreply`), then mail is *only* forwarded (or replied to) but not delivered. If you intend to keep delivering as well as forward, you must set the following:

```
mailDeliveryOption: mailbox
mailDeliveryOption: forward
```

1.95 mailDetourHostOptin Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1022.1.1

1.96 mailDomainAllowedServiceAccess Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1087.1.1

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.

Note the effect of the preceding rule:

- If no rule is specified for mailAllowedServiceAccess, users are allowed access to all services from all clients.

- If an allow filter is explicitly specified for any service, users are denied access to all other services that are not specified.

For example, suppose you want to enable S/MIME for a domain. If you do not specify any allow filters or deny filters for `mailAllowedServiceAccess`, S/MIME is enabled.

Now suppose you specify an allow filter for the pop service. In this case, S/MIME is disabled until you also specify an allow filter for the smime service.

For a full explanation of access filters and an alternate way to control access through the administration console or the configutil utility, see Configuring Client Access to POP, IMAP, and HTTP Services.

1.96.1 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, http, and smime. Note that the MMP supports imap, imaps, pop, pops, and smtp, and smime. The back-end supports imap, pop, smtp, http, and smime.

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

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

Table 1.9   Wild Cards

Wild cards	Meanings
ALL, *	The universal wild card. 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 wild card.
UNKNOWN	Matches any host whose name or address are unknown. Use this with care.

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

1.96.2 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.

1.96.3 Example

This example shows a single rule with multiple services and a single wild card 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 wild cards 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.

1.97 mailDomainAutoReplyTimeOut Attribute

Syntax   signed integer, single-valued

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1042.1.1

1.98 mailDomainCaptureAddress Attribute

Syntax   directory string (UTF-8)

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1196.1.1

1.99 mailDomainCatchAllAddress Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1088.1.1

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.

1.100 mailDomainCatchallMapping Attribute

Syntax   1.3.6.1.4.1.1466.115.121.1.26{128}, single-valued

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1043.1.1

1.101 mailDomainConversionTag Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1089.1.1

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.

1.102 mailDomainDetourHostOptin Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1048.1.1

1.103 mailDomainDiskQuota Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1063.1.1

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\>`.

Valid numeric values for mailDomainDiskQuota are

`pos_num[G|M|K] or -1 or -2.`

where `pos_num` is a positive number up to a maximum of 4294966272 and G (gigabytes), M
(megabytes), and K (kilobytes) are the valid units of measurement.

You can specify the full quota value as a positive number by itself (for example, 20000000) or use a unit of measurement (for example, 20M).

The maximum mailDomainDiskQuota value is 4096G.

Specifying a mailDomainDiskQuota value of 0 will mean that no mail will be delivered. You can also use the values shown in the following table.

Table 1.10 mailDomainDiskQuota Values

Value	Meaning
-1	No limit on space usage allowed.
-2	Use system default quota.

Example

To specify a quota of 4 gigabytes:

```
mailDomainDiskQuota: 4G
```

To specify the system default quota, do not add `mailDomainDiskQuota` to the LDAP entry. Or you can use the following value:

```
mailDomainDiskQuota: -2
```

1.104 mailDomainMaxMsgRecipientCutoff Attribute

Syntax	signed integer, single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1047.1.1

1.105 mailDomainMaxMsgRecipients Attribute

Syntax	signed integer, single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1046.1.1

1.106 mailDomainMsgMaxBlocks Attribute

Syntax	signed integer, single-valued
OID	2.16.840.1.113894.1009.1.101.0.1064.1.1
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.

1.107 mailDomainMsgQuota Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1065.1.1

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
```

1.108 mailDomainNosolicit Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1041.1.1

1.109 mailDomainOptin1 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1033.1.1

1.110 mailDomainOptin2 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1034.1.1

1.111 mailDomainOptin3 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1035.1.1

1.112 mailDomainOptin4 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1036.1.1

1.113 mailDomainOptin5 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1037.1.1

1.114 mailDomainOptin6 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1038.1.1

1.115 mailDomainOptin7 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1039.1.1

1.116 mailDomainOptin8 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1040.1.1

1.117 mailDomainPrefixText Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1192.1.1

1.118 mailDomainReportAddress Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1066.1.1

Definition

This value is used as the header From: address in DSN's 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 non-local 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.

1.119 mailDomainSenderSieve Attribute

Syntax   directory string (UTF-8)

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1194.1.1

1.120 mailDomainSieveRuleSource Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1067.1.1

Definition

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"];
# $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!" { discard; }
```

1.120.1 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.

1.120.2 MTA Override Option

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

1.120.3 Example

```
require ["fileinto","reject"];
if header :contains "Subject" "New Rules Suggestion" {
    redirect "rules@sesta.com"; # Forward message
}
if header :contains "Sender" "porn.com" {
    discard; # Discard the email, don't inform the sender
}
if size :over 1M {
reject text: # Reject message, send multi-line reply back to sender.
Please do not send large attachments.
Put your file on a server and send the URL. Thank you.
.
;}
if header :contains "Sender" "domainadminstrator@sesta.com" {
    fileinto "complaints.refs"; # File message into folder
}
```

1.121 mailDomainSourceChannel Attribute

Syntax	1.3.6.1.4.1.1466.115.121.1.26{32}, single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1045.1.1

1.122 mailDomainSourceConversionTag Attribute

Syntax	directory string (UTF-8)

Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1032.1.1

1.123 mailDomainSourceMsgMaxBlocks Attribute

Syntax	signed integer, single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1044.1.1

1.124 mailDomainStatus Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1068.1.1

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 1.11   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.
disabled	Mail service for all users in the domain is disabled. All user login attempts are rejected and messages sent to users in this domain result in a permanent failure returned top the sending MTA with text specified by the ERROR_TEST_DISABLED_USER MTA option. If the option is not set, one of the following messages will be used: "user disabled; cannot receive new mail" or "group disabled; cannot receive new

	mail" (depending on whether it is a user or a group).
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 MTA's where the user mailboxes now reside.
overquota	The MTA will not accept new messages for any users in the domain until this value is changed back to active.
unused	Specifies that the MTA will ignore this domain. For this domain no email administrative authority is to be assumed. This attribute is used when a domain entry is not using messaging, but is using other applications.

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 Delegated Administrator commadmin utility, which only recognize and use the current value of mailDomainStatus.

Example

```
mailDomainStatus: active
```

1.125 mailDomainSuffixText Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetDomain sunManagedOrganization
OID	2.16.840.1.113894.1009.1.101.0.1193.1.1

1.126 mailDomainUplevel Attribute

Syntax   signed integer, single-valued

Object Classes   inetDomain sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1031.1.1

1.127 mailDomainWelcomeMessage Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1029.1.1

Definition

Welcome message sent to new users added to this domain. The message must contain a header and a message body. The message header must contain at least a subject line. The header and body are separated by a blank line. Enter the mail-domain welcome message on a single line. You must use a $ (dollar sign) to represent a new line. To indicate a blank line, use $$ (two dollar signs).

You can use the following variables in the mail-domain welcome message:

- [ID] The userid (message store user ID).

- [URL] The url location specified with the configutil parameter, gen.accounturl. You can configure this parameter to point the user to, for example, the url of the administrative interface where the user can customize the client configuration.

Example

The following example would be entered on a single line, even though it appears on this page on multiple lines:

```
mailDomainWelcomeMessage: From: postmaster@siroe.com$Subject: Welcome!$
Dear \
[ID],$Welcome to the mail system.$To customize your email preferences,
go to the following url:$$[URL]$$--postmaster@siroe.com
```

When the user anne logs in for the first time, the following sample mail-domain welcome message would be displayed (depending on the url configuration):

```
From: postmaster@siroe.com
Subject: Welcome!
To: anne@siroe.com
Date: Tue, 7 Nov 2006 10:10:04 --0800
MIME--Version 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Dear anne,
```

```
Welcome to the mail system.
To customize your email preferences, please go to the following url:
http://anne@west.siroe.com:8080/bin/user/admin/bin/enduser
--postmaster@siroe.com
```

1.128 mailEquivalentAddress Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1090.1.1

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.

Example

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

1.129 mailEventNotificationDestination Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   inetMailUser

OID   2.16.840.1.113894.1009.1.101.0.1091.1.1

1.130 mailFolderDefaultAcl Attribute

Syntax   directory string (UTF-8)

Object Classes   inetMailUser mailDomain

OID   2.16.840.1.113894.1009.1.101.0.1092.1.1

1.131 mailForwardingAddress Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1093.1.1

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
```

1.132 mailGrantSendPermissionsTo Attribute

Syntax	directory string (UTF-8)
Object Classes	mailGrantPermission
OID	2.16.840.1.113894.1009.1.101.0.1199.1.1

Definition

This attribute stores the email ID for the delegates for that account. Value of attribute for each entry will be some String, which will be the email ID of the delegate. One instance of the attribute will store one email ID. This attribute is supposed to be multi-valued and case insensitive. This attribute could store any of the user's mail/mailalternate/mailEquivalent addresses. It depends on the client to do the necessary validation and redirection if required.

Examples

```
mailGrantSendPermissionsTo : user1@idc.oracle.com
mailGrantSendPermissionsTo : user2@idc.oracle.com
mailGrantSendPermissionsTo : user3@idc.sun.com
```

1.133 mailHeadOfHouseholdDN Attribute

Syntax	distinguished name (DN), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1024.1.1

1.134 mailHost Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1094.1.1

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
```

1.135 mailingAddress Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1061.1.1
Definition	

Specifies the mailing address, that could be work/home/other

1.136 mailMaxMsgRecipientCutoff Attribute

Syntax	signed integer, single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1003.1.1

1.137 mailMaxMsgRecipients Attribute

Syntax	signed integer, single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1002.1.1

1.138 mailMessageStore Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1095.1.1

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
```

1.139 mailMsgMaxBlocks Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1096.1.1

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.

1.140 mailMsgQuota Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1097.1.1

Definition

Maximum number of messages permitted for a user is set with `mailMsgQuota`. This is a cumulative count for all folders in the store.

This attribute also can specify the number of messages allowed for a particular folder or message type.

Although `mailMsgQuota` is a single-valued attribute, you can use it to specify multiple quota values. You can set individual quota values for specific folders and message types. For details, see Specifying Quotas for Folders and Message Types.

If the `mailMsgQuota` 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.

To specify a mailMsgQuota value for the user's entire mailbox tree, use the following format:

```
mailMsgQuota: msgquota
```

where `msgquota` is the number of messages.

1.140.1 msgquota Values

Valid values for `msgquota` are up to a maximum of 4294967292. Specifying a `msgquota` value of 0 will mean that no mail will be delivered. You can also use the values shown in the following table:

Table 1.12 MsgQuota Values

Value	Meaning
-1	No limit on number of messages allowed
-2	Use system default quota

1.140.2 Specifying Quotas for Folders and Message Types

To enable the quotas for individual folders or specific message types, enable (set to "1") either the `store.folderquota.enable` or `store.typequota.enable` parameter.

To enable and configure message types, you also must enable the `configutil` parameter `store.messagetype.enable` and configure other `configutil` parameters.

1.140.3 Guidelines for Specifying Multiple Quota Values

You can specify the following `mailMsgQuota` values for a user's mailbox tree:

- Quota values for specific folders in the user's mailbox

- Quota values for specific message types such as voice mail or text messages. A message type quota applies to messages of that type in all folders in the user's mailbox.

- A default quota value that applies to all folders and message types in the user's mailbox that are not explicitly assigned quotas.

The following guidelines apply when you assign multiple quota values for a user:

- Quotas do not overlap. For example, when there is a quota for a particular message type or folder, messages of that type or messages in that folder are not counted toward the default quota. Each message counts toward one and only one quota.

- The total quota for the whole user mailbox equals the sum of the values of all the quotas specified by default, type, and folder.

- Message type quotas take precedence over folder quotas. For example, suppose one quota is specified for a user's memos folder and another quota is specified for voice messages. Now suppose the user stores eight voice messages in the memos folder. The eight messages are counted toward the voice-mail quota and excluded from the memos folder quota.

1.140.4 Formatting Quota Values for Folders and Message Types

To specify mailMsgQuota values for folders or message types, use the following format:

```
mailMsgQuota: {msgquota}[;{name}%{msgquota}]...
```

where

{msgquota} is the number of messages. For a description of the valid numeric values, see msgquota Values.

{name} is the name of the folder or message type.

The semicolon (";") is a separator that separates multiple quota values.

The percent sign ("%") associates a folder or message-type name with the quota value that follows it.

1.140.5 Additional Formatting Guidelines for Quota Values

- The first {msgquota} in the syntax shown previously--that is, the first quota value entered after the mailMsgQuota attribute--does not have a name. This value represents the default quota for all folders in the user's mailbox that are not explicitly assigned quotas. The default value applies to all the unnamed folders combined, not individual folders.

- A message-type name starts with a pound sign ("#").

- A folder name does not start with a pound sign ("#").

- The "%" and "#" signs are not allowed in folder names or message-type names.

1.140.6 Example

To specify a quota of 2,000 messages:

```
mailMsgQuota: 2000
```

To specify the system default quota, do not add mailMsgQuota to the LDAP entry. Or you can use the following value:

```
mailMsgQuota: -2
```

To specify a default quota of 2,000 messages for all user folders not explicitly assigned a quota; a voice-message quota of 100 messages; and a quota for the Archive folder of 4,000 messages:

```
mailMsgQuota: 2000;#voice%100;Archive%4000
```

In the preceding example, the 2,000 message default quota includes messages in all user folders except the Archive folder; it also excludes voice messages. The 100 message voice-mail quota includes voice messages in all user folders, including the Archive folder. The 4,000 message Archive-folder quota includes messages in the Archive folder and its subfolders; it includes messages of all types except voice messages.

1.141 mailNosolicit Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1028.1.1

1.142 mailOptin1 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1006.1.1

1.143 mailOptin2 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1007.1.1

1.144 mailOptin3 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1008.1.1

1.145 mailOptin4 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1009.1.1

1.146 mailOptin5 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1010.1.1

1.147 mailOptin6 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetMailUser inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1011.1.1

1.148 mailOptin7 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetMailUser inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1012.1.1

1.149 mailOptin8 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetMailUser inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1013.1.1

1.150 mailParentalControl Attribute

Syntax   directory string (UTF-8)

Object Classes   inetMailUser

OID   2.16.840.1.113894.1009.1.101.0.1098.1.1

Definition

Set to true when parental control is enabled for a user.

Messaging Server uses sieve rules to implement parental control (the ability of a family administrative account to specify mail delivery rules for one or more sub-accounts).

Parental control rules are stored in the family group entry (implemented by using `mailSieveRuleSource` as an attribute of the `inetManagedGroup` object class). When a head of family specifies parental control rules, the rules are transformed to sieve rules and stored in the family group entry.

When a sub-account is tagged for parental control, the DN of the family group entry is stored in the sub-account's user entry (implemented with the `mailSieveRuleRef` attribute). In addition, the `mailParentalControl` attribute is set to `true`.

Allowed values: `true`, `false`

Default value: `false`

Example

```
mailParentalControl: true
```

1.151 mailProgramDeliveryInfo Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.101.0.1099.1.1

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 Sun Java System Messaging Server Administration Guide.

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

Example

```
mailProgramDeliveryInfo: procmail
```

1.152 mailQuota Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1100.1.1

Definition

Specifies, in bytes, the amount of disk space allowed for the user's mailbox.

This attribute also can specify the amount of disk space allowed for a particular folder or message type.

Although `mailQuota` is a single-valued attribute, you can use it to specify multiple quota values. You can set individual quota values for specific folders and message types. For details, see Specifying Quotas for Folders and Message Types.

For a description of the numeric values for specifying quotas, see quota Values.

If the `mailQuota` 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.

To specify a `mailQuota` value for the user's entire mailbox tree, use the following format:

```
mailQuota: quota
```

where quota is the number of bytes or a number with a special meaning.

1.152.1 quota Values

Valid numeric values for quota are

```
pos_num[G|M|K] or 0 or -1  or -2
```

where pos_num is a positive number up to a maximum of 4294967292

and G (gigabytes), M (megabytes), and K (kilobytes) are the valid units of measurement.

You can specify the full quota value as a positive number by itself (for example, 20000000) or use a unit of measurement (for example, 20M).

The maximum quota value of the user mailbox is 4294967292K.

You can also use the values shown in the following table.

Table 1.13 quota Values

Value	Meaning
0	No mail will be delivered
-1	No limit on space usage allowed
-2	Use system default quota

1.152.2 Specifying Quotas for Folders and Message Types

To enable the quotas for individual folders or specific message types, you must run the `configutil` command with the parameters `store.folderquota.enable` and `store.typequota.enable`.

To enable and configure message types, you also must enable the `configutil` parameter `store.messagetype.enable` and configure other `configutil` parameters.

1.152.3 Guidelines for Specifying Multiple Quota Values

You can specify the following mailQuota values for a user's mailbox tree:

• Quota values for specific folders in the user's mailbox

- Quota values for specific message types such as voice mail or text messages. A message type quota applies to messages of that type in all folders in the user's mailbox.

- A default quota value that applies to all folders and message types in the user's mailbox that are not explicitly assigned quotas.

The following guidelines apply when you assign multiple quota values for a user:

- Quotas do not overlap. For example, when there is a quota for a particular message type or folder, messages of that type or messages in that folder are not counted toward the default quota. Each message counts toward one and only one quota.

- The total quota for the whole user mailbox equals the sum of the values of all the quotas specified by default, type, and folder.

- Message type quotas take precedence over folder quotas. For example, suppose one quota is specified for a user's memos folder and another quota is specified for voice messages. Now suppose the user stores eight voice messages in the memos folder. The eight messages are counted toward the voice-mail quota and excluded from the memos folder quota.

1.152.4 Formatting Quota Values for Folders and Message Types

To specify `mailQuota` values for folders or message types, use the following format:

```
mailQuota: {quota}[;{name}%{quota}]...
```

where

{quota} is the number of bytes. For a description of the allowed numeric values, see quota Values.

{name} is the name of the folder or message type.

The semicolon (";") is a separator that separates multiple quota values.

The percent sign ("%") associates a folder or message-type name with the quota value that follows it.

1.152.5 Additional Formatting Guidelines for Quota Values

- The first {quota} in the syntax shown above--that is, the first quota value entered after the mailQuota attribute--does not have a name. This value represents the default quota for all folders in the user's mailbox that are not explicitly assigned quotas. The default value applies to all the unnamed folders combined, not individual folders.

- A message-type name starts with a pound sign ("#").

- A folder name does not start with a pound sign ("#").

- The "%" and "#" signs are not allowed in folder names or message-type names.

1.152.6 Example

To specify a quota of 4 gigabytes for the user mailbox:

```
mailQuota: 4G
```

To specify the system default quota, do not add `mailQuota` to the LDAP entry. Or you can use the following value:

```
mailQuota: -2
```

To specify a 20 MB default quota for all user folders not explicitly assigned a quota; a 10 MB voice-message quota; and a 100 MB quota for the Archive folder:

```
mailQuota: 20M;#voice%10M;Archive%100M
```

In the preceding example, the 20 MB default quota includes messages in all user folders except the Archive folder; it also excludes voice messages. The 10 MB voice-message quota includes voices messages in all user folders, including the Archive folder. The 100 MB Archive folder quota includes messages in the Archive folder and its subfolders; it includes messages of all types except voice messages.

1.153 mailRoutingAddress Attribute

Syntax　　directory string (UTF-8), single-valued

OID　　2.16.840.1.113894.1009.1.101.0.1101.1.1

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.

1.154 mailRoutingHosts Attribute

Syntax　　directory string (UTF-8)

OID　　2.16.840.1.113894.1009.1.101.0.1102.1.1

Definition

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

When a domain is found to be non-local, the use of this attribute depends on the value of the `route_to_routing_host` MTA option:

- If the value is zero (0), which is the default setting, the attribute was checked as part of the $*
rewrite rule. With a non-local 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.

The `ldap_domain_attr_routing_hosts` MTA option may be used to specify a different
attribute name for this function.

Example

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

1.155 mailRoutingSmartHost Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1103.1.1

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.

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
```

1.156 mailSenderSieve Attribute

Syntax   directory string (UTF-8)

Object Classes	inetMailGroup inetMailUser inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1195.1.1

1.157 mailSendMaxMsgBlocks Attribute

Syntax	signed integer, single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1004.1.1

1.158 mailSieveCollection Attribute

Syntax	directory string (UTF-8)
Object Classes	inetMailGroup inetMailUser inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1001.1.1

1.159 mailSieveRuleRef Attribute

Syntax	distinguished name (DN)
Object Classes	inetMailUser
OID	2.16.840.1.113894.1009.1.101.0.1190.1.1

Definition

Specifies the DN of an LDAP entry. The referenced LDAP entry can contain additional mail filters in the entry's `mailSieveRuleSource` attribute. Sieve rules specified in the referenced LDAP entry are applied before sieve rules specified in this user entry. This reference is used only when the `mailParentalControl` attribute is set to `true`.

Example

```
mailSieveRuleRef: cn=Sample Family Group,o=groups,o=Residential,o=userGroupRoot
```

1.160 mailSieveRuleSource Attribute

Syntax	directory string (UTF-8)
Object Classes	inetMailGroup inetMailUser inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1191.1.1

Definition

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 Messaging Server MTA

combines the rules into a single SIEVE script using an ordering parameter (Order) found in a #Rule Info: comment.

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. A script has the following form:

```
require ["fileinto"];
# 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!"
{ discard; }
```

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

Example

```
require ["fileinto", "reject"];
if header :contains "Subject" "New Rules Suggestion" {
    redirect "rules@sesta.com"; # Forward message
}
if header :contains "Sender" "porn.com" {
    discard; # Discard the email, don't inform the sender
}
if size :over 1M {
reject text: # Reject message, send multi-line reply back to sender.
Please do not send large attachments.
Put your file on a server and send the URL. Thank you.
.
;}
if header :contains "Sender" "barkley@sesta.com" {
    fileinto "complaints.refs"; # File message into folder
}
```

1.161 mailSMTPSubmitChannel Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1104.1.1

Definition

Specifies source channel to use (switch) when the user submits messages.

Most commonly, this attribute is used to set up guaranteed message delivery, or other special classes of service. When defined, this attribute tells the MTA to consider the specified channel to be the effective submission channel (ie, the source channel will be switched to the specified

channel), if SMTP AUTH is successful. SMTP authentication is required to determine it is this user and thereby find this attribute.

For mailSMTPSubmitChannel to work, the current source channel must have the `saslswitchchannel` keyword. Connections originating on the tcp_local or tcp_intranet channels will work by default because those have `saslswitchchannel tcp_auth`. For connections originating on the tcp_submit channel, you will need to add `saslswitchchannel tcp_submit` on the tcp_submit channel, if it does not already have it.

For switching based on the MAIL FROM address, see the `userswitchchannel` channel option.

Example

```
mailSMTPSubmitChannel: tcp_tas
```

1.162 mailSourceChannel Attribute

Syntax	1.3.6.1.4.1.1466.115.121.1.26{32}, single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1005.1.1

1.163 mailSourceConversionTag Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1029.1.1

1.164 mailSourceOptin1 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1014.1.1

1.165 mailSourceOptin2 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1015.1.1

1.166 mailSourceOptin3 Attribute

Syntax	directory string (UTF-8), single-valued

Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1016.1.1

1.167 mailSourceOptin4 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1017.1.1

1.168 mailSourceOptin5 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1018.1.1

1.169 mailSourceOptin6 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1019.1.1

1.170 mailSourceOptin7 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1020.1.1

1.171 mailSourceOptin8 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailUser inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1021.1.1

1.172 mailUserStatus Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1105.1.1

Definition

Current status of the mail user. Can be one of the values in the following table: A missing value implies status is `active`. An illegal value is treated as `inactive`.

Table 1.14 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.
disabled	User's mail account is disabled. Messages sent to the user result in a permanent failure returned to the sending MTA with text specified by the ERROR_TEST_DISABLED_USER MTA option. If option is not set, the message "user disabled; cannot receive new mail" will be used.
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.
deliver	A mailUserStatus of deliver is now treated by the MTA as equivalent to active. This new status settings allows mail delivery to continue uninterrupted while effectively locking the user out their account (because other components will treat deliver the same way as inactive). (Feature introduced in Messaging Server 7 Update 3.)
removed	Indicates that the resource (mailbox) associated with this entry has been removed. In addition, the user entry itself 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 Delegated Administrator `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. Messages places in the hold channel queue will be held, meaning they are renamed to the .HELD extension and will not be retried without administrative intervention - see the `qm release` command.
overquota	The MTA will not deliver mail to a mailbox with this status.
defer	Used by `rehostuser` to prevent user from logging in, like hold, but causes mail to be placed in the reprocess queue and retried automatically as per the `backoff` option.
defer-submit	Same as `defer`, but only for message submission (ie, messages arriving via channels with the `submit` keyword, like `tcp_submit`). This allows mail from local senders to be accepted into the `reprocess` channel queue while mail from external users is rejected with a transient failure so the remote MTA will retain the message and retry later.

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 Delegated Administrator `commadmin` utility, which only recognize and use the current value of `mailUserStatus`.

Example

```
mailUserStatus: active
```

1.173 maxPabEntries Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1106.1.1

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
```

1.174 memberOfManagedGroup Attribute

Syntax   distinguished name (DN), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1108.1.1

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
```

1.175 memberOfPAB Attribute

Syntax   directory string (UTF-8)

Object Classes   pabPerson

OID   2.16.840.1.113894.1009.1.101.0.1109.1.1

Definition

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

Example

```
memberOfPAB:addressbook122FA7
```

1.176 memberOfPABGroup Attribute

Syntax   directory string (UTF-8)

Object Classes   pabPerson

OID   2.16.840.1.113894.1009.1.101.0.1110.1.1

Definition

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

Example

```
memberOfPabGroup:testgroup15577F2D
```

1.177 memberOfPIBook Attribute

Syntax   IA5 string (ASCII)

Object Classes   piEntry piTypeCert

OID   2.16.840.1.113894.1009.1.107.1.1101.1.1

Definition

Specifies the piEntryID of each address book that this entry belongs to.

1.178 memberOfPIGroup Attribute

Syntax   IA5 string (ASCII)

Object Classes   piEntry

OID   2.16.840.1.113894.1009.1.107.1.1104.1.1

Definition

Specifies the piEntryID of each group that is entry is present.

1.179 mgmanAllowSubscribe Attribute

Syntax   directory string (UTF-8)

Object Classes   inetMailGroupManagement

OID   2.16.840.1.113894.1009.1.101.0.1111.1.1

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.

1.180 mgmanDenySubscribe Attribute

Syntax   directory string (UTF-8)

Object Classes	inetMailGroupManagement
OID	2.16.840.1.113894.1009.1.101.0.1112.1.1
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
```

1.181 mgmanGoodbyeText Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailGroupManagement
OID	2.16.840.1.113894.1009.1.101.0.1113.1.1
Definition	

TBD

1.182 mgmanHidden Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailGroupManagement
OID	2.16.840.1.113894.1009.1.101.0.1114.1.1
Definition	

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
```

Delegated Administrator 6.4 will set this value. Messaging Express 6.3, Communications Express 6.3, Convergence 1.0 ignore this value when searching for groups.

1.183 mgmanIntroText Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailGroupManagement

OID	2.16.840.1.113894.1009.1.101.0.1115.1.1

Definition

TBD

1.184 mgmanJoinability Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailGroupManagement
OID	2.16.840.1.113894.1009.1.101.0.1116.1.1

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 Delegated Administrator) to subscribe.

- NONE - Only owner can add members to a closed distribution list.

Example

```
mgmanJoinability:All
mgmanjoinability: NONE
```

Delegated Administrator 6.4 will set this value.

1.185 mgmanMemberVisibility Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailGroupManagement
OID	2.16.840.1.113894.1009.1.101.0.1117.1.1

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 1.15 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
```

1.186 mgmanVisibility Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetMailGroupManagement
OID	2.16.840.1.113894.1009.1.101.0.1118.1.1
Definition	

TBD

1.187 mgrpAddHeader Attribute

Syntax	directory string (UTF-8)
OID	2.16.840.1.113894.1009.1.101.0.1119.1.1
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
```

1.188 mgrpAdvertised Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1120.1.1

1.189 mgrpAllowedBroadcaster Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.101.0.1121.1.1

Definition

Identifies mail users allowed to send messages to the mail group. The purpose of this attribute is to restrict who can send messages to the mail group. If no instances of this attribute exist on the `inetMailGroup` entry, there are no restrictions on who can send messages to the mail group unless the `mgrpAllowedDomain`, `mgrpDisallowedDomain`, and `mgrpDisAllowedBroadcaster` attributes are used.

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 multi-valued, each URL or DN 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.

Any email addresses specified are expanded as if they are a mailing list. Unlike a mailing list, this expansion includes all the attributes used to store email addresses (normally `mail`, `mailAlternateAddress`, and `mailEquivalentAddress`). Thus, if an address for the list itself is specified as a `mgrpAllowedBroadcaster`, a user can subscribe to a restricted list using one address and use an alternate address to send messages to the list.

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, the message will bounce or be directed to a moderator (as determined by the `mgrpMsgRejectAction` attribute).

You can specify metacharacter substitutions in this attribute. In particular, the address-related metacharacter sequences ($A for the entire address, $U for the mailbox part, $D for the domain part) refer to the current envelope "from" address and can in some cases be used to limit the results returned by the URL to entries that are likely (or guaranteed) to match. This may make authorization checks more efficient.

Suppose you define a dynamic list through an LDAP lookup where anyone on the list is allowed to post to the mailing group. For example:

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

The effect of this definition is to expand the whole list for the authorization check. However, if you add a restriction so only entries containing the current envelope "from" address are returned to the authorization check, the operation may be much more efficient:

```
mgrpAllowedBroadcaster:
ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)
(objectClass=inetOrgPerson)(mail=$A)
```

In this case, only the sender's entry is checked for broadcast authorization. In the preceding example, all the mail user entries in the Sesta US domain are checked.

To enable metacharacter substitutions, you must enable the MTA option PROCESS_SUBSTITUTIONS. For details about this option, see the Sun Java System Messaging Server Administration Guide.

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

Example

```
mgrpAllowedBroadcaster: uid=bjensen,o=siroe.com
mgrpAllowedBroadcaster: ldap:///uid=bjensen,o=siroe.com
mgrpAllowedBroadcaster:mailto:group1@siroe.com
mgrpAllowedBroadcaster:
ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)(objectClass=inetOrgPerson)(mai
```

1.190 mgrpAllowedDomain Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1122.1.1

Definition

Identifies domains or subdomains from which users are allowed to send messages to the mail group. Note that glob-style wild carding can be used in the domains. In other words, any part of the domain specification can be wild carded.

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.

Examples

`mgrpAllowedDomain:siroe.com` will only match the siroe.com domain.

`mgrpAllowedDomain:*.siroe.com` will match any subdomain of the siroe.com domain.

`mgrpAllowedDomain:*.com` will match any *.com domain.

mgrpAllowedDomain:siroe.* will match any top-level domain beginning with siroe.

1.191 mgrpAuthPassword Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1123.1.1

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.

1.192 mgrpBroadcasterPolicy Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1124.1.1

Definition

Policy for determining allowed broadcaster. It specifies the level of authentication required to verify that the sender matches value of the mgrpAllowedBroadcaster attribute and is therefore allowed to send to the list. 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
```

1.193 mgrpCheckHeader Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	inetMailGroup inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1026.1.1

1.194 mgrpDelayNotifications Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1125.1.1

1.195 mgrpDeliverTo Attribute

Syntax	directory string (UTF-8)
OID	2.16.840.1.113894.1009.1.101.0.1126.1.1

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 URL's, 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.

1.196 mgrpDescription Attribute

Syntax	directory string (UTF-8)
OID	2.16.840.1.113894.1009.1.101.0.1127.1.1

1.197 mgrpDigestInterval Attribute

Syntax	directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1128.1.1

1.198 mgrpDisallowedBroadcaster Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.101.0.1129.1.1

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.

You can specify metacharacter substitutions in this attribute. In particular, the address-related metacharacter sequences ($A for the entire address, $U for the mailbox part, $D for the domain part) refer to the current envelope "from" address and can in some cases be used to limit the results returned by the URL to entries that are likely (or guaranteed) to match. This may make authorization checks more efficient.

Suppose you define a dynamic list through an LDAP lookup where everyone on the list is prohibited from posting to the mailing group. For example:

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

The effect of this definition is to expand the whole list for the authorization check. However, if you add a restriction so only entries containing the current envelope "from" address are returned to the authorization check, the operation may be much more efficient:

```
mgrpDisallowedBroadcaster:
ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)
(objectClass=inetOrgPerson)(mail=$A)
```

In this case, only the sender's entry is checked for broadcast authorization and prevented from posting the message. In the preceding example, all the mail user entries in the Sesta US domain are checked.

To enable metacharacter substitutions, you must enable the MTA option PROCESS_SUBSTITUTIONS. For details about this option, see the Sun Java System Messaging Server Administration Guide.

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: sys50@sesta.com
```

```
mgrpDisallowedBroadcaster: ldap:///o=Sesta,c=US??sub?(&(objectClass=inetMailUser)(obj
```

1.199 mgrpDisallowedDomain Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1130.1.1

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
```

1.200 mgrpErrorsTo Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1131.1.1

Definition

The mgrpErrorsTo attribute specifies either an email address or a URL, which is resolved to produce an address. The address is placed in the MAIL FROM (envelope from) field of all messages the list produces. Additionally, the presence of the `mgrpErrorsTo` attribute causes the MTA to treat the group as a full-fledged mailing list and not as a simple autoforwarder. The basic purpose of the MAIL FROM address is to create a place to send reports of message delivery problems. As such, the main effect of `mgrpErrorsTo` is to cause errors delivering list mail to be directed to the `mgrpErrorsTo` address.

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

1.201 mgrpJettisonBroadcasters Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1132.1.1

1.202 mgrpJettisonDomain Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1133.1.1

1.203 mgrpListTag Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1134.1.1

1.204 mgrpMaxMessagesPerDay Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1135.1.1

1.205 mgrpModerator Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.101.0.1136.1.1

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).

You can specify metacharacter substitutions in this attribute. In particular, the address-related metacharacter sequences ($A for the entire address, $U for the mailbox part, $D for the domain part) refer to the current envelope "from" address and can in some cases be used to limit the results returned by the URL to entries that are likely (or guaranteed) to match. This may make authorization checks more efficient.

To enable metacharacter substitutions, you must enable the MTA option PROCESS_SUBSTITUTIONS. For details about this option, see the Sun Java System Messaging Server Administration Guide.

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

Example

```
mgrpModerator: [jordan@sesta.com|mailto:jordan@sesta.com]
```

1.206 mgrpMsgMaxSize Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.101.0.1137.1.1

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
```

1.207 mgrpMsgPrefixText Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1138.1.1

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.

The prefix text is inserted in the body of a message that is text-only. If a message is not text-only, the prefix text is not added.

1.208 mgrpMsgRejectAction Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1139.1.1

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
```

1.209 mgrpMsgRejectText Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1140.1.1

Definition

Specifies the error text to use in the 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.)

1.210 mgrpMsgSuffixText Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1141.1.1

Definition

Specifies the text to be appended to the text message. You must supply the formatting. That is, you must insert any CRLF's (carriage return, line feeds) that belong in the text. The suffix text is inserted in the body of a message that is text-only. If a message is not text-only, the suffix text is not added.

Note: The `ldap_suffix_test` MTA option can be used to specify a different attribute to be used for this function.

1.211 mgrpPublicRoster Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1142.1.1

1.212 mgrpRemoveHeader Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1144.1.1

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.

1.213 mgrpRFC822MailMember Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.101.0.1143.1.1

1.214 mgrpSubscribePolicy Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1145.1.1

1.215 mgrpTrustNewMembers Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1146.1.1

1.216 mgrpUniqueId Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1147.1.1

1.217 mgrpUnsubscribePolicy Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1148.1.1

1.218 mgrpURLResultMapping Attribute

Syntax   1.3.6.1.4.1.1466.115.121.1.26{128}, single-valued

Object Classes   inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1025.1.1

1.219 mgStatus Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.109.0.1001.1.1

1.220 middlename Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1056.1.1

Definition

Specifies the contact's middle name.

1.221 mlsubActionKey Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1149.1.1

1.222 mlsubDigest Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1150.1.1

1.223 mlsubJoinDate Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1151.1.1

1.224 mlsubJoinIPAddress Attribute

Syntax   directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1152.1.1

1.225 mlsubListIdentifier Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1153.1.1

1.226 mlsubMail Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1154.1.1

1.227 mlsubReceiveMail Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1155.1.1

1.228 mlsubRole Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1156.1.1

1.229 mlsubSuppressDuplicates Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1157.1.1

1.230 mlsubTentativeEmail Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1158.1.1

1.231 mlsubTrack Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1159.1.1

1.232 mluserJoinDate Attribute

Syntax directory string (UTF-8), single-valued

OID 2.16.840.1.113894.1009.1.101.0.1160.1.1

1.233 mluserJoinIPAddress Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1161.1.1

1.234 mluserPassword Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1162.1.1

1.235 mluserUniqueId Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1163.1.1

1.236 mnggrpAdditionPolicy Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1164.1.1

Definition

TBD

1.237 mnggrpBillableUser Attribute

Syntax   distinguished name (DN), single-valued

Object Classes   inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1165.1.1

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
```

1.238 mnggrpCurrentUsers Attribute

Syntax   signed integer, single-valued

Object Classes   inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1166.1.1

Definition

Current number of users allowed in the managed group. Intended for reporting purposes only. No operational impact.

Example

```
mnggrpCurrentUsers: 20
```

1.239 mnggrpDeletionPolicy Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1167.1.1

Definition

TBD

1.240 mnggrpMailQuota Attribute

Syntax   signed integer, single-valued

Object Classes   inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1168.1.1

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
```

1.241 mnggrpMaxUsers Attribute

Syntax   signed integer, single-valued

Object Classes   inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1169.1.1

Definition

Maximum number of users allowed in the managed group.

1.242 mnggrpStatus Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1170.1.1
Definition	

TBD

1.243 mnggrpUserClassOfServices Attribute

Syntax	directory string (UTF-8)
Object Classes	inetManagedGroup
OID	2.16.840.1.113894.1009.1.101.0.1171.1.1
Definition	

TBD

1.244 msgCRLMappingRecord Attribute

Syntax	directory string (UTF-8)
Object Classes	msgCRLMappingTable
OID	2.16.840.1.113894.1009.1.101.0.1172.1.1

1.245 msgVanityDomain Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	msgVanityDomainUser
OID	2.16.840.1.113894.1009.1.101.0.1173.1.1
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.

1.246 multiLineDescription Attribute

Syntax	directory string (UTF-8)
Object Classes	inetMailGroupManagement piTypeBook
OID	2.16.840.1.113894.1009.1.101.0.1174.1.1

Definition

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

For an address book entry, it specifies the detailed description associated with the address book.

For the piEntry objectclass, this specifies the URL that identifies recipient(s) of request-to-be-added to messages.

Example

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

1.247 nabDomainAcl Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.108.0.1002.1.1

Definition

For use with cross-domain access.

1.248 nabDomainNames Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.108.0.1003.1.1

Definition

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

1.249 nabStatus Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.108.0.1001.1.1

Definition

Absence of this attribute or a value of `active` indicates `active` status. A value of `removed`, `deleted`, or `inactive` disables the Contacts Server service. Any other value enables the service, but this is not recommended.

1.250 nabStore Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.108.0.1004.1.1

Definition

Indicates the Contacts Server back-end host on which a user's data resides, if the deployment uses multiple back-end hosts.

1.251 nickName Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	pabGroup pabPerson
OID	2.16.840.1.113894.1009.1.101.0.1175.1.1

Definition

Specifies a short name associated with the contact. This must be unique amongst all contacts in any address book store.

1.252 notes Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1117.1.1

Definition

Specifies the notes associated with this contact

1.253 nsdaCapability Attribute

Syntax	directory string (UTF-8)
OID	2.16.840.1.113894.1009.1.101.0.1182.1.1

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.

1.254 nsDADomain Attribute

Syntax	directory string (UTF-8), single-valued
OID	2.16.840.1.113894.1009.1.101.0.1176.1.1

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.

1.255 nsdaModifiableBy Attribute

Syntax	distinguished name (DN)
Object Classes	inetManagedGroup nsManagedDomain
OID	2.16.840.1.113894.1009.1.101.0.1183.1.1

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 ACI's to grant rights to manage other groups.

For example:

```
nsdaModifiableBy: cn=service administrators,ou=group,o=isp
```

1.256 nsMaxDomains Attribute

Syntax	signed integer, single-valued
Object Classes	nsManagedDomain
OID	2.16.840.1.113894.1009.1.101.0.1177.1.1

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
```

1.257 nsMaxUsers Attribute

Syntax	signed integer, single-valued
Object Classes	nsManagedDomain
OID	2.16.840.1.113894.1009.1.101.0.1178.1.1

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
```

1.258 nsNumDomains Attribute

Syntax   signed integer, single-valued

Object Classes   nsManagedDomain

OID   2.16.840.1.113894.1009.1.101.0.1179.1.1

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
```

1.259 nsNumMailLists Attribute

Syntax   signed integer, single-valued

Object Classes   nsManagedDomain

OID   2.16.840.1.113894.1009.1.101.0.1180.1.1

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
```

1.260 nsNumUsers Attribute

Syntax   signed integer, single-valued

Object Classes   nsManagedDomain

OID   2.16.840.1.113894.1009.1.101.0.1181.1.1

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
```

1.261 nsRoleDN Attribute

Syntax	distinguished name (DN), single-valued
Object Classes	nsNestedRoleDefinition
OID	2.16.840.1.113894.1009.1.104.1.1030.1.1

1.262 nsRoleScopeDN Attribute

Syntax	distinguished name (DN), single-valued
Object Classes	nsNestedRoleDefinition
OID	2.16.840.1.113894.1009.1.104.1.1031.1.1

1.263 nsValueBin Attribute

Syntax	binary
OID	2.16.840.1.113894.1009.1.100.0.1001.1.1

1.264 nsValueCES Attribute

Syntax	IA5 string (ASCII)
OID	2.16.840.1.113894.1009.1.100.0.1002.1.1

1.265 nsValueCIS Attribute

Syntax	directory string (UTF-8)
OID	2.16.840.1.113894.1009.1.100.0.1003.1.1

1.266 nsValueDefault Attribute

Syntax	directory string (UTF-8)
OID	2.16.840.1.113894.1009.1.100.0.1005.1.1

1.267 nsValueDescription Attribute

Syntax	directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.100.0.1006.1.1

1.268 nsValueDN Attribute

Syntax   distinguished name (DN)

OID   2.16.840.1.113894.1009.1.100.0.1004.1.1

1.269 nsValueFlags Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.100.0.1007.1.1

1.270 nsValueHelpURL Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.100.0.1008.1.1

1.271 nsValueInt Attribute

Syntax   signed integer

OID   2.16.840.1.113894.1009.1.100.0.1009.1.1

1.272 nsValueSyntax Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.100.0.1010.1.1

1.273 nsValueTel Attribute

Syntax   telephone number

OID   2.16.840.1.113894.1009.1.100.0.1011.1.1

1.274 nsValueType Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.100.0.1012.1.1

1.275 nswmExtendedUserPrefs Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.106.1.1003.1.1

Definition

This attribute holds the pairs that define client user 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=OtisFanning$ofanning@sesta.com


Example 5: nswmExtendedUserPrefs: meDraftFolder=Drafts
```

1.276 officeLocation Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1123.1.1

1.277 officenumber Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1107.1.1
Definition	

Specifies the office number.

1.278 organizationUnitName Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	pabPerson
OID	2.16.840.1.113894.1009.1.101.0.1184.1.1
Definition	

Name of the organization unit to which the user belongs. This is a standard attribute. See RFC 4519.

1.279 otherCity Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1046.1.1
Definition	

Specifies the other city

1.280 otherCountry Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1031.1.1
Definition	

Specifies the other country

1.281 otherDate Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1001.1.1
Definition	

Specifies the other date

1.282 otherDateDescr Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1100.1.1
Definition	

Specifies the other date description

1.283 otherDomDelivery Attribute

Syntax	boolean (TRUE or FALSE), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1150.1.1

Definition

Specifies whether the contact's other address will be used as domestic delivery address

1.284 otherIntlDelivery Attribute

Syntax   boolean (TRUE or FALSE), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1151.1.1

Definition

Specifies whether the contact's other address will be used as international delivery address

1.285 otherParcelDelivery Attribute

Syntax   boolean (TRUE or FALSE), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1153.1.1

Definition

Specifies whether the contact's other address will be used as parcel delivery address

1.286 otherPOBox Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1152.1.1

Definition

Specifies the other PO Box

1.287 otherPostalAddress Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1047.1.1

Definition

Specifies the other postal address.

1.288 otherPostalCode Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1055.1.1

Definition

Specifies the other postal code

1.289 otherPostalDelivery Attribute

Syntax   boolean (TRUE or FALSE), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1154.1.1

Definition

Specifies whether the contact's other address will be used as postal delivery address

1.290 otherState Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1051.1.1

Definition

Specifies the other state

1.291 ou Attribute

OID   2.5.4.11

1.292 owner Attribute

Object Classes   inetManagedGroup nsManagedDomain

OID   2.5.4.32

Definition

This is a standard attribute, see RFC 4519.

Identifies the distinguished name (DN) of the person or group with administrative privileges over the entry. For any resource entry, it defines the owner of the resource.

If the group has Calendar service (is a Calendar group), the owner must be a Calendar user or group in the same domain as the entry. That is, Calendar service must be assigned to the owner as well as the Calendar group.

1.293 pabURI Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.107.1.1155.1.1

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
```

1.294 photoBinaryData Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1156.1.1

Definition

Specifies the image or photograph information that annotates some aspect of the contact in binary encoded format.

1.295 photoType Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1157.1.1

Definition

Specifies the image or photograph type of the contact associated with the attribute photoBinaryData.

1.296 photoURL Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1034.1.1
Definition	

Specifies the URL that points to a picture of this person.

1.297 piBackpointer Attribute

Syntax	IA5 string (ASCII)
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1039.1.1
Definition	

Specifies the LDAP URL that points to the directory entry containing information on this person.

1.298 piBookType Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypeBook
OID	2.16.840.1.113894.1009.1.107.1.1037.1.1
Definition	

Address Book supports three piBookTypes. These are: `abook`, `imbook`, or `pbook`.

1.299 piCertId Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypeCert
OID	2.16.840.1.113894.1009.1.107.1.1158.1.1

1.300 piCreator Attribute

Syntax	IA5 string (ASCII)
Object Classes	piLocalBook
OID	2.16.840.1.113894.1009.1.107.1.1052.1.1

Definition

Allows users to create entries in an address book.

1.301 piDefaultAB Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piPStoreRoot

OID   2.16.840.1.113894.1009.1.107.1.1073.1.1

Definition

Specifies the location of default address book or category in which all new entries in the address book are stored.

1.302 piDeleter Attribute

Syntax   IA5 string (ASCII)

Object Classes   piLocalBook

OID   2.16.840.1.113894.1009.1.107.1.1035.1.1

Definition

Allows users to delete entries in an address book.

1.303 piEmail1 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1103.1.1

Definition

Specifies the contact's primary Email address.

For a group contact, this attribute specifies the Email address of the group. If this is not specified, the message sent to a group are sent to all group members.

1.304 piEmail1CN Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1064.1.1

Definition

The display name for piEmail1.

1.305 piEmail1TransType Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1067.1.1
Definition	

The transport type for piEmail1.

1.306 piEmail1Type Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1060.1.1
Definition	

The "type" for piEmail1, e.g. "Work", "Personal", "Other".

1.307 piEmail2 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1105.1.1
Definition	

piEmail2 through piEmail3 are used to store other email addresses of the contact. The corresponding piEmail2Type and piEmail3Type attributes are used to determine the type of the email address.

1.308 piEmail2CN Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1065.1.1
Definition	

The display name for piEmail2.

1.309 piEmail2TransType Attribute

Syntax	IA5 string (ASCII), single-valued

Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1068.1.1

Definition

The transport type for piEmail1.

1.310 piEmail2Type Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1062.1.1

Definition

The "type" for piEmail2, e.g. "Work", "Personal", "Other".

1.311 piEmail3 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1106.1.1

Definition

piEmail2 through piEmail3 are used to store other email addresses of the contact. The corresponding piEmail2Type and piEmail3Type attributes are used to determine the type of the email address.

1.312 piEmail3CN Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1066.1.1

Definition

The display name for piEmail3.

1.313 piEmail3TransType Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1069.1.1

Definition

The transport type for piEmail1.

1.314 piEmail3Type Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1063.1.1

Definition

The "type" for piEmail3, e.g. "Work", "Personal", "Other".

1.315 piEntryID Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piEntry piTypeBook piTypeCert

OID   2.16.840.1.113894.1009.1.107.1.1109.1.1

Definition

Unique "d" used for entry. The 128 bit UID is generated by address book server and never displayed.

1.316 piIM1ID Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1026.1.1

Definition

Specifies the contact's primary IM identifier

1.317 piIM1Service Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1102.1.1

Definition

Specifies the type of IM service associated with the contact's IM identifier specified in the piIM1ID attribute.

1.318 piIM2ID Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1054.1.1

Definition

Specifies the contact's other IM identifier

1.319 piIM2Service Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1059.1.1

Definition

Specifies the type of IM service associated with the contact's specified by the IM identifier in the piIM2ID attribute.

1.320 piIM3ID Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1028.1.1

Definition

Specifies the contact's other IM identifier

1.321 piIM3Service Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1045.1.1

Definition

Specifies the type of IM service associated with the contact's specified by the IM identifier in the piIM3ID attribute.

1.322 piLastModifiedBy Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes	piEntry piTypeBook
OID	2.16.840.1.113894.1009.1.107.1.1097.1.1
Definition	

Stores the identifier of the user modifying this entry.

1.323 piMaxStoreEntries Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piPStoreRoot
OID	2.16.840.1.113894.1009.1.107.1.1036.1.1
Definition	

Specifies the maximum number of entries that can be created in the store.

1.324 pipEntryTextData Attribute

Syntax	IA5 string (ASCII)
Object Classes	piEntry
OID	2.16.840.1.113894.1009.1.107.1.1112.1.1
Definition	

Specifies the generic Text type data to keep extended attributes, which are typically free-floating <index1\>|<index2\>|<index3\>

1.325 pipEntryXMLData Attribute

Syntax	IA5 string (ASCII)
Object Classes	piEntry
OID	2.16.840.1.113894.1009.1.107.1.1075.1.1
Definition	

Specifies the XML data

1.326 piPhone1 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1005.1.1

Definition

Specifies the primary phone number for this user

1.327 piPhone10 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1014.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone10Type attribute is used to determine that what the number represents.

1.328 piPhone10Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1085.1.1

Definition

Specifies the type for piPhone10, e.g. "Work", "Home", "Mobile", etc.

1.329 piPhone11 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1015.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone11Type attribute is used to determine that what the number represents.

1.330 piPhone11Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1086.1.1

Definition

Specifies the type for piPhone11, e.g. "Work", "Home", "Mobile", etc.

1.331 piPhone12 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1016.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone12Type attribute is used to determine that what the number represents.

1.332 piPhone12Type Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1087.1.1

Definition

Specifies the type for piPhone12, e.g. "Work", "Home", "Mobile", etc.

1.333 piPhone13 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1017.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone13Type attribute is used to determine that what the number represents.

1.334 piPhone13Type Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1088.1.1

Definition

Specifies the type for piPhone13, e.g. "Work", "Home", "Mobile", etc.

1.335 piPhone14 Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1018.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone14Type attribute is used to determine that what the number represents.

1.336 piPhone14Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1089.1.1

Definition

Specifies the type for piPhone14, e.g. "Work", "Home", "Mobile", etc.

1.337 piPhone15 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1019.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone15Type attribute is used to determine that what the number represents.

1.338 piPhone15Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1090.1.1

Definition

Specifies the type for piPhone15, e.g. "Work", "Home", "Mobile", etc.

1.339 piPhone16 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1020.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone16Type attribute is used to determine that what the number represents.

1.340 piPhone16Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1091.1.1

Definition

Specifies the type for piPhone16, e.g. "Work", "Home", "Mobile", etc.

1.341 piPhone17 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1021.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone17Type attribute is used to determine that what the number represents.

1.342 piPhone17Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1092.1.1

Definition

Specifies the type for piPhone17, e.g. "Work", "Home", "Mobile", etc.

1.343 piPhone18 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1022.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone18Type attribute is used to determine that what the number represents.

1.344 piPhone18Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1093.1.1
Definition	

Specifies the type for piPhone18, e.g. "Work", "Home", "Mobile", etc.

1.345 piPhone19 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1023.1.1
Definition	

Stores the other phone numbers of the contact. The corresponding piPhone19Type attribute is used to determine that what the number represents.

1.346 piPhone19Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1094.1.1
Definition	

Specifies the type for piPhone19, e.g. "Work", "Home", "Mobile", etc.

1.347 piPhone1Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1076.1.1
Definition	

Specifies the type for piPhone1, e.g. "Work", "Home", "Mobile", etc.

1.348 piPhone2 Attribute

Syntax	directory string (UTF-8), single-valued

Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1006.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone2Type attribute is used to determine that what the number represents.

1.349 piPhone20 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1024.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone20Type attribute is used to determine that what the number represents.

1.350 piPhone20Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1095.1.1

Definition

Specifies the type for piPhone20, e.g. "Work", "Home", "Mobile", etc.

1.351 piPhone2Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1077.1.1

Definition

Specifies the type for piPhone2, e.g. "Work", "Home", "Mobile", etc.

1.352 piPhone3 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1007.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone3Type attribute is used to determine that what the number represents.

1.353 piPhone3Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1078.1.1
Definition	

Specifies the type for piPhone3, e.g. "Work", "Home", "Mobile", etc.

1.354 piPhone4 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1008.1.1
Definition	

Stores the other phone numbers of the contact. The corresponding piPhone4Type attribute is used to determine that what the number represents.

1.355 piPhone4Type Attribute

Origin	sun defined
Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1079.1.1
Definition	

Specifies the type for piPhone4, e.g. "Work", "Home", "Mobile", etc.

1.356 piPhone5 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1009.1.1
Definition	

Stores the other phone numbers of the contact. The corresponding piPhone5Type attribute is used to determine that what the number represents.

1.357 piPhone5Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1080.1.1

Definition

Specifies the type for piPhone5, e.g. "Work", "Home", "Mobile", etc.

1.358 piPhone6 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1010.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone6Type attribute is used to determine that what the number represents.

1.359 piPhone6Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1081.1.1

Definition

Specifies the type for piPhone6, e.g. "Work", "Home", "Mobile", etc.

1.360 piPhone7 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1011.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone7Type attribute is used to determine that what the number represents.

1.361 piPhone7Type Attribute

Syntax	directory string (UTF-8), single-valued

Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1082.1.1

Definition

Specifies the type for piPhone7, e.g. "Work", "Home", "Mobile", etc.

1.362 piPhone8 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1012.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone8Type attribute is used to determine that what the number represents.

1.363 piPhone8Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1083.1.1

Definition

Specifies the type for piPhone8, e.g. "Work", "Home", "Mobile", etc.

1.364 piPhone9 Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1013.1.1

Definition

Stores the other phone numbers of the contact. The corresponding piPhone9Type attribute is used to determine that what the number represents.

1.365 piPhone9Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1084.1.1

Definition

Specifies the type for piPhone9, e.g. "Work", "Home", "Mobile", etc.

1.366 pipProfileBinaryData Attribute

Syntax　　　　　binary

Object Classes　　piTypeProfile

OID　　　　　　2.16.840.1.113894.1009.1.107.1.1110.1.1

1.367 pipProfileTextData Attribute

Syntax　　　　　IA5 string (ASCII)

Object Classes　　piTypeProfile

OID　　　　　　2.16.840.1.113894.1009.1.107.1.1111.1.1

1.368 pipProfileXMLData Attribute

Syntax　　　　　IA5 string (ASCII)

Object Classes　　piTypeProfile

OID　　　　　　2.16.840.1.113894.1009.1.107.1.1074.1.1

1.369 piPStoreOwner Attribute

Syntax　　　　　IA5 string (ASCII), single-valued

Object Classes　　piPStoreRoot

OID　　　　　　2.16.840.1.113894.1009.1.107.1.1002.1.1

Definition

Specifies the address book owner's ID. It is assigned this UID from the user entry available in the Corporate Directory

1.370 piReader Attribute

Syntax　　　　　IA5 string (ASCII)

Object Classes　　piLocalBook

OID　　　　　　2.16.840.1.113894.1009.1.107.1.1040.1.1

Definition

Allows users to read entries in the address book. The owner of the address book store is implicitly granted read, write, modify and delete permissions.

1.371 piRemotePiURL Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piRemoteBook
OID	2.16.840.1.113894.1009.1.107.1.1029.1.1
Definition	

Specifies the LDAP URL for a remote address book. For each user, a piRemoteBook node is created for each remote book defined for the domain.

1.372 piWebsite1 Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1114.1.1
Definition	

Specifies the URL of the primary web-site associated with the person or group.

1.373 piWebsite1Descr Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1027.1.1
Definition	

Specifies the description associated with piWebsite1.

1.374 piWebsite1Type Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1138.1.1

1.375 piWebsite2 Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1116.1.1

Definition

Specifies the URL of the secondary web-site associated with the person.

1.376 piWebsite2Descr Attribute

Syntax   IA5 string (ASCII), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1043.1.1

Definition

Specifies the description associated with piWebsite2

1.377 piWebsite2Type Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1139.1.1

1.378 piWriter Attribute

Syntax   IA5 string (ASCII)

Object Classes   piLocalBook

OID   2.16.840.1.113894.1009.1.107.1.1108.1.1

Definition

Allows users to add or modify entries in an address book. The owner of the address book store is implicitly granted read, write, modify and delete permissions.

1.379 preferredCountry Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   inetMailUser inetMailGroup inetManagedGroup

OID   2.16.840.1.113894.1009.1.101.0.1027.1.1

1.380 preferredLanguage Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113730.3.1.39

Definition

This is a standard attribute, see RFC 2798.

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 Access Manager in user LDAP entries to store a user's preferred language. Note that only Access Manager uses the `iPlanetPreferences` object class to host this attribute.

Table 1.16 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
```

1.381 preferredLocale Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.107.1.1159.1.1

Definition

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

Example

```
preferredLocale:en-US
```

1.382 preferredMailHost Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   mailDomain sunMailOrganization inetDomain
sunManagedOrganization

OID   2.16.840.1.113894.1009.1.101.0.1185.1.1

Definition

If you are provisioning an LDAP Schema 2 directory with Communications Suite Delegated Administrator, use the following definition:

Sets the mail host name for new users in this business organization. When a user is created, the `mailHost` attribute of the user entry is filled by the value of `preferredMailHost`.

The `preferredMailHost` attribute is required when the business organization has a mail service.

If this is a full business organization, `preferredMailHost` is an attribute of the `mailDomain` object class. If this is a shared business organization, `preferredMailHost` is an attribute of the `sunMailOrganization` object class.

If you are provisioning an LDAP Schema 1 directory with iPlanet Delegated Administrator: See `preferredMailHost` for a definition of how to use this attribute with Schema 1.

Example

```
preferredMailHost: mail.siroe.com
```

1.383 preferredMailMessageStore Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1186.1.1

Definition

If you are provisioning an LDAP Schema 2 directory with Communications Suite Delegated Administrator, use the following definition:

Sets the message store partition name for new users in this business organization. When a user is created, the `mailMessageStore` attribute of the user entry is filled by the value of `preferredMailMessageStore`.

If the `preferredMailMessageStore` attribute is 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.

If this is a full business organization, `preferredMailMessageStore` is an attribute of the `mailDomain` object class. If this is a shared business organization, `preferredMailMessageStore` is an attribute of the `sunMailOrganization` object class.

If you are provisioning an LDAP Schema 1 directory with iPlanet Delegated Administrator: See `preferredMailMessageStore` for a definition of how to use this attribute with Schema 1.

Example

```
preferredMailMessageStore: primary
```

1.384 privacy Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1137.1.1

1.385 profession Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1127.1.1

Definition

Specifies the contact's profession

1.386 psIncludeInGAB Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	ipUser
OID	2.16.840.1.113894.1009.1.104.1.1032.1.1

Definition

Includes this user in the Global Address Book (GAB) and gives this user access to the Global Address Book.

Allowed values: `true`, `false`

Default value: `truex`

1.387 psRoot Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	ipUser
OID	2.16.840.1.113894.1009.1.107.1.1160.1.1

1.388 sortString Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1161.1.1

Definition

Specifies that the contact's family name or given name text to be used for national-language-specific sorting of the FN and N types.

1.389 spouse Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1122.1.1

Definition

Specifies the contact's spouse

1.390 suffix Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1125.1.1

Definition

Specifies suffixes such as Jr., Sr.

1.391 sunAbExtendedUserPrefs Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.106.1.1004.1.1

1.392 sunAllowBusinessOrgType Attribute

Syntax   IA5 string (ASCII)

Object Classes   sunManagedProvider

OID   2.16.840.1.113894.1009.1.104.1.1011.1.1

Definition

Defines the types of business organizations this provider administrator can create. This is a required attribute. Allowed values:

• shared - Designates a business organization that is assigned to a shared domain. Multiple business organizations can be part of a shared domain. The business organization being created shares its namespace with the other organizations in the domain.

- full - Designates a business organization that is a full-fledged domain with an authorized domain name and its own unique namespace.

The `sunAllowBusinessOrgType` attribute can enable the provider to create

- Only shared business organizations (`shared` value only)

- Only business organizations that are real, full-fledged domains (`full` value only)

- Both shared and full-fledged business organizations (`shared` and `full` values)

Example

```
sunAllowBusinessOrgType: shared
sunAllowBusinessOrgType: full
```

1.393 sunAllowMultipleDomains Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	sunManagedProvider
OID	2.16.840.1.113894.1009.1.104.1.1013.1.1

Definition

Determines whether this provider organization can create business organizations that permit multiple domain names or a single domain name for their users.

The `sunAllowMultipleDomains` attribute applies only to business organizations created in shared domains. If a business organization is created as a domain with its own namespace, it can always have multiple domain names specified with the `associatedDomain` attribute.

If the `sunAllowMultipleDomains` attribute is not present, the LDAP semantics allow multiple domain names for the users of the business organizations. (The default value is true.)

Allowed values: `true`, `false`

Example

```
sunAllowMultipleDomains: true
```

1.394 sunAllowOutsideAdmins Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	sunAllowOutsideAdmins
OID	2.16.840.1.113894.1009.1.104.1.1015.1.1

1.395 sunAssignableDomains Attribute

Syntax	IA5 string (ASCII)

Object Classes	sunAllowOutsideAdmins
OID	2.16.840.1.113894.1009.1.104.1.1016.1.1

Definition

Specifies a list of domain names the provider administrator can choose from when assigning domains to business organizations in this provider organization. This list is derived from the domain names specified in the `sunPreferredDomain` and `associatedDomain` attributes of the parent or ancestor shared domain node.

If the sunAssignableDomains attribute is not present, all of the `sunPreferredDomain` and `associatedDomain` attributes are available to be assigned to business organizations by this provider.

Example

```
sunAssignableDomains: sesta.com
sunAssignableDomains: siroe.com
sunAssignableDomains: varius.com
```

1.396 sunAvailableDomainNames Attribute

Syntax	IA5 string (ASCII)
OID	2.16.840.1.113894.1009.1.104.1.1007.1.2

Definition

Specifies a list of domain names available for use by the business organization. This list is a subset of domain names derived from the sunAssignableDomains attribute in the provider organization.

If the sunAvailableDomainNames attribute is not present, all domains from the sunAssignableDomains attribute in the provider organization are available for use by this business organization.

Example

```
sunAvailableDomainNames: sesta.com
sunAvailableDomainNames: siroe.com
```

1.397 sunAvailableServices Attribute

Syntax	IA5 string (ASCII)
OID	2.16.840.1.113894.1009.1.104.1.1001.1.1

Definition

Specifies a list of Service Packages available to the business organization for its users and groups. Also specifies the number of instances of each named class-of-service. This is a required attribute.

The value of the attribute has two possible formats: Limited Allocation or Unlimited

The format for Limited Allocation is `servicename:number:number_assigned` where

- `number` is the number of service packages allocated to the organization

- `number_assigned` is the number of service packages assigned to users or groups in the organization. If no service packages have been assigned, the value of `number_assigned` is -1.

The Unlimited format is `servicename`

If you specify servicename only--if you do not specify the number of services allocated and assigned--an unlimited number of that service is available to the business organization.

Example

```
sunAvailableServices:Gold:10:--1
sunAvailableServices:Mercury:20:5
sunAvailableServices:Silver
```

In this example, 10 Gold services are available to the organization, 0 have been assigned. 20 Mercury services are available to the organization, 5 have been assigned. An unlimited number of Silver services are available to the organization.

1.398 sunBusinessOrgBase Attribute

Syntax	distinguished name (DN)
Object Classes	sunAllowOutsideAdmins
OID	2.16.840.1.113894.1009.1.104.1.1017.1.1

Definition

Contains the DN for the node underneath which all full domains for this provider organization are to be created.

You can assign this attribute only if the `sunAllowBusinessOrgType` attribute was provisioned to allow full domains (`sunAllowBusinessOrgType: full`).

Example

```
sunBusinessOrgBase: o=providerorgDomainsRoot,o=Business,o=userGroupRoot
```

1.399 sunBusinessRoot Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	sunManagedLocation
OID	2.16.840.1.113894.1009.1.104.1.1018.1.1

Definition

Holds the DN of the root entry that contains the business organization tree.

Example

```
sunBusinessRoot: o=Business,o=userGroupRoot
```

1.400 sunConfRoomCapacity Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypeABConferenceRoom

OID   2.16.840.1.113894.1009.1.107.1.1053.1.1

Definition

Specifies the number that represents the maximum occupants of who could be in the room.

1.401 sunEnableGAB Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1002.1.1

Definition

Enables use of a global address book for this business organization.

Allowed values: `true`, `false`

Default value: `false`

Example

```
sunEnableGAB: true
```

1.402 sunExcludeServices Attribute

Syntax   IA5 string (ASCII)

Object Classes   sunManagedProvider

OID   2.16.840.1.113894.1009.1.104.1.1019.1.1

Definition

Specifies a list of classes-of-service that will be excluded from the business organizations in this provider organization.

If both the `sunIncludeServices` and `sunExcludeServices` attributes are specified, only `sunIncludeServices` takes effect. If neither attribute is present, all classes-of-service

found underneath the container specified with the `sunServicesRoot` attribute will also be available to the business organizations in this provider organization.

Example

```
sunExcludeServices: Bronze
```

1.403 sunIMConferenceAffiliations Attribute

Syntax directory string (UTF-8)

Object Classes sunIMConference

OID 2.16.840.1.113894.1009.1.103.0.1001.1.1

Definition

TBD

1.404 sunIMConferenceConfiguration Attribute

Syntax directory string (UTF-8)

Object Classes sunIMConference

OID 2.16.840.1.113894.1009.1.103.0.1002.1.1

Definition

TBD

1.405 sunIMMessageContent Attribute

Syntax directory string (UTF-8)

Object Classes sunIMStoredMessage

OID 2.16.840.1.113894.1009.1.103.0.1003.1.1

Definition

Specifies the XMPP message content.

1.406 sunIMMessageID Attribute

Syntax directory string (UTF-8)

Object Classes sunIMStoredMessage

OID 2.16.840.1.113894.1009.1.103.0.1004.1.1

Definition

Specifies the XMPP message ID.

1.407 sunIMPrivateSettings Attribute

Syntax   directory string (UTF-8)

Object Classes   sunIMUser

OID   2.16.840.1.113894.1009.1.103.0.1005.1.1

Definition

TBD

1.408 sunIMProperties Attribute

Origin   Sun Microsystems

Syntax   directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.769

1.409 sunIMRoster Attribute

Syntax   directory string (UTF-8)

Object Classes   sunIMUser

OID   2.16.840.1.113894.1009.1.103.0.1006.1.1

Definition

TBD

1.410 sunIMUserPrivateSettings Attribute

Syntax   directory string (UTF-8)

Object Classes   sunIMUser

OID   2.16.840.1.113894.1009.1.103.0.1007.1.1

Definition

Reserved. Not implemented.

1.411 sunIMUserProperties Attribute

Origin   Sun Microsystems

Syntax   directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.764

1.412 sunIMUserRoster Attribute

Syntax   directory string (UTF-8)

Object Classes   sunIMUser

OID   2.16.840.1.113894.1009.1.103.0.1008.1.1

Definition

Reserved. Not implemented.

1.413 sunIncludeServices Attribute

Syntax   IA5 string (ASCII)

Object Classes   sunManagedProvider

OID   2.16.840.1.113894.1009.1.104.1.1012.1.1

Definition

Specifies a list of the classes-of-service available to business organizations in this provider organization.

The complete list of classes-of-service available in this directory is found underneath the container specified with the `sunServicesRoot` attribute.

If the `sunIncludeServices` attribute is not present, all classes-of-service specified underneath the class-of-service container will also be available to the business organizations in this provider organization.

Example

```
sunIncludeServices: Gold
```

1.414 sunkeyvalue Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.100.0.1013.1.1

Definition

Each value is a "key=value" pair. It is used under the well-knonw DN o=comms-config to store configuration values for dssetup.

In search templates, the key is the name of the XML element. The table below lists the keys for search templates.

Table 1.17 Search Template Keys

Key	Description

attrs	Attribute to retrieve from LDAP entry
rfc2247Flag	Boolean (`true`, `false`) that tells applications to use the RFC 2247 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 Communications Suite Schema Reference Overview.

Example

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

```
sunKeyValue:attrs=objectclasssunKeyValue:
    attrs=ousunKeyValue: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=objectclasssunKeyValue:
    attrs=ousunKeyValue:attrs=inetDomainStatussunKeyValue:
    rfc2247=truesunKeyValue: basedn=o=internet
```

1.415 sunMaxGroups Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1009.1.1

Definition

Specifies the maximum number of groups that can be created in this business organization.

To enable the business organization to contain an unlimited number of groups, specify a value of -1. Allowed values are integers.

Example

```
sunMaxGroups: 20
```

1.416 sunMaxUsers Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1005.1.1

Definition

Specifies the maximum number of users who can be created in this business organization.

To enable the business organization to contain an unlimited number of users, specify a value of -1. Allowed values are integers.

Example

```
sunMaxUsers: 50
```

1.417 sunNameSpaceUniqueAttrs Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.105.0.1001.1.1

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 object class description for `sunNameSpace`.

Example

```
sunNameSpaceUniqueAttrs:uid
sunNameSpaceUniqueAttrs:c
```

1.418 sunNumGroups Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1003.1.1

Definition

Specifies the current number of groups in this business organization. Allowed values are integers.

Example

```
sunNumGroups: 8
```

1.419 sunNumUsers Attribute

Syntax   IA5 string (ASCII), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1004.1.1

Definition

Specifies the current number of users in this business organization. Allowed values are integers. NOTE: This number is maintained by Delegated Administrator. Manual changes to the number of users (using ldapmodify) will not be reflected in the count.

Example

```
sunNumUsers: 12
```

1.420 sunOrganizationAlias Attribute

Syntax	directory string (UTF-8)
Object Classes	sunOrganizationAlias
OID	2.16.840.1.113894.1009.1.104.1.1033.1.1

Definition

Access Manager 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
```

1.421 sunOrgType Attribute

Syntax	IA5 string (ASCII), single-valued
OID	2.16.840.1.113894.1009.1.104.1.1006.1.1

Definition

Determines whether this business organization is part of a shared domain (shared) or is a full-fledged domain with its own namespace (full).

This is a required attribute. Allowed values:

- `shared` --- Designates a business organization that is assigned to a shared domain. Multiple business organizations can be part of a shared domain. This business organization shares its namespace with the other organizations in the domain.

- `full` --- Designates a business organization that is a full-fledged domain with an authorized domain name and its own unique namespace.

Example

```
sunOrgType: shared
```

```
sunorgtype: full
```

1.422 sunpluginschema Attribute

Syntax directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.104.1.1034.1.1

1.423 sunPreferredDomain Attribute

Syntax directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.105.0.1002.1.1

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 Schema 2 native mode LDAP directories only; it must not be used in DC Tree nodes.

Example

```
sunPreferredDomain:sesta.com
```

1.424 sunPresenceAccessDenied Attribute

Origin Sun Microsystems

Syntax directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.760

1.425 sunPresenceAccessPermitted Attribute

Origin Sun Microsystems

Syntax directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.761

1.426 sunPresenceDefaultAccess Attribute

Origin Sun Microsystems

Syntax   directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.759

1.427 sunPresenceEntityAccessDenied Attribute

Origin   Sun Microsystems

Syntax   directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.755

1.428 sunPresenceEntityAccessPermitted Attribute

Origin   Sun Microsystems

Syntax   directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.756

1.429 sunPresenceEntityDefaultAccess Attribute

Origin   Sun Microsystems

Syntax   directory string (UTF-8)

OID   1.3.6.1.4.1.42.2.27.9.1.754

1.430 sunPresencePrivacy Attribute

Syntax   directory string (UTF-8)

Object Classes   sunPresenceUser

OID   2.16.840.1.113894.1009.1.103.0.1009.1.1

Definition

TBD

1.431 sunPresenceUserPrivacy Attribute

Syntax   directory string (UTF-8)

Object Classes   sunPresenceUser

OID	2.16.840.1.113894.1009.1.103.0.1010.1.1

Definition

Specifies XMPP privacy profiles.

1.432 sunProviderOrgDN Attribute

Syntax	IA5 string (ASCII), single-valued
Object Classes	sunManagedProvider
OID	2.16.840.1.113894.1009.1.104.1.1014.1.1

Definition

Contains the base DN that points to the business organization for this provider organization. The users of this provider organization are created in this business organization.

The provider organization cannot have any user entries directly under the provider organization node. All users in the provider organization must be managed in the separate business organization identified by the sunProviderOrgDN attribute. This business organization is like any other business organization.

Example

```
sunProviderOrgDN: o=providerorg,o=sesta.com,o=sharedDomainsRoot,o=Business
```

1.433 sunRegisteredServiceName iplanet-am-service-status Attribute

Syntax	directory string (UTF-8)
Object Classes	sunManagedOrganization
OID	2.16.840.1.113894.1009.1.104.1.1028.1.1

Definition

Defines the set of names of the registered services. The following services are defined for Messaging Server and Calendar Server:

Table 1.18 Registered Service Names

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 Access Manager for authentication with SSO (Single Sign-On). These services must be registered to the root suffix node. This step is done by Access Manager 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 Access Manager. For information on how to do this, see the Access Manager documentation at: http://docs.sun.com

Example

```
sunRegisterdServiceName: DomainMailService
```

1.434 sunserviceid Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1035.1.1

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
```

1.435 sunserviceschema Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.104.1.1036.1.1

1.436 sunsmspriority Attribute

Syntax   signed integer, single-valued

OID   2.16.840.1.113894.1009.1.104.1.1037.1.1

Definition

Stores the priority of the service with respect to its siblings.

Example

```
sunSmsPriority:
```

1.437 sunUCColorScheme Attribute

Syntax　　directory string (UTF-8), single-valued

OID　　2.16.840.1.113894.1009.1.106.1.1005.1.1

1.438 sunUCDateDelimiter Attribute

Syntax　　directory string (UTF-8), single-valued

OID　　2.16.840.1.113894.1009.1.106.1.1006.1.1

Definition

Delimiter is the character that separates date, month and year in the date. The options available are: ".", "/", "-".

1.439 sunUCDateFormat Attribute

Syntax　　directory string (UTF-8), single-valued

OID　　2.16.840.1.113894.1009.1.106.1.1007.1.1

Definition

Specifies date display and input format. Valid formats are: Y/M/D, M/D/Y and D/M/Y.

1.440 sunUCDefaultApplication Attribute

Syntax　　directory string (UTF-8), single-valued

OID　　2.16.840.1.113894.1009.1.106.1.1008.1.1

Definition

Specifies the default tab that appears to the user upon login to Convergence. A value of mail indicates that Convergence opens to the inbox. A value of calendar indicates that Convergence opens to the calendar.

1.441 sunUCDefaultEmailHandler Attribute

Syntax　　directory string (UTF-8), single-valued

OID　　2.16.840.1.113894.1009.1.106.1.1009.1.1

Definition

Specifies the default mail handler for all mail links. The valid values are as follows:

- `uc` - If the value is `uc`, Communication Express' mail compose feature is used to compose a new message.

- `desktop` - If the value is `desktop`, the default `mailto:` handler as specified by the desktop operating system is used to compose a new message.

1.442 sunUCExtendedClientPrefs Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.106.1.1010.1.1

Definition

Defines Convergence client-specific options for a domain. It also defines the default values of user options for users within the domain.

The `sunUCExtendedClientPrefs` attribute stores client preferences for a domain at the domain level; its corresponding attribute for individual users is `sunUCExtendedUserPrefs`. Options for an individual user can be extended by using the `sunUCExtendedUserPrefs` attribute in the individual user's LDAP entry.

The following table lists the properties available with `sunUCExtendedClientPrefs`, their definitions, and their values.

Table 1.19 Extended Client Preferences

Property	Value	Description
ClientCustomizationEnabled	true, false (boolean)	Enables or disables customization for the end user
MailCheckInterval	integer	Specifies the interval, in seconds, that Convergence waits before checking for incoming mail.
MailAutoSaveInterval	integer	Specifies the interval, in seconds, that Convergence automatically saves the end user's current draft of a message.
MailDefaultTags	string	Specifies the default tags available to end users in the domain.
DictLocale	string	Defines the default language to be presented to end users in the domain.
AntiSpamServiceURL	string	Identifies the url location of the anti-spam service used for the domain.
AutoLogoutTimeout	integer	Specifies the idle time, in minutes, before the end user's current session times out (for all users in the domain).
SmartTimeZones	string	Specifies the smart time zones available to end users in the domain.
MainPage	string	Specifies the configured main page in the Convergence UI. For example

		sunUCExtendedClientPrefs: `mainpage=/iwc_static/layout/` `my-mainpage.html`. If this attribute is not configured, then the default main page is loaded, as configured by the `client.mainpage` Convergence configuration option.

Example

```
sunUCExtendedClientPrefs:ClientCustomizationEnabled=false
sunUCExtendedClientPrefs:MailCheckInterval=300
sunUCExtendedClientPrefs:MailAutoSaveInterval=60
sunUCExtendedClientPrefs:MailDefaultTags=work,personal
sunUCExtendedClientPrefs:DictLocale=en_US
sunUCExtendedClientPrefs:AntiSpamServiceURL=some_antispam_url
sunUCExtendedClientPrefs:AutoLogoutTimeout=15
sunUCExtendedClientPrefs:SmartTimeZones=APAC
```

1.443 sunUCExtendedUserPrefs Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.106.1.1011.1.1

Definition

Defines end user preferences in the Convergence UI. The user chooses preferences by specifying options in the User Options tab. Used to extend stored client preferences.

The `sunUCInitialized` sub-attribute is a set of attribute=value pairs that can be set for `sunUCExtendedUserPrefs`. The `sunUCInitialized` sub-attribute specifies whether the user has previously logged into Communications Express. When a user logs in for the first time, this value is set to true. If this entry is absent in LDAP, the value is set to false.

Table 1.20 Extended User Preferences

Property	Value	Description
ClientCustomizationEnabled	true, false (boolean)	Enables or disables customization for the end user.
smartTZenabled	true, false (boolean)	Allows the end user to enable or disable the smart Time zone feature for the client.
theme	string	Specifies a standard theme (such as "classic") or a customized theme. The theme determines the UI look and feel---the icons, colors, banners, fonts used in the UI. The administrator can create customized UI themes and make them available to end users. End users can choose from a selection of site-defined themes. User choices persist across sessions.

keyboardShortCutEnabled	true, false (boolean)	Allows the end user to enable or disable keyboard shortcuts.
defaultDictionary	string. For example: en, fr	Specifies the language of the default dictionary.
homePage	string. For example: classic	Allows the end user to define a customized start page---that is, a customized display of the UI when the client is launched. For example, the start page may display unread email messages; appointments for the day; overview of the week; unfinished tasks; online chat buddies; related RSS/atom feeds, as well as other UI components.
panelSize		Specifies a custom panel size defined by the end user. The user can resize panels by dragging the mouse; in User Options, the user can specify that the custom size become the default. The custom size persists across user sessions.

Example

```
sunUCExtendedUserPrefs: smarttzenabled=true
sunUCExtendedUserPrefs: keyboardShortCutEnabled=true
sunUCExtendedUserPrefs: defaultDictionary=en
sunUCExtendedUserPrefs: theme=classic
```

1.444 sunUCExternalMailProfile Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.106.1.1012.1.1

1.445 sunUCMailSendProfiles Attribute

Syntax   directory string (UTF-8)

OID   2.16.840.1.113894.1009.1.106.1.1013.1.1

Definition

Defines alternate sender identities created or modified by a user of Convergence. A sender identity allows the user to specify settings (attributes) when sending a new message, or replying to or forwarding an existing message. All attributes of the sender identity (email address, signature, vCard, and so on) are applied to the outgoing message.

The user can specify these attributes in the Convergence UI. The user can specify multiple alternate sender identities. They are stored in multiple instances of sunUCMailSenderProfile. Each instance of sunUCMailSenderProfile is a set of attribute=value pairs separated by semicolons.

A sender identity consists of the following attributes:

- User name (the comment part of the RFC 822 address)

- Email address

- Reply-to address (optional): Set a valid RFC 2822 email address to be used in the 'reply-to' header of the message.

- Add Signature: A boolean option to enable the use of a signature.

- Signature: Text (plain text or HTML using the rich text editor) appended to the bottom of all messages sent by the user.

- Add vCard: A boolean option that adds the vCard as an attachment to all messages sent by the user.

- vCard: Various fields of vCard can be set by the user. The fields include: first name, last name, email address, and so on.

- Default: A boolean option that identifies this sender identity as the default identity.

Example

```
sunUCMailSendProfiles:username=user1;email=emai1;reply--to=;
addsign=true;signature=signature1;addvcard=true;vcard=vcard1,default=tr
sunUCMailSendProfiles:username=user2;email=emai2;reply--to=replyadd2;
addsign=false;signature=;addvcard=true;vcard=vcard2,default=false
sunUCMailSendProfiles:username=user1;email=emai3;reply--to=replytoadd3;
addsign=false;signature=;addvcard=false;vcard=,default=false
```

1.446 sunUCTheme Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.106.1.1014.1.1

Definition

Specifies the name of user interface theme used to display all localizable resources. The list of resources include text labels, icons, color schemes, and so on. Communications Express 6.0 supports only domain-wide themes and not user-specific themes.

1.447 sunUCTimeFormat Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.106.1.1015.1.1

Definition

Specifies the time display format. Valid formats are: 12 hour clock, 24 hour clock

1.448 sunUCTimeZone Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.106.1.1016.1.1

Definition

Specifies the time zone used to normalize all time/date information in the client.

In Delegated Administrator 6.4 (Communications Suite 6), new users with calendar service are created with `sunUCTimeZone` having the same value of `icsTimezone`.

1.449 sunxmlkeyvalue Attribute

Syntax   IA5 string (ASCII)

OID   2.16.840.1.113894.1009.1.104.1.1038.1.1

1.450 tz Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1162.1.1

Definition

Specifies the contact's time zone

1.451 uid Attribute

Syntax   directory string (UTF-8)

Object Classes   inetOrgPerson

OID   0.9.2342.19200300.100.1.1

Definition

This is a standard attribute, see RFC 4519

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.

1.452 un Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1187.1.1

Definition

This is a standard attribute, see RFC XXX?.

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).

1.453 uniquemember Attribute

Syntax   name and optional UID

OID   2.5.4.50

Definition

This is a standard attribute, see RFC 4519.

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

Contrary to what its name seems to imply, the uniqueMember is not restricted to specifying the DN of an individual user object, although that is a valid and perhaps normal usage. The uniqueMember attribute can specify the DN of a container and thereby include an entire subtree. For this reason, each object specified by a uniqueMember attribute is looked up again. See the GROUP_DN_TEMPLATE MTA option and the discussion of uniqueMember in Group Expansion Attributes.

1.454 userPassword Attribute

Syntax   1.3.6.1.4.1.1466.115.121.1.40, single-valued

OID   2.5.4.35

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.

1.455 vacationEndDate Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1188.1.1

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.

The webmail interfaces set the value to "the last minute of this day, in the local time zone". For Messaging Express and Convergence, the local timezone is the timezone of the browser (OS). For Communications Express, the time zone is the sunuctimezone (set in the Options > Global > Time Zone UI).

When the current date falls outside the range of dates specified by the attributes `vacationStartDate` and `vacationEndDate`, then any delivery options (in the `delivery_option` MTA option 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.

This value is only used with "`mailAutoReplyMode: reply`".

1.456 vacationStartDate Attribute

Syntax   directory string (UTF-8), single-valued

OID   2.16.840.1.113894.1009.1.101.0.1189.1.1

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.

The webmail interfaces set the value to "midnight of this day, in the local time zone". For Messaging Express and Convergence, the local timezone is the timezone of the browser (OS). For Communications Express, the time zone is the sunuctimezone (set in the Options > Global > Time Zone UI).

This value is only used with "mailAutoReplyMode: reply"

1.457 workCity Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1071.1.1

Definition

Specifies the contact's work city.

1.458 workCountry Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1032.1.1

Definition

Specifies the country of work

1.459 workDomDelivery Attribute

Syntax	boolean (TRUE or FALSE), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1163.1.1
Definition	

Specifies whether the contact's work address will be used as domestic delivery address

1.460 workIntlDelivery Attribute

Syntax	boolean (TRUE or FALSE), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1164.1.1
Definition	

Specifies whether the contact's work address will be used as international delivery address

1.461 workParcelDelivery Attribute

Syntax	boolean (TRUE or FALSE), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1166.1.1
Definition	

Specifies whether the contact's work address will be used as parcel delivery address

1.462 workPOBox Attribute

Syntax	directory string (UTF-8), single-valued
Object Classes	piTypePerson
OID	2.16.840.1.113894.1009.1.107.1.1165.1.1
Definition	

Specifies the PO BOX.

1.463 workPostalAddress Attribute

Syntax	directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1113.1.1

Definition

Specifies the contact's work postal address

1.464 workPostalCode Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1044.1.1

Definition

Specifies the postal code of the contact's workplace

1.465 workPostalDelivery Attribute

Syntax   boolean (TRUE or FALSE), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1167.1.1

Definition

Specifies whether the contact's work address will be used as postal delivery address

1.466 workState Attribute

Syntax   directory string (UTF-8), single-valued

Object Classes   piTypePerson

OID   2.16.840.1.113894.1009.1.107.1.1004.1.1

Definition

Specifies the contact's work state.

Chapter 2 LDAP Object Classes

2.1 davEntity Object Class

Object class type	auxiliary
Allowed attributes	mail davStore davUniqueId
OID	2.16.840.1.113894.1009.1.102.1.1010.2.1
Definition	

Common DAV object

2.2 domain Object Class

Object class type	structural
Superior class	top
Required attributes	dc
Allowed attributes	userPassword searchGuide seeAlso businessCategory x121Address registeredAddress destinationIndicator

> preferredDeliveryMethod telexNumber teletexTerminalIdentifier
> telephoneNumber internationaliSDNNumber
> facsimileTelephoneNumber street postOfficeBox postalCode
> postalAddress physicalDeliveryOfficeName st l description o
> associatedName

OID   0.9.2342.19200300.100.4.13

Definition

Object class used to define entries that represent DNS domains. This class can only be used
with an entry that does 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.

2.3 icsAdministrator Object Class

Object class type   structural

Allowed attributes   icsAdminRole icsExtended icsExtendedGroupPrefs

OID   2.16.840.1.113730.3.2.145

Definition

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

2.4 icsCalendarDomain Object Class

Object class type   auxiliary

Allowed attributes   icsDomainNames icsStatus icsDomainAcl icsTimezone

OID   2.16.840.1.113894.1009.1.102.1.1002.2.1

Definition

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

2.5 icsCalendarDWPHost Object Class

Object class type   structural

Allowed attributes   cn description icsDWPHost icsRegularExpressions icsExtended
                           icsDomainNames icsStatus

OID   1.3.6.1.4.1.42.2.27.9.2.1

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.

2.6 icsCalendarGroup Object Class

Object class type	auxiliary
Superior class	top
Required attributes	groupid
Allowed attributes	icsStatus icsTimezone icsDoublebooking icsAutoaccept mail icsSecondaryowners icsCalendar icsDWPHost
OID	2.16.840.1.113894.1009.1.102.1.1003.2.1
Definition	

Specifies a calendar group; that is, a calendar created for, and used by, a group. Must be used in conjunction with `groupOfUniqueNames` or `groupOfURLs`.

2.7 icsCalendarResource Object Class

Object class type	auxiliary
Allowed attributes	cn mail mailalternateaddress icsStatus uid description owner icsDoublebooking icsAutoaccept icsTimezone icsSecondaryowners icsCalendar icsDWPHost
OID	2.16.840.1.113894.1009.1.102.1.1004.2.1
Definition	

Specifies a calendar resource, such as a conference room or piece of equipment that must be scheduled.

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

2.8 icsCalendarUser Object Class

Object class type	auxiliary
Allowed attributes	cn givenName mail mailalternateaddress preferredLanguage sn uid userPassword icsExtendedUserPrefs icsFirstDay icsStatus icsTimezone icsCalendar icsDWPHost
OID	2.16.840.1.113894.1009.1.102.1.1005.2.1
Definition	

Specifies a calendar user, including the DWP host name.

2.9 inetAdmin Object Class

Object class type	auxiliary

Superior class	top
Required attributes	objectclass
Allowed attributes	aci memberof
OID	2.16.840.1.113894.1009.1.104.1.1009.2.1

Definition

Identifies administrator user or group.

2.10 inetDomain Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	inetDomainBaseDN inetDomainStatus mailDomainUplevel mailDomainSourceConversionTag mailDomainOptin1 mailDomainOptin2 mailDomainOptin3 mailDomainOptin4 mailDomainOptin5 mailDomainOptin6 mailDomainOptin7 mailDomainOptin8 mailDomainNosolicit mailDomainAutoReplyTimeOut preferredMailHost mailDomainCatchallMapping mailDomainSourceMsgMaxBlocks mailDomainSourceChannel mailDomainMaxMsgRecipients mailDomainMaxMsgRecipientCutoff mailDomainDetourHostOptin mailDomainPrefixText mailDomainSuffixText mailDomainSenderSieve mailDomainCaptureAddress
OID	2.16.840.1.113894.1009.1.101.0.1008.2.1

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` or `icsCalendarDomain`, (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. `inetDomain` is a Schema 1 only object class. In Schema 2, the `sunManagedOrganization` object class is used to create a domain.

Access Manager uses this as a marker class for domains in the DC Tree.

2.11 inetDomainAlias Object Class

Object class type	structural
Superior class	alias
Required attributes	dc
OID	2.16.840.1.113894.1009.1.101.0.1009.2.1

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.

2.12 inetDomainAuthInfo Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	inetDomainSearchFilter domainUidSeparator inetCanonicalDomainName externalAuthPreUrlTemplate externalAuthPostUrlTemplate
OID	2.16.840.1.113894.1009.1.104.1.1002.2.1
Definition	

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

2.13 inetGroup Object Class

Object class type	auxiliary
Allowed attributes	inetgroupstatus
OID	2.16.840.1.113894.1009.1.104.1.1011.2.1
Definition	

Object class to be added to a group entity to give the group a status attribute, which can be `active`, `inactive`, or `deleted`.

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

Table 2.1 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`.

2.14 inetLocalMailRecipient Object Class

Object class type   auxiliary

Superior class   top

Allowed attributes   mail mailAlternateAddress mailHost mailRoutingAddress

OID   2.16.840.1.113894.1009.1.101.0.1010.2.1

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.

2.15 inetMailAdministrator Object Class

Object class type   auxiliary

Superior class   top

Allowed attributes   mailAdminRole

OID   2.16.840.1.113894.1009.1.101.0.1011.2.1

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.

2.16 inetMailGroup Object Class

Object class type   auxiliary

Superior class	top
Allowed attributes	mgrpErrorsTo mgrpAddHeader mgrpRemoveHeader mgrpModerator mgrpAuthPassword mgrpAllowedDomain mgrpDisallowedDomain mgrpAllowedBroadcaster mgrpDisallowedBroadcaster inetMailGroupStatus mailDeliveryFileURL mailDeliveryOption mailProgramDeliveryInfo mgrpRFC822MailMember mgrpDeliverTo mgrpBroadcasterPolicy mgrpMsgMaxSize mgrpMsgRejectAction mgrpMsgRejectText preferredLanguage dataSource mailEquivalentAddress mailMsgMaxBlocks mailConversionTag mailDeferProcessing mgrpMsgPrefixText mgrpMsgSuffixText mailSieveRuleSource groupid mgrpUniqueId cn mgrpDescription mgrpDelayNotifications mgrpDigestInterval mgrpMaxMessagesPerDay mgrpAdvertised mgrpPublicRoster mgrpSubscribePolicy mgrpUnsubscribePolicy mgrpJettisonBroadcasters mgrpJettisonDomain mgrpTrustNewMembers mail mgrpListTag mailSieveCollection mailMaxMsgRecipients mailMaxMsgRecipientCutoff mailSendMaxMsgBlocks mailSourceChannel mailOptin1 mailOptin2 mailOptin3 mailOptin4 mailOptin5 mailOptin6 mailOptin7 mailOptin8 mailSourceOptin1 mailSourceOptin2 mailSourceOptin3 mailSourceOptin4 mailSourceOptin5 mailSourceOptin6 mailSourceOptin7 mailSourceOptin8 mailDetourHostOptin mailApplyHOHControls mailHeadOfHouseholdDN mgrpURLResultMapping mgrpCheckHeader preferredCountry mailNosolicit mailSourceConversionTag mailAutoReplyAddresses mailAutoReplyMode mailAutoReplySubject mailAutoReplyText mailAutoReplyTextInternal mailAutoReplyTimeout mailSenderSieve mailCaptureAddress
OID	2.16.840.1.113894.1009.1.101.0.1002.2.3
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).

2.17 inetMailGroupManagement Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	mgmanAllowSubscribe mgmanDenySubscribe mgmanHidden mgmanJoinability mgmanVisibility mgmanMemberVisibility mgmanIntroText mgmanGoodbyeText multiLineDescription
OID	2.16.840.1.113894.1009.1.101.0.1012.2.1
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.

2.18 inetMailingListSubscription Object Class

Object class type   auxiliary

Superior class   top

Required attributes   mlsubListIdentifier mlsubRole

Allowed attributes   mlsubMail mlsubDigest mlsubReceiveMail
                               mlsubSuppressDuplicates mlsubJoinDate mlsubJoinIPAddress
                               mlsubTentativeEmail mlsubTrack mlsubActionKey

OID   2.16.840.1.113894.1009.1.101.0.1013.2.1

2.19 inetMailingListUser Object Class

Object class type   auxiliary

Superior class   top

Required attributes   mail mluserUniqueId

Allowed attributes   mluserPassword cn mluserJoinDate mluserJoinIPAddress

OID   2.16.840.1.113894.1009.1.101.0.1014.2.1

2.20 inetMailUser Object Class

Object class type   auxiliary

Superior class   top

Allowed attributes   mailAutoReplyTimeout mailAutoReplySubject mailAutoReplyText
                               mailAutoReplyTextInternal mailAutoReplyMode
                               mailDeliveryOption mailForwardingAddress mailMessageStore
                               mailProgramDeliveryInfo mailQuota mailMsgQuota
                               mailSieveRuleSource mailSMTPSubmitChannel
                               nswmExtendedUserPrefs mailAllowedServiceAccess
                               mailUserStatus cn dataSource mailEquivalentAddress
                               mailMsgMaxBlocks mailConversionTag mailDeferProcessing
                               mailAntiUBEService mailSieveCollection mailParentalControl
                               mailEventNotificationDestination mailSieveRuleRef
                               mailFolderDefaultAcl aclGroupAddr mailMaxMsgRecipients
                               mailMaxMsgRecipientCutoff mailSendMaxMsgBlocks
                               mailSourceChannel mailOptin1 mailOptin2 mailOptin3 mailOptin4
                               mailOptin5 mailOptin6 mailOptin7 mailOptin8 mailSourceOptin1
                               mailSourceOptin2 mailSourceOptin3 mailSourceOptin4

mailSourceOptin5 mailSourceOptin6 mailSourceOptin7
mailSourceOptin8 mailDetourHostOptin mailApplyHOHControls
mailHeadOfHouseholdDN preferredCountry mailNosolicit
mailSourceConversionTag mailAutoReplyAddresses
mailSenderSieve mailCaptureAddress

OID   2.16.840.1.113894.1009.1.101.0.1001.2.3

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.

2.21 inetManagedGroup Object Class

Object class type   auxiliary

Superior class   top

Required attributes   commonname

Allowed attributes   mnggrpDeletionPolicy mnggrpAdditionPolicy
                         mnggrpBillableUser description mnggrpStatus
                         mnggrpMaxUsers mnggrpCurrentUsers mnggrpMailQuota
                         owner nsdaModifiableBy mnggrpUserClassOfServices
                         mailSieveRuleSource mailSieveCollection mailMaxMsgRecipients
                         mailMaxMsgRecipientCutoff mailSendMaxMsgBlocks
                         mailSourceChannel mailOptin1 mailOptin2 mailOptin3
                         mailOptin4 mailOptin5 mailOptin6 mailOptin7 mailOptin8
                         mailSourceOptin1 mailSourceOptin2 mailSourceOptin3
                         mailSourceOptin4 mailSourceOptin5 mailSourceOptin6
                         mailSourceOptin7 mailSourceOptin8 mailDetourHostOptin
                         mailApplyHOHControls mailHeadOfHouseholdDN
                         mgrpURLResultMapping mgrpCheckHeader preferredCountry
                         mailNosolicit mailSourceConversionTag mailAutoReplyAddresses
                         mailAutoReplyMode mailAutoReplySubject mailAutoReplyText
                         mailAutoReplyTextInternal mailAutoReplyTimeout mgrpListTag
                         mailSenderSieve

OID   2.16.840.1.113894.1009.1.101.0.1003.2.3

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.

2.22 inetOrgPerson Object Class

Object class type   structural

Superior class   organizationalPerson

Allowed attributes	audio businessCategory carLicense departmentNumber displayName employeeNumber employeeType givenName homePhone homePostalAddress initials jpegPhoto labeledURI mail manager mobile o pager photo roomNumber secretary uid userCertificate x500uniqueIdentifier preferredLanguage userSMIMECertificate userPKCS12
OID	2.16.840.1.113730.3.2.2

Definition

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

2.23 inetResource Object Class

Object class type	structural
Required attributes	cn
Allowed attributes	telephoneNumber facsimileTelephoneNumber mail postalAddress inetResourceStatus floor building l ucapsCountryCode inetResourceType inetResourceCapacity street st postalCode
OID	2.16.840.1.113894.1009.1.104.1.1012.2.3

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.

2.24 inetSubscriber Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	inetSubscriberAccountId inetSubscriberChallenge inetSubscriberResponse
OID	2.16.840.1.113894.1009.1.102.1.1001.2.1

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.

2.25 inetUser Object Class

Object class type	auxiliary
Superior class	top

Allowed attributes	uid inetUserStatus inetUserHTTPURL userPassword memberOf inetExternalNotificationAddress inetExternalNotificationAddressVerified
OID	2.16.840.1.113894.1009.1.101.0.1015.2.2

Definition

For Mail:

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

For Calendar:

This objectclass can be used with the objectclass `icsCalendarUser` for creating a calendar user account. (Note that the objectclass 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.

2.26 ipGroup Object Class

Object class type	auxiliary
Allowed attributes	inetCos
OID	2.16.840.1.113894.1009.1.104.1.1005.2.1

Definition

Object class to be added to a group entity so that a group service package can be assigned to the group.

2.27 iplanet-am-managed-group Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	inetgroupstatus
OID	2.16.840.1.113894.1009.1.105.1.1002.2.1

Definition

This is the superior class for iplanet-am-managed-static-group

2.28 iplanet-am-managed-group-container Object Class

Object class type	auxiliary

Superior class   top

OID   2.16.840.1.113894.1009.1.102.1.1006.2.1

Definition

The Access Manager class that defines the groups container under each Messaging Server hosted domain.

2.29 iplanet-am-managed-people-container Object Class

Object class type   auxiliary

Superior class   top

OID   2.16.840.1.113894.1009.1.102.1.1007.2.1

Definition

The Access Manager class that defines the people container under each Messaging Server hosted domain.

2.30 iplanet-am-managed-person Object Class

Object class type   auxiliary

Superior class   top

Allowed attributes   iplanet-am-user-account-life

OID   2.16.840.1.113894.1009.1.105.1.1001.2.1

Definition

Specifies Access Manager attributes used to manage users.

2.31 iplanet-am-managed-static-group Object Class

Object class type   auxiliary

Superior class   iplanet-am-managed-group

OID   2.16.840.1.113894.1009.1.105.1.1003.2.1

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.

2.32 ipUser Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	pabURI memberOfManagedGroup maxPabEntries inetCOS psRoot psIncludeInGAB
OID	2.16.840.1.113894.1009.1.107.0.1001.2.1
Definition	

Objectclass 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.

2.33 mailDomain Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	mailRoutingHosts mailRoutingSmartHost preferredMailHost preferredMailMessageStore mailAccessProxyReplay mailDomainAllowedServiceAccess mailDomainWelcomeMessage mailDomainDiskQuota mailDomainMsgQuota mailClientAttachmentQuota mailQuota mailAccessProxyPreAuth mailDomainStatus preferredLanguage mailDomainReportAddress mailDomainMsgMaxBlocks mailDomainSieveRuleSource mailDomainConversionTag mailDomainCatchAllAddress mailAntiUBEService mailFolderDefaultAcl
OID	2.16.840.1.113894.1009.1.104.1.1013.2.1
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 `mailPublicFolder` entry, the presence of the attribute in the `mailDomain` entry allows administrators to specify the default rights to assign to the public folder.

2.34 mailGrantPermission Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	mailGrantSendPermissionsTo sendOnBehalfOf
OID	2.16.840.1.113894.1009.1.101.0.1021.2.1

Definition

The mailGrantPermission object class contains the attribute required to enable Email account delegation.

2.35 mgDomain Object Class

Object class type	auxiliary
Allowed attributes	mgStatus
OID	2.16.840.1.113894.1009.1.109.0.1002.2.1

2.36 mgUser Object Class

Object class type	auxiliary
Allowed attributes	mgStatus cn givenName mail mailAlternateAddress preferredLanguage sn uid userPassword davUniqueId mailHost
OID	2.16.840.1.113894.1009.1.109.0.1001.2.1

2.37 msgCRLMappingTable Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	msgCRLMappingRecord
OID	2.16.840.1.113894.1009.1.101.0.1019.2.1

2.38 msgVanityDomainUser Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	msgVanityDomain
OID	2.16.840.1.113894.1009.1.101.0.1020.2.1

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.

2.39 nabDomain Object Class

Object class type	auxiliary

Allowed attributes	nabDomainNames nabStatus nabDomainAcl nabStore corpDirectoryUrl
OID	2.16.840.1.113894.1009.1.108.0.1001.2.1

Definition

Defines a domain entry with Contacts Server enabled users. This object class enables you to set domain-level access control for Contacts Server users' cross-domain access using its attributes `nabDomainNames` and `nabDomainAcl`. You can use the `nabStatus` attribute in this objectclass to enable or disable NAB service for an entire domain.

2.40 nabUser Object Class

Object class type	auxiliary
Allowed attributes	cn givenName mail mailalternateaddress preferredLanguage sn uid userPassword nabStatus nabStore
OID	2.16.840.1.113894.1009.1.108.0.1002.2.1

Definition

Defines a user entry with Contacts Server service enabled. This object class is recommended for Contacts Server users, but it is not mandatory. By default, a user entry containing the deployment's `uniqueid`, `uid`, `userPassword`, and `mail` attributes works as a valid Contacts Server user entry. This object class provides the capability to enable and disable the Contacts Server service for provisioned users by using the `nabStatus` attribute.

2.41 nsComplexRoleDefinition Object Class

Object class type	structural
Superior class	nsRoleDefinition
Allowed attributes	description
OID	2.16.840.1.113894.1009.1.104.1.1016.2.1

2.42 nsManagedDept Object Class

Object class type	structural
Superior class	groupOfUniqueNames
Allowed attributes	nsNumUsers nsMaxUsers owner nsdaModifiableBy
OID	2.16.840.1.113894.1009.1.101.0.1004.2.1

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.

2.43 nsManagedDeptAdminGroup Object Class

Object class type   auxiliary

Superior class   top

OID   2.16.840.1.113894.1009.1.102.1.1008.2.1

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.

2.44 nsManagedDomain Object Class

Object class type   auxiliary

Superior class   top

Allowed attributes   nsNumUsers nsMaxUsers nsNumMailLists nsNumDomains
                             nsMaxDomains owner nsdaModifiableBy

OID   2.16.840.1.113894.1009.1.101.0.1005.2.1

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.

2.45 nsManagedMailList Object Class

Object class type   auxiliary

Superior class   top

Allowed attributes   nsNumUsers nsMaxUsers owner nsdaModifiableBy

OID   2.16.840.1.113894.1009.1.104.1.1017.2.1

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.

2.46 nsManagedPerson Object Class

Object class type   auxiliary

Superior class   top

Allowed attributes	memberOf nsdaDomain nsdaCapability owner nsdaModifiableBy
OID	2.16.840.1.113894.1009.1.101.0.1006.2.1
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.

2.47 nsNestedRoleDefinition Object Class

Object class type	structural
Superior class	nsComplexRoleDefinition
Required attributes	nsRoleDN
Allowed attributes	nsRoleScopeDN
OID	2.16.840.1.113894.1009.1.104.1.1014.2.1

2.48 nsRoleDefinition Object Class

Object class type	structural
Superior class	ldapSubEntry
Allowed attributes	description
OID	2.16.840.1.113894.1009.1.104.1.1015.2.1

2.49 nsValueItem Object Class

Object class type	structural
Superior class	top
Required attributes	objectClass cn
Allowed attributes	nsValueCIS nsValueCES nsValueTel nsValueInt nsValueBin nsValueDN nsValueType nsValueSyntax nsValueDescription nsValueHelpURL nsValueFlags nsValueDefault
OID	2.16.840.1.113894.1009.1.100.0.1001.2.1

2.50 pab Object Class

Object class type	structural
Superior class	top
Required attributes	cn

Allowed attributes	un description
OID	2.16.840.1.113894.1009.1.101.0.1016.2.1
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";

2.51 pabGroup Object Class

Object class type	structural
Superior class	top
Required attributes	cn
Allowed attributes	un memberOfPAB nickName description
OID	2.16.840.1.113894.1009.1.101.0.1017.2.1
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.

2.52 pabPerson Object Class

Object class type	structural
Superior class	inetOrgPerson
Allowed attributes	un organizationName organizationUnitName co mailAlternateAddress dateOfBirth memberOfPAB memberOfPABGroup nickName
OID	2.16.840.1.113894.1009.1.101.0.1007.2.1

Definition

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

2.53 piEntry Object Class

Object class type   structural

Superior class   top

Required attributes   piEntryID

Allowed attributes   displayName memberOfPIGroup memberOfPiBook
                             multilineDescription piLastModifiedBy deleted attachment
                             category piPEntryXMLData piPEntryTextData privacy alarmflag
                             alarmstatus alarmtime alarmtopic

OID   2.16.840.1.113894.1009.1.107.1.1005.2.1

Definition

All address book entries are created using this structural object class. The basic entry can be
further extended by specific object classes for users (to represent an individual contact entry)
and groups (to represent an address book group).

2.54 piLocalBook Object Class

Object class type   structural

Superior class   piTypeBook

Allowed attributes   piReader piWriter piDeleter piCreator abBookType

OID   2.16.840.1.113894.1009.1.107.1.1003.2.1

Definition

Used to store the access control values for an address book entry and book type. This class is
typically used to extend an address book node created using piAddressBook object class and
the attributes are used to specify access control granted by a user to other users.

2.55 piProfileBook Object Class

Object class type   structural

Superior class   piTypeBook

Required attributes   objectclass

OID   2.16.840.1.113894.1009.1.107.1.1009.2.1

2.56 piPStoreRoot Object Class

Object class type   structural

Superior class	top
Required attributes	piPStoreOwner
Allowed attributes	piDefaultAB piMaxStoreEntries lastPurgeDate
OID	2.16.840.1.113894.1009.1.107.1.1001.2.1
Definition	

Used to create the root node of an address book store root node for a user.

2.57 piRemoteBook Object Class

Object class type	structural
Superior class	piTypeBook
Required attributes	piRemotePiURL
OID	2.16.840.1.113894.1009.1.107.1.1004.2.1
Definition	

Used to store the attributes necessary for a remote address book server. These are typically corporate address books shared by users and have shared and read-only access.

2.58 piTypeABConferenceRoom Object Class

Object class type	structural
Superior class	piEntry
Allowed attributes	telephoneNumber sunConfRoomCapacity campus building floor officeNumber inetCalendar inetFreeBusy contactPerson
OID	2.16.840.1.113894.1009.1.107.1.1007.2.1
Definition	

Used to create an entry to represent a conference room entry. This object class is intended to be used for entries in the users' personal address book store. The corresponding object class used in the corporate LDAP to represent a generic resource entry (including a conference room) is icsCalendarResource.

Since users may find resources in the corporate LDAP directory and decide to add them to their personal address book, you need to map the values from icsCalendarResource to the attributes in piTypeABConferenceRoom. As of now, calendar server has no typing information in the icsCalendarResource entry to indicate what type of resource is represented by LDAP entry. Hence we should assume that the corporate entry is for a conference room.

Table 2.2 Mapping of Attributes

icsCalendarResource	piTypeABConferenceRoom / piEntry

cn	displayName
description	multilineDescription
icsCapacity	sunConfRoomCapacity
	campus
	building
	floor
	officeNumber
icsCalendar	inetCalendar
	inetFreeBusy
icsContact	contactPerson

2.59 piTypeBook Object Class

Object class type structural

Superior class top

Required attributes piEntryID pibooktype

Allowed attributes displayName multilineDescription piLastModifiedBy

OID 2.16.840.1.113894.1009.1.107.1.1002.2.1

Definition

Used to create a basic address book entry. This entry is extended by piAddressBook and piLocalBook object classes.

2.60 piTypeCert Object Class

Object class type structural

Superior class top

Required attributes piEntryID

Allowed attributes piEmail1 piCertId displayName userCertificate memberOfPIBook

OID 2.16.840.1.113894.1009.1.107.1.1010.2.1

2.61 piTypeGroup Object Class

Object class type structural

Superior class piEntry

Allowed attributes piEmail1 piWebsite1 piWebsite1Descr inetCalendar inetFreeBusy

OID 2.16.840.1.113894.1009.1.107.1.1006.2.1

Definition

Used to extend the base entry created by piEntry. Entries extended using this object class are used to represent an address book group entry.

2.62 piTypePerson Object Class

Object class type	structural
Superior class	piEntry
Allowed attributes	piBackpointer givenname middlename fullname sn nickname spouse suffix title gender profession jobTitle company ou department assistantname location officeLocation manager campus building floor officeNumber piPhone1 piPhone2 piPhone3 piPhone4 piPhone5 piPhone6 piPhone7 piPhone8 piPhone9 piPhone10 piPhone11 piPhone12 piPhone13 piPhone14 piPhone15 piPhone16 piPhone17 piPhone18 piPhone19 piPhone20 piPhone1Type piPhone2Type piPhone3Type piPhone4Type piPhone5Type piPhone6Type piPhone7Type piPhone8Type piPhone9Type piPhone10Type piPhone11Type piPhone12Type piPhone13Type piPhone14Type piPhone15Type piPhone16Type piPhone17Type piPhone18Type piPhone19Type piPhone20Type pieMail1 pieMail2 piemail3 pieMail1Type pieMail2Type pieMail3Type pieMail1cn pieMail2cn pieMail3cn pieMail1transtype pieMail2transtype pieMail3transtype piWebsite1 piWebsite2 piWebsite1Descr piWebsite2Descr piWebsite1Type piWebsite2Type inetCalendar inetFreeBusy piIM1ID piIM2ID piIM3ID piIM1Service piIM2Service piIM3Service homePostalAddress homeCity homeState homePostalCode homeCountry homePOBox workPostalAddress workCity workState workPostalCode workCountry workPOBox otherPostalAddress otherCity otherState otherPostalCode otherCountry otherPOBox mailingAddress anniversary dateOfBirth otherDate otherDateDescr photoURL notes contact userSMIMEcertificate logoURL homePostalDelivery homeParcelDelivery homeDomDelivery homeIntlDelivery workPostalDelivery workParcelDelivery workDomDelivery workIntlDelivery label tz latitude longitude sortString otherPostalDelivery otherParcelDelivery otherDomDelivery otherIntlDelivery photoBinaryData photoType
OID	2.16.840.1.113894.1009.1.107.1.1011.2.1

Definition

Used to extend the base entry created by piEntry. Entries extended using this object class are used to represent an individual contact entry.

2.63 piTypeProfile Object Class

Object class type	structural
Superior class	piEntry

Required attributes	objectclass
Allowed attributes	pipProfileTextData pipProfileBinaryData pipProfileXMLData
OID	2.16.840.1.113894.1009.1.107.1.1008.2.1

2.64 sunCommsMetaData Object Class

Object class type	structural
Superior class	top
Required attributes	cn
Allowed attributes	sunkeyvalue
OID	2.16.840.1.113894.1009.1.100.0.1002.2.1

2.65 sunDelegatedOrganization Object Class

Object class type	auxiliary
Allowed attributes	sunAvailableDomainNames sunAvailableServices sunOrgType sunMaxUsers sunNumUsers sunMaxGroups sunNumGroups sunEnableGAB preferredLanguage
OID	2.16.840.1.113894.1009.1.104.1.1004.2.1
Definition	

Object class that defines the properties of a business organization. For example, one property of `sunDelegatedOrganization` can designate a list of domain names the business organization can use for its users. Also, it can define the list of services designated by the provider organization, as available to the business organization, to be assigned to the users.

2.66 sunIMConference Object Class

Object class type	structural
Superior class	top
Allowed attributes	sunIMConferenceAffiliations sunIMConferenceConfiguration cn uid
OID	2.16.840.1.113894.1009.1.103.0.1001.2.1
Definition	

Contains conference room properties.

If `iim.userprops.store` is set to ldap, when a new conference room is created, an entry for the conference room is added to the directory. The conference room entry will contain the `sunIMConference` object class.

The conference entry is created under $iim_ldap.conferencecontainer, $iim_ldap.searchbase. (Here $val refers to the corresponding property in the iim.conf file.) The default value of $iim_ldap.conferencecontainer is ou=sunConferences.

2.67 sunIMStoredMessage Object Class

Object class type	structural
Superior class	top
Allowed attributes	sunIMMessageID sunIMMessageContent
OID	2.16.840.1.113894.1009.1.103.0.1002.2.1

Definition

Contains stored message properties.

If iim.userprops.store is set to ldap, when a new stored message is created, an entry for the stored message is added to the directory. The stored message entry will contain the sunIMStoredMessage object class.

The stored message entry is created under $iim_ldap.storedmessagecontainer, $iim_ldap.searchbase. (Here $val refers to the corresponding property in the iim.conf file.) The default value of $iim_ldap.storedmessagecontainer is ou=sunStoredMessages.

2.68 sunIMUser Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	sunIMUserPrivateSettings sunIMUserRoster sunIMPrivateSettings sunIMRoster imUserStatus
OID	2.16.840.1.113894.1009.1.103.0.1003.2.2

Definition

Provides user services to IM users (contains user properties). Added to user entries under the base DN specified when you run the imadmin assign services command or when you assign IM service to users in Delegated Administrator.

2.69 sunISManagedOrganization Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	sunOrganizationAlias
OID	2.16.840.1.113894.1009.1.104.1.1018.2.1

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.

2.70 sunMailOrganization Object Class

Object class type	auxiliary
Allowed attributes	preferredMailHost preferredMailMessageStore
OID	2.16.840.1.113894.1009.1.104.1.1008.2.1

Definition

Object class to be added to a shared business organization that has mail service. sunMailOrganization adds two attributes (preferredMailHost and preferredMailMessageStore) that specify the mail host and message store partition where mail is stored for all users in the business organization.

You can only add the sunMailOrganization object class to a shared business organization (defined as "shared" with the sunOrgType attribute).

Do not add sunMailOrganization to a full domain business organization (defined as "full" with the sunOrgType attribute). For a full domain business organization, add the mailDomain object class, which also uses the preferredMailHost and preferredMailMessageStore attributes for provisioning the preferred mail host and message store for the domain.

2.71 sunManagedLocation Object Class

Object class type	auxiliary
Allowed attributes	sunBusinessRoot
OID	2.16.840.1.113894.1009.1.104.1.1007.2.1

2.72 sunManagedOrganization Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	inetDomainStatus sunPreferredDomain associatedDomain sunRegisteredServiceName organizationName mailDomainUplevel mailDomainSourceConversionTag mailDomainOptin1 mailDomainOptin2 mailDomainOptin3 mailDomainOptin4 mailDomainOptin5 mailDomainOptin6 mailDomainOptin7 mailDomainOptin8 mailDomainNosolicit mailDomainAutoReplyTimeOut preferredMailHost mailDomainCatchallMapping mailDomainSourceMsgMaxBlocks

mailDomainSourceChannel mailDomainMaxMsgRecipients
mailDomainMaxMsgRecipientCutoff mailDomainDetourHostOptin
mailDomainPrefixText mailDomainSuffixText
mailDomainSenderSieve mailDomainCaptureAddress

OID   2.16.840.1.113894.1009.1.105.0.1001.2.1

Definition

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

2.73 sunManagedProvider Object Class

Object class type   auxiliary

Allowed attributes   sunAllowBusinessOrgType sunBusinessOrgBase
                            sunIncludeServices sunExcludeServices sunAssignableDomains
                            sunAllowMultipleDomains sunAllowOutsideAdmins
                            sunProviderOrgDN

OID   2.16.840.1.113894.1009.1.104.1.1006.2.1

Definition

Object class used for storing the properties of a provider organization. Following are some of the properties maintained by sunManagedProvider:

• Types of business organizations this provider can create

• Where to create the business organizations

• Services available to this provider

• Domain names that can be used by the shared business organizations created under this provider organization

2.74 sunNameSpace Object Class

Object class type   auxiliary

Allowed attributes   sunNameSpaceUniqueAttrs

OID   2.16.840.1.113894.1009.1.102.1.1009.2.1

Definition

Used for LDAP Schema 2 only. Required to be present at the root of a subtree representing a namespace. Access Manager 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 Access Manager 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.

2.75 sunPresenceUser Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	sunPresenceUserPrivacy sunPresencePrivacy
OID	2.16.840.1.113894.1009.1.103.0.1004.2.1
Definition	

Provides presence service to IM users (contains user presence properties). Added to user entries under the base DN specified when you run the imadmin assign services command or when you assign IM service to users in Delegated Administrator.

2.76 sunRealmService Object Class

Object class type	structural
Superior class	top
Allowed attributes	o labeleduri sunkeyvalue sunxmlkeyvalue description
OID	2.16.840.1.113894.1009.1.104.1.1003.2.1

2.77 sunservice Object Class

Object class type	auxiliary
Superior class	top
Required attributes	ou
Allowed attributes	labeleduri sunserviceschema sunkeyvalue sunxmlkeyvalue sunpluginschema description
OID	2.16.840.1.113894.1009.1.104.1.1010.2.1

2.78 sunservicecomponent Object Class

Object class type	structural
Superior class	top

Required attributes	ou
Allowed attributes	sunserviceid sunsmspriority sunkeyvalue sunxmlkeyvalue description
OID	2.16.840.1.113894.1009.1.104.1.1001.2.1
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.

2.79 sunUCPreferences Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	sunUCDefaultApplication sunUCTheme sunUCColorScheme sunUCDefaultEmailHandler sunUCDateFormat sunUCDateDelimiter sunUCTimeFormat sunUCTimeZone sunUCMailSendProfiles sunUCExtendedUserPrefs nswmExtendedUserPrefs icsExtendedUserPrefs sunAbExtendedUserPrefs sunUCExtendedClientPrefs sunUCExternalMailProfile abEventNotificationDestination
OID	2.16.840.1.113894.1009.1.106.1.1001.2.1
Definition	

Used to extend a user entry with attributes required for storing Convergence and Communications Express preferences.

2.80 userPresenceProfile Object Class

Object class type	auxiliary
Superior class	top
Allowed attributes	vacationStartDate vacationEndDate
OID	2.16.840.1.113894.1009.1.101.0.1018.2.1
Definition	

Used to store the presence information for a user.

Index

Colophon

This manual was automatically generated from a master schema definition file. A series of custom stylesheets were used to produce DocBook 5 source, which was then processed using the DocBook XSL stylesheets to produce XSL:FO source. Finally, the XSL:FO source was processed using Apache FOP to produce a Portable Document Format file.

The titles in this document are typeset in Helvetica; the body text is in Palatino.