



## DESS/AUTH Schema Extensions

---

This appendix describes the LDAP directory schema extensions that are installed with the Directory Enabled Service Selection and Authorization (DESS/AUTH) software. These extensions are used by the DESS/AUTH components of the Cisco Subscriber Edge Services Manager (SESM) software. Some objects may contain more attributes than are documented here; only those attributes that are used in the current release are documented.

### Cisco-Specific Schema Extensions

The DESS/AUTH schema extensions include the Cisco-specific classes and attributes described in this section.

#### Classes

Classes are listed in alphabetical order.

```
CiscoAznAssocRoleToResActionAux  
CiscoAznCreatorAux  
CiscoAznFiltrPolicyInheritActAux  
CiscoAznPolicyConditionAux  
CiscoAznPolicyRuleUsageAux  
CiscoAznParentSubjectAux  
CiscoAznRole  
CiscoAznRoleOccupancyAux  
CiscoAznSubordinateSubjectAux  
CiscoDESSaclProfileAux  
CiscoDESSnrpSSG  
CiscoDESSpassthroughService  
CiscoDESSpersonAux  
CiscoDESSproxyService  
CiscoDESSradiusProfileAux  
CiscoDESSservice  
CiscoDESSserviceGroup  
CiscoDESSsubscriberAux  
CiscoDESStunnelService
```

**CiscoAznAssocRoleToResActionAux**

Associates a set of roles with specified resources, either objects in the directory or external entities (such as a file or directory on a web server).

Directory objects should be identified by Distinguished Names. External objects should be identified according to a resource-specific naming convention, such as a filename.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoAznAllowAccess*—single-value integer
- *CiscoAznPrivileges*—multivalued Distinguished Name (dn)
- *CiscoAznResourceName*—single-value case-ignore string
- *CiscoAznRoleList*—multivalued Distinguished Name (dn) containing a list of roles to be associated with the resource

**OID:** 1.2.840.113548.3.2.6.3

**CiscoAznCreatorAux**

Attaches a **CiscoAznCreatorsName** name to directory entries.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoAznCreatorsName*—single-value Distinguished Name (dn) that contains the name of the user that created the entry (can be user name, role name, or group name)

**OID:** 1.2.840.113548.3.2.6.2

**CiscoAznFiltrPolicyInheritActAux**

Blocks **policyRule** inheritance.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoAznFilterAction*—single-value case-ignore string; if *true* filter action is on, if *false* filter action is off

**OID:** 1.2.840.113548.3.2.6.4

**CiscoAznPolicyConditionAux**

Evaluates a variable (specified in the object's *CiscoAznVariableName* attribute) against a value (the *CiscoAznValue* attribute) according to a specified operator (the *CiscoAznOperator* attribute).

Condition is true if the following evaluates to true:

```
<variable><operator><value>
```

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoAznOperator*—single-value case-ignore string that specifies the relationship between the *CiscoAznVariableName* and *CiscoAznValue* attributes; can be one of the following values (definition in parentheses):

```
EQ (equals)
LE (less than or equal to)
LT (less than)
GE (greater than or equal to)
GT (greater than)
NE (not equal to)
```

- *CiscoAznVariableName*—single-value case-ignore string that specifies the variable part of the condition; can be one of the following (description in parentheses):

```
AuthenticationLevel
```

```
(in systems which recognize multiple levels of authentication,
specifies the security level used when establishing the session;
valid operators are EQ, LT, LE, GT, GE, and NE)
```

```
ResourceClass
```

```
(the objectClass value of the object being accessed; any class in
the class hierarchy may be specified; the only valid operator is
EQ)
```

- *CiscoAznValue*—single-value case-ignore string that specifies the value part of the condition; can be *high*, *medium*, or *low* if the attribute *CiscoAznVariableName* is equal to *AuthenticationLevel*, or any valid class name defined in the LDAP schema if the attribute *CiscoAznVariableName* is equal to *ResourceClass*.

**OID:** 1.2.840.113548.3.2.6.5

**CiscoAznPolicyRuleUsageAux**

Contains the resources of a **policyRule** (a core LDAP schema class to which the **CiscoAznPolicyRuleUsageAux** is attached).

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoAznApplicableResources*—multivalued Distinguished Name (dn) that lists the resources of a **policyRule**

**OID:** 1.2.840.113548.3.2.6.1

**CiscoAznParentSubjectAux**

Specifies a parent subject (class is attached to subjects that have associated subordinated subjects).

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoAznSubordinateSubjects*—multivalued Distinguished Name (dn) which contains a list of subordinate subjects

**OID:** 1.2.840.113548.3.2.6.8

**CiscoAznRole**

Defines a role.

**Type:** Structural

**Superior Class:** top

**Naming:** Common Name (cn)

**Containment:** Organization (o)  
Organizational Unit (ou)

- Attributes:**
- *CiscoAznPrivileges*—multivalued case-insensitive string containing a list of valid privileges
  - *CiscoAznRoleOccupants*—multivalued Distinguished Name (dn) which lists the occupants of the role (either users or groups)
  - *CiscoAznDynamicRoleOccupants*—a Cisco schema extension object which specifies occupants which are identified by special names, such as [SELF], [PARENT], [PUBLIC], [CREATOR]
  - *CiscoAznRoleOccupancyCondition*—single-valued case-insensitive string which specifies a condition (filter) determining role occupancy
  - *CiscoAznDenyRoleOccupancy*—multivalued Distinguished Name (dn) which lists users or groups to be denied occupancy
  - *CiscoAznSuperiorRole*—single-valued Distinguished Name (dn) which specifies the role object that is superior to this role (and from which privileges and occupants are inherited)
  - *CiscoAznSubordinateRoles*—multivalued Distinguished Name (dn) which specifies roles that are subordinate to this role

**OID:** 1.2.840.113548.3.2.6.6

#### CiscoAznRoleOccupancyAux

Specifies the list of roles an object occupies (serves as a backpointer to the role objects that include this object as an occupant).

**Type:** Auxiliary

**Superior Class:** top

- Attributes:**
- *CiscoAznRoleList*—multivalued Distinguished Name (dn) which lists the roles occupied by this object
  - *CiscoAznBlockedRoleList*—multivalued Distinguished Name (dn) which lists the roles that have been blocked for this object

**OID:** 1.2.840.113548.3.2.6.7

#### CiscoAznSubordinateSubjectAux

Specifies a subordinate subject.

**Type:** Auxiliary

**Superior Class:** top

- Attributes:**
- *CiscoAznParentSubject*—single-valued Distinguished Name (dn) which identifies the parent subject

**OID:** 1.2.840.113548.3.2.6.9

**CiscoDESSaclProfileAux**

Defines inbound and outbound access control list (ACL) values. Cisco IOS ACL parameters can be specified at the group or user level. ACLs can also be specified at the service level. Settings applied at the group level apply to all users that are members of the group.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoDESSciscoAVPair*—specifies additional service configuration parameters, as *name/value* pairs (may contain *inACL* and *outACL* parameters); in the following XML format:

```
<CISCOAVPAIR>
  <ATTRIBUTENAME>attribute name</ATTRIBUTENAME>
  <VALUE>value</value>
</CISCOAVPAIR>
```

- *CiscoDESSapplicableClassACL*—the class to which the ACL applies; case-ignore string

**OID:** 1.2.840.113548.3.2.7.1

**CiscoDESSnrpSSG**

Represents the NRP-SSG (Network Route Processor-Service Selection Gateway) interface on the Cisco 6400 device. Each NRP-SSG reads configuration data from its own **nrpSSG** object.

**Type:** Structural

**Superior Class:** top

**Naming:** Common Name (cn)

**Containment:** Organization (o)  
Organization Unit (ou)

**Attributes:**

- *CiscoDESSnextHopGatewayEntry*—multivalue case-ignore string which associates next-hop gateway keys with IP addresses; XML format as follows:

```
<NEXTHOPGATEWAYENTRY>
  <KEY>key</KEY>
</NEXTHOPGATEWAYENTRY>
```

The DESS RADIUS translator will encode this attribute (if needed) in the following format:

```
Gkey: ip-address
```

**OID:** 1.2.840.113548.3.2.7.2

**CiscoDESSpassthroughService**

Specifies a passthrough service.

**Type:** Structural

**Superior Class:** top

**Naming:** Common Name (cn)

**Containment:** Organization (o)  
Organization Unit (ou)

**OID:** 1.2.840.113548.3.2.7.4

**CiscoDESSPersonAux**

Contains additional attributes of a person.

**Type:** Auxiliary

**Superior Class:** top

**Containment:** Organization (o)  
Organization Unit (ou)

**Attributes:**

- *CiscoDESSGender*—single-value integer (0 male; 1 female)
- *CiscoDESSHobbies*—multivalued case-insensitive string
- *CiscoDESSageGroup*—single-value string

**OID:** 1.2.840.113548.3.2.7.10

**CiscoDESSproxyService**

Represents a proxy service.

**Type:** Structural

**Superior Class:** CiscoDESSpassthroughService

**Naming:** Common Name (cn)

**Attributes:**

- *CiscoDESSradiusServer*—multivalued string

**OID:** 1.2.840.113548.3.2.7.5

**CiscoDESSradiusProfileAux**

RADIUS attributes for a user or service.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *CiscoDESSidleTimeout*—single-value case-ignore string which specifies, in seconds, the maximum time a connection can remain idle
- *CiscoDESSsessionTimeout*—single-value case-ignore string which specifies, in seconds, the maximum length of a user's session
- *CiscoDESSradiusAttr*—multivalued case-ignore string which specifies RADIUS name/value-pair attributes in XML format, as follows:

```
<RADIUS ATTRIBUTE>
  <ATTRIBUTENAME>name</ATTRIBUTENAME>
  <VALUE>value</VALUE>
</RADIUS ATTRIBUTE>
```

**OID:** 1.2.840.113548.3.2.7.6

**CiscoDESSservice**

Defines the attributes that are common for the *passthrough*, *transparent passthrough*, and *proxy* services.

**Type:** Abstract

**Superior Class:** top

**Naming:** Common Name (cn)

**Containment:** Organization (o)  
Organization Unit (ou)



- Attributes:**
- CiscoDESSserviceRoute*—(required) multivalued case-insensitive string that specifies the IP address and subnet mask of the networks or the hosts where the service is located; XML format is as follows:

```
<SERVICEROUTE>
  <IPADDRESS>address</IPADDRESS>
  <MASK>mask</MASK>
</SERVICEROUTE>
```

The DESS RADIUS translator will encode this attribute (if needed) in the following format:

```
Raddress;mask
```
  - CiscoDESSnextHopGatewayKey*—single-value case-insensitive string that specifies the next-hop key for this service. The DESS RADIUS translator will encode this attribute, if needed, as follows:

```
Gkey
```
  - CiscoDESSaccessMode*—single-value case-insensitive string; can be one of the following values:

```
Concurrent
Sequential
```

The DESS RADIUS translator will encode this attribute, if needed, as follows:

```
MS or MC
```
  - CiscoDESSserviceType*—single-value case-insensitive string which specifies the level of service; must have the following value:

```
outbound
```
  - CiscoDESSprimaryDNSServer*—multivalued case-insensitive string that specifies the primary DNS servers for this service. The DESS RADIUS translator will encode this attribute, if needed, in the following format:

```
Dprimary;secondary;secondary
```
  - CiscoDESSsecondaryDNSServer*—multivalued case-insensitive string which specifies the secondary DNS servers for this service
  - CiscoDESSdomainName*—multivalued case-insensitive string that specifies domain names to be resolved by the specified DNS server
  - CiscoDESSdescription*—single-value case-insensitive string that describes the object

**OID:** 1.2.840.113548.3.2.7.3

**CiscoDESSserviceGroup**

Group of services.

**Type:** Structural

**Superior Class:** top

- Naming:** Common Name (cn)
- Containment:** Organization (o)  
Organization (ou)
- Attributes:**
- *CiscoDESSmemberServices*—multivalued Distinguished Name (dn) that specifies the services that are members of this **serviceGroup** object
  - *description*—single-value case-ignore string that describes the object
- OID:** 1.2.840.113548.3.2.7.7

**CiscoDESSsubscriberAux**

A subscriber (can be an individual user or a group)

- Type:** Auxiliary
- Superior Class:** top
- Attributes:**
- *CiscoDESSAllowCreateSubAccounts*—single-value integer; specifies whether a user can create sub-accounts
  - *CiscoDESSautoLogonService*—multivalued case-ignore string which specifies parameters for services that users will be logged on to automatically; XML format is as follows:
 

```
<AUTOLOGONSERVICE>
  <SERVICENAME></SERVICENAME>
  <USERNAME></USERNAME>
  <PASSWORD></PASSWORD>
</AUTOLOGONSERVICE>
```
  - *CiscoDESSEnableSingleSignon*—single-value integer; specifies whether the single sign-on feature is currently enabled for the subscriber
  - *CiscoDESSGenericAttribute*—multivalued case-ignore string; can be used to store any application-specific information; DESS does not interpret this attribute
  - *CiscoDESSPoolName*—single-value case-ignore string; represents the name of the pool. No longer used.
  - *CiscoDESSPrimaryService*—single-value Distinguished Name (dn); represents the primary service for the user
  - *CiscoDESSserviceFilter*—multivalued Distinguished Name (dn) which lists the set of services that are blocked for (not inherited by) this user
  - *CiscoDESSsubscribedServices*—multivalued Distinguished Name (dn) of the service to which the user has subscribed (may be a service name, or service group name)
- OID:** 1.2.840.113548.3.2.7.8

**CiscoDESStunnelService**

Tunnel service.

**Type:** Structural**Superior Class:** Service**Naming:** Common Name (cn)**Containment:** Organization (o)  
Organization Unit (ou)

**Attributes:**

- *CiscoDESStunnelID*—single-value case-ignore string containing the tunnel ID
- *CiscoDESStunnelType*—single-value case-ignore string that contains the tunnel type (such as 12tp)
- *CiscoDESStunnelIPAddress*—single-value case-ignore string that contains the IP address of the tunnel
- *CiscoDESStunnelPassword*—single-value case-ignore string that contains the password for the tunnel

**OID:** 1.2.840.113548.3.2.7.9

## Attributes

Attributes are listed in alphabetical order.

CiscoAznAllowAccess  
 CiscoAznApplicableResources  
 CiscoAznBlockedRoleList  
 CiscoAznCreatorsName  
 CiscoAznDenyRoleOccupancy  
 CiscoAznDynamicMutuallyExRoles  
 CiscoAznDynamicRoleFlag  
 CiscoAznDynamicRoleOccupants  
 CiscoAznFilterAction  
 CiscoAznOperator  
 CiscoAznParentSubject  
 CiscoAznPrivileges  
 CiscoAznResourceName  
 CiscoAznRoleList  
 CiscoAznRoleOccupants  
 CiscoAznRoleOccupancyCondition  
 CiscoAznStaticMutuallyExRoles  
 CiscoAznSubordinateRoles  
 CiscoAznSubordinateSubjects  
 CiscoAznSuperiorRole  
 CiscoAznValue  
 CiscoAznVariableName  
 CiscoDESSaccessMode  
 CiscoDESSageGroup  
 CiscoDESSallowCreateSubAccounts  
 CiscoDESSapplicableClassACL  
 CiscoDESSapplicableClassRadius  
 CiscoDESSautoLogonService

CiscoDESSblockServiceInheritance  
 CiscoDESSciscoAVPair  
 CiscoDESSclearpassword  
 CiscoDESSciscoAVPair  
 CiscoDESSdomainName  
 CiscoDESSenableSingleSignon  
 CiscoDESSgender  
 CiscoDESSgenericAttribute  
 CiscoDESShobbies  
 CiscoDESShomeURL  
 CiscoDESSidleTimeout  
 CiscoDESSmemberServices  
 CiscoDESSnextHopGatewayEntry  
 CiscoDESSnextHopGatewayKey  
 CiscoDESSpoolName  
 CiscoDESSprimaryService  
 CiscoDESSprimaryDNSServer  
 CiscoDESSradiusAttr  
 CiscoDESSradiusServer  
 CiscoDESSsecondaryDNSServer  
 CiscoDESSserviceFilter  
 CiscoDESSserviceRoute  
 CiscoDESSserviceType  
 CiscoDESSserviceURL  
 CiscoDESSsessionTimeout  
 CiscoDESSsubscribedServices  
 CiscoDESStunnelID  
 CiscoDESStunnelIPAddress  
 CiscoDESStunnelPassword  
 CiscoDESStunnelType  
 CiscoDESSunsubscribedServices

#### CiscoAznAllowAccess

**Type:** single-value integer  
**OID:** 1.2.840.113548.3.1.6.1

#### CiscoAznApplicableResources

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.2

#### CiscoAznBlockedRoleList

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.17

**CiscoAznCreatorsName**

**Type:** single-value dn  
**OID:** 1.2.840.113548.3.1.6.3

**CiscoAznDenyRoleOccupancy**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.11

**CiscoAznDynamicMutuallyExRoles**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.12

**CiscoAznDynamicRoleFlag**

**Type:** single-value IA5 string  
**OID:** 1.2.840.113548.3.1.6.16

**CiscoAznDynamicRoleOccupants**

**Type:** multivalue directory string  
**OID:** 1.2.840.113548.3.1.6.9

**CiscoAznFilterAction**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.6.22

**CiscoAznOperator**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.6.4

**CiscoAznParentSubject**

**Type:** single-value dn  
**OID:** 1.2.840.113548.3.1.6.18

**CiscoAznPrivileges**

**Type:** multivalue directory string  
**OID:** 1.2.840.113548.3.1.6.7

**CiscoAznResourceName**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.6.6

**CiscoAznRoleList**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.5

**CiscoAznRoleOccupants**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.8

**CiscoAznRoleOccupancyCondition**

**Type:** multivalue directory string  
**OID:** 1.2.840.113548.3.1.6.10

**CiscoAznStaticMutuallyExRoles**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.13

**CiscoAznSubordinateRoles**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.15

**CiscoAznSubordinateSubjects**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.6.19

**CiscoAznSuperiorRole**

**Type:** single-value dn  
**OID:** 1.2.840.113548.3.1.6.14

**CiscoAznValue**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.6.20

**CiscoAznVariableName**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.6.21

**CiscoDESSaccessMode**

**Type:** single-value case-ignore string  
**OID:** 1.2.840.113548.3.1.7.1

**CiscoDESSageGroup**

**Type:** single-value case-ignore string  
**OID:** 1.2.840.113548.3.1.7.34

**CiscoDESSallowCreateSubAccounts**

**Type:** single-value integer  
**OID:** 1.2.840.113548.3.1.7.31

**CiscoDESSapplicableClassACL**

**Type:** single-value case-ignore string  
**OID:** 1.2.840.113548.3.1.7.2

**CiscoDESSapplicableClassRadius**

**Type:** single-value case-ignore string  
**OID:** 1.2.840.113548.3.1.7.3

**CiscoDESSautoLogonService**

**Type:** multivalue case-ignore string  
**OID:** 1.2.840.113548.3.1.7.4

**CiscoDESSblockServiceInheritance**

**Type:** single-value integer  
**OID:** 1.2.840.113548.3.1.7.5

**CiscoDESSciscoAVPair**

**Type:** multivalue directory string  
**OID:** 1.2.840.113548.3.1.7.6

**CiscoDESSclearpassword**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.7.7



**CiscoDESSdomainName****Type:** multivalue directory string**OID:** 1.2.840.113548.3.1.7.8**CiscoDESSenableSingleSignOn****Type:** single-value integer**OID:** 1.2.840.113548.3.1.7.27**CiscoDESSgender****Type:** single-value integer**OID:** 1.2.840.113548.3.1.7.32**CiscoDESSgenericAttribute****Type:** multivalue string**OID:** 1.2.840.113548.3.1.7.30**CiscoDESShobbies****Type:** multivalue string**OID:** 1.2.840.113548.3.1.7.33**CiscoDESShomeURL****Type:** single-value directory string**OID:** 1.2.840.113548.3.1.7.36**CiscoDESSidleTimeout****Type:** single-value directory string**OID:** 1.2.840.113548.3.1.7.9

**CiscoDESSmemberServices**

**Type:** single-value dn  
**OID:** 1.2.840.113548.3.1.7.10

**CiscoDESSnextHopGatewayEntry**

**Type:** multivalue directory string  
**OID:** 1.2.840.113548.3.1.7.11

**CiscoDESSnextHopGatewayKey**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.7.12

**CiscoDESSPoolName**

**Type:** single-value string  
**OID:** 1.2.840.113548.3.1.7.29

**CiscoDESSPrimaryService**

**Type:** single-value dn  
**OID:** 1.2.840.113548.3.1.7.28

**CiscoDESSprimaryDNSServer**

**Type:** multivalue directory string  
**OID:** 1.2.840.113548.3.1.7.13

**CiscoDESSradiusAttr**

**Type:** multivalue directory string  
**OID:** 1.2.840.1135548.3.1.7.14

**CiscoDESSradiusServer****Type:** multivalue directory string**OID:** 1.2.840.113548.3.1.7.15**CiscoDESSsecondaryDNSServer****Type:** multivalue directory string**OID:** 1.2.840.113548.3.1.7.16**CiscoDESSserviceFilter****Type:** multivalue dn**OID:** 1.2.840.113548.3.1.7.17**CiscoDESSserviceRoute****Type:** multivalue directory string**OID:** 1.2.840.113548.3.1.7.18**CiscoDESSserviceType****Type:** single-value directory string**OID:** 1.2.840.113548.3.1.7.19**CiscoDESSserviceURL****Type:** single-value directory string**OID:** 1.2.840.113548.3.1.7.20**CiscoDESSsessionTimeout****Type:** single-value directory string**OID:** 1.2.840.113548.3.1.7.21

**CiscoDESSubscribedServices**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.7.22

**CiscoDESStunnelID**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.7.23

**CiscoDESStunnelIPAddress**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.7.24

**CiscoDESStunnelPassword**

**Type:** single-value case-ignore string  
**OID:** 1.2.840.113548.3.1.7.25

**CiscoDESStunnelType**

**Type:** single-value directory string  
**OID:** 1.2.840.113548.3.1.7.26

**CiscoDESSunsubscribedServices**

**Type:** multivalue dn  
**OID:** 1.2.840.113548.3.1.7.35

# Core Policy Objects

In addition to the Cisco-specific schema objects, the Cisco schema uses the following classes from the core Policy schema. These classes were defined in the Internet Engineering Task Force (IETF) draft document, “Policy Framework LDAP Core Schema” (*draft-ietf-policy-core-schema-09.txt*).

## Classes

Classes are listed in alphabetical order.

```

policy
policyActionAuxClass
policyActionInstance
policyConditionAuxClass
policyConditionInstance
policyElementAuxClass
policyGroup
policyGroupContainmentAuxClass
policyInstance
policyRepository
policyRule
policyRuleActionAssociation
policyRuleConditionAssociation
policyRuleContainmentAuxClass
policySubtreesPtrAuxClass
policyTimePeriodConditionAuxClass
vendorPolicyActionAuxClass
vendorPolicyConditionAuxClass

```

### **policy**

Describes a policy-related instance

**Type:** Abstract

**Superior Class:** **cim23ManagedElement**

**Attributes:**

- *cn*—single-value string, containing a user-friendly name of a policy-related object
- *policyKeywords*—multivalued case-exact string containing a set of keywords to assist directory clients in locating policy objects applicable to them. Each value of the multivalued attribute contains a single keyword.
- *cimCaption*—string containing a one-line description of this policy-related object
- *cimDescription*—string containing a long description of this policy-related object

**OID:** 1.2.840.113548.2.2.1

**policyActionAuxClass**

Represents an action to be performed as a result of a policy rule.

**Type:** Auxiliary

**Superior Class:** top

**OID:** 1.2.840.113548.2.2.2

**policyActionInstance**

Contains a reusable policy action.

**Type:** Structural

**Superior Class:** **policyInstance**

**Attributes:** • *policyActionName*—single-value case-ignore string naming the policy action

**OID:** 1.2.840.113548.2.2.3

**policyConditionAuxClass**

Represents a condition to be evaluated in conjunction with a policy rule.

**Type:** Auxiliary

**Superior Class:** top

**OID:** 1.2.840.113548.2.2.4

**policyConditionInstance**

Contains a reusable policy condition.

**Type:** Structural

**Superior Class:** **policyInstance**

**Attributes:** • *policyConditionName*—single-value case-ignore string naming the policy condition

**OID:** 1.2.840.113548.2.2.5

**policyElementAuxClass**

Tags instances of classes defined outside the realm of policy as relevant to a particular policy specification.

**Type:** Auxiliary

**Superior Class:** **policy**

**OID:** 1.2.840.113548.2.2.6

**policyGroup**

Container for either a set of related policy rules or a set of related **policyGroup** objects.

**Type:** Structural

**Superior Class:** **policyGroupName**

**Attributes:**

- *policyGroupName*—(required) single-value case-ignore string naming the policy group

**OID:** 1.2.840.113548.2.2.7

**policyGroupContainmentAuxClass**

Binds policyGroups to an appropriate container object.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *policySubtreesAuxContainedSet*—an unordered set of Distinguished Name (dn) pointers to one or more **policyRule** objects associated with the instance of the class

**OID:** 1.2.840.113548.2.2.8

**policyInstance**

Contains reusable policy information.

**Type:** Structural

**Superior Class:** **policy**

**Attributes:**

- *policyInstanceName*—single-value case-ignore string naming the policy instance

**OID:** 1.2.840.113548.2.2.9

**policyRepository**

A container for reusable information.

**Type:** Structural

**Superior Class:** **cim23AdminDomain**

**Attributes:**

- *policyRepositoryName*—(required) single-value case-ignore string naming the policy repository

**OID:** 1.2.840.113548.2.2.10

**policyRule**

Represents the *if condition then action* semantics associated with a policy rule.

**Type:** Structural

**Superior Class:** **policy**



- Attributes:**
- *policyRuleName*—(required) case-ignore string containing the name of this policy rule
  - *policyRuleEnabled*—enumeration, one of the following (meaning is in parentheses):
    - enabled (policy rule administratively enabled)
    - disabled (policy rule administratively disabled)
    - enabledForDebug (policy rule disabled for debug mode)
  - *policyRuleConditionListType*—enumeration, can be one of the following (meaning is in parentheses):
    - DNF (policy rule is in disjunctive normal form)
    - CNF (policy rule is in conjunctive normal form)
  - *policyRuleConditionList*—unordered set of Distinguished Names (dn) representing associations between this policy rule and its conditions
  - *policyRuleActionList*—unordered set of Distinguished Names (dn) representing associations between this policy rule and its actions
  - *policyRuleValidityPeriodList*—unordered set of Distinguished Names (dn) of **policyTimePeriodCondition** objects that determine when the policy rule is scheduled to be active or inactive
  - *policyRuleUsage*—single-value case-ignore string providing guidelines on how the policy should be used
  - *policyRulePriority*—integer (non-negative) which prioritizes this policy rule relative to other policy rules; the larger the value, the higher the priority
  - *policyRuleMandatory*—boolean; if true, evaluation of the policy conditions and execution of policy actions is mandatory
  - *policyRuleSequencedActions*—enumeration indicating how to interpret the action-ordering indicated by the *policyRuleActionList* attribute; can be one of the following:
    - mandatory
    - recommended
    - dontCare
  - *policyRoles*—multivalued case-ignore string with the following form:
    - <RoleName> [ &&<RoleName> ]

Role names are alphabetized; each value represents a role combination, including the special case of a “combination” containing only one role.

**OID:** 1.2.840.113548.2.2.11

**policyRuleActionAssociation**

Contains an attribute that represents an execution order for an action in the context of a policy rule.

**Type:** Structural

**Superior Class:** *policy*

**Attributes:**

- *policyActionOrder*—(required) integer indicating the relative order of an action in the context of a policy rule
- *policyActionName*—(required) single-value case-ignore string containing the name of the policy action
- *policyActionDN*—single-value Distinguished Name (dn) pointing to a reusable policy action

**OID:** 1.2.840.113548.2.2.12

**policyRuleConditionAssociation**

Contains attributes characterizing the relationship between a policy rule and one of its policy conditions.

**Type:** Structural

**Superior Class:** *policy*

**Attributes:**

- *policyConditionGroupNumber*—boolean; if true, the policy condition is negated in the DNF or CNF expression associated with a policy rule
- *policyConditionNegated*—integer indicating the number of the group to which a policy condition belongs
- *policyConditionName*—single-value case-ignore string naming the policy condition
- *policyConditionDN*—single-value Distinguished Name (dn) pointing to a reusable policy condition

**OID:** 1.2.840.113548.2.2.13

**policyRuleContainmentAuxClass**

Binds policy rules to an appropriate container object.

**Type:** Auxiliary

**Superior Class:** *top*

**Attributes:**

- *policyRulesAuxContainedSet*—unordered set of Distinguished Names (dn) representing policy rules associated in some way with the instance to which this attribute has been appended

**OID:** 1.2.840.113548.2.2.14

**policySubtreesPtrAuxClass**

Provides pointers to roots of DIT (directory information tree) subtrees containing policy-related objects.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *policySubtreesAuxContainedSet*—unordered set of Distinguished Names (dn) of objects that serve as roots for DIT subtrees containing policy-related objects

**OID:** 1.2.840.113548.2.2.15

**vendorPolicyActionAuxClass**

Defines a registered means to describe a policy action.

**Type:** Auxiliary

**Superior Class:** **policyActionAuxClass**

**Attributes:**

- *vendorPolicyActionData*—Octet string, used as an escape mechanism for actions that have not been modeled as specific attributes
- *vendorPolicyActionEncoding*—an OID identifying the format and semantics for this instance of the *vendorPolicyActionData* attribute

**OID:** 1.2.840.113548.2.2.17

**vendorPolicyConditionAuxClass**

Defines a registered means to describe a policy condition.

**Type:** Auxiliary

**Superior Class:** top

**Attributes:**

- *vendorPolicyConstraintData*—Octet string used as an escape mechanism for representing constraints that have not been modeled as specific attributes
- *vendorPolicyConstraintEncoding*—an OID for identifying the format and semantics for this instance of the *vendorPolicyConstraintData* attribute

**OID:** 1.2.840.113548.2.2.18

## Attributes

Attributes are listed in alphabetical order.

```

policyActionDN
policyActionName
policyActionOrder
policyConditionDN
policyConditionGroupName
policyConditionName
policyGroupName
policyGroupNegated
policyGroupsAuxContainedSet
policyInstanceName
policyKeywords
policyRepositoryName
policyRoles
policyRuleActionList
policyRuleConditionList
policyRuleConditionListType
policyRuleEnabled
policyRuleMandatory
policyRuleName
policyRulePriority
policyRulesAuxcontainedSet
policyRuleSequencedActions
policyRuleUsage
policyRuleValidityPeriodList
policySubtreesAuxContainedSet
ptpConditionDayOfMonthMask
ptpConditionDayOfWeekMask
ptpConditionLocalOrUtcTime
ptpConditionMonthOfYearMask
ptpConditionTime
ptpConditionTimeOfDayMask
vendorPolicyActionData
vendorPolicyActionEncoding
vendorPolicyConstraintData
vendorPolicyConstraintEncoding

```

### policyActionDN

**Type:** single-value distinguishedNameMatch dn

**OID:** 1.2.840.113548.2.1.1

### policyActionName

**Type:** single-value caseExactIA5Match IA5String

**OID:** 1.2.840.113548.2.1.2

**policyActionOrder****Type:** single-value integerMatch integer**OID:** 1.2.840.113548.2.1.3**policyConditionDN****Type:** single-value distinguishedNameMatch dn**OID:** 1.2.840.113548.2.1.4**policyConditionGroupNumber****Type:** single-value integerMatch integer**OID:** 1.2.840.113548.2.1.5**policyConditionName****Type:** single-value caseExactIA5Match IA5String**OID:** 1.2.840.113548.2.1.6**PolicyConditionNegated****Type:** single-value caseExactIA5Match IA5String**OID:** 1.2.840.113548.2.1.7**policyGroupName****Type:** caseExactMatch IA5String**OID:** 1.2.840.113548.2.1.8**policyGroupNegated****Type:** single-value booleanMatch boolean**OID:** 1.2.840.113548.2.1.7

**policyGroupsAuxContainedSet****Type:** distinguishedNameMatch dn**OID:** 1.2.840.113548.2.1.9**policyInstanceName****Type:** single-value caseExactIA5Match IA5String**OID:** 1.2.840.113548.2.1.10**policyKeywords****Type:** caseExactMatch IA5String**OID:** 1.2.840.113548.2.1.11**policyRepositoryName****Type:** single-value caseExactIA5Match IA5String**OID:** 1.2.840.113548.2.1.12**policyRoles****Type:** caseIgnoreMatch DirectoryString**OID:** 1.2.840.113548.2.1.13**policyRuleActionList****Type:** distinguishedNameMatch dn**OID:** 1.2.840.113548.2.1.14**policyRuleConditionList****Type:** distinguishedNameMatch dn**OID:** 1.2.840.113548.2.1.15

**policyRuleConditionListType****Type:** single-value integerMatch integer**OID:** 1.2.840.113548.2.1.16**policyRuleEnabled****Type:** single-value integerMatch integer**OID:** 1.2.840.113548.2.1.17**policyRuleMandatory****Type:** single-value booleanMatch boolean**OID:** 1.2.840.113548.2.1.18**policyRuleName****Type:** caseExactMatch IA5String**OID:** 1.2.840.113548.2.1.19**policyRulePriority****Type:** single-value integerMatch integer**OID:** 1.2.840.113548.2.1.20**policyRulesAuxcontainedSet****Type:** distinguishedNameMatch dn**OID:** 1.2.840.113548.2.1.21**policyRuleSequencedActions****Type:** integerMatch integer**OID:** 1.2.840.113548.2.1.22

**policyRuleUsage****Type:** single-value case-ignore DirectoryString**OID:** 1.2.840.113548.2.1.23**policyRuleValidityPeriodList****Type:** distinguishedNameMatch dn**OID:** 1.2.840.113548.2.1.24**policySubtreesAuxContainedSet****Type:** distinguishedNameMatch dn**OID:** 1.2.840.113548.2.1.25**ptpConditionDayOfMonthMask****Type:** single-value bitStringMatch bit string**OID:** 1.2.840.113548.2.1.26**ptpConditionDayOfWeekMask****Type:** single-value bitStringMatch bit string**OID:** 1.2.840.113548.2.1.27**ptpConditionLocalOrUtcTime****Type:** single-value integerMatch integer**OID:** 1.2.840.113548.2.1.28**ptpConditionMonthOfYearMask****Type:** single-value bitStringMatch bit string**OID:** 1.2.840.113548.2.1.29



**ptpConditionTime****Type:** single-value caseIgnoreMatch PrintableString**OID:** 1.2.840.113548.2.1.30**ptpConditionTimeOfDayMask****Type:** single-value bitstringMatch bit string**OID:** 1.2.840.113548.2.1.31**vendorPolicyActionData****Type:** octetStringMatch OctetString**OID:** 1.2.840.113548.2.1.32**vendorPolicyActionEncoding****Type:** single-value objectIdentifierMatch OID**OID:** 1.2.840.113548.2.1.33**vendorPolicyConstraintData****Type:** octetStringMatch OctetString**OID:** 1.2.840.113548.2.1.34**vendorPolicyConstraintEncoding****Type:** single-value objectIdentifierMatch OID**OID:** 1.2.840.113548.2.1.35

# Core LDAP Schema Objects

The Cisco DESS/AUTH schema also uses of the following classes that are defined in the core LDAP schema. Only those attributes used by DESS/AUTH are listed.

## Classes

Classes are listed in alphabetical order.

```
groupOfNames
inetOrgPerson
organizationalPerson
organizationalUnit
person
```

### groupOfNames

**Type:** Structural

**Superior Class:** top

**Attributes:**

- *cn*—multivalued string; name of the group
- *description*—multivalued string; description of the group
- *uniqueMember*—multivalued dn

**OID:** 2.5.6.9

### inetOrgPerson

**Type:** Structural

**Superior Class:** organizationalPerson

**Attributes:**

- *groupMembership*—multivalued dn
- *UID*—multivalued string
- *givenName*—multivalued string
- *homePhone*—multivalued telephone number
- *initials*—multivalued string
- *mail*—multivalued string
- *mobile*—multivalued telephone number
- *pager*—multivalued telephone number
- *uid*—multivalued string

**OID:** 2.16.840.1.113730.3.2.2

**organizationalPerson****Type:** structural**Superior Class:** person**Attributes:**

- *facsimileTelephoneNumber*—multivalued facsimile telephone number
- *postalAddress*—multivalued postal address
- *street*—multivalued string

**OID:** 2.5.6.7**organizationalUnit****Type:** structural**Superior Class:** ndsLoginProperties  
ndsContainerLoginProperties**Attributes:**

- *facsimileTelephoneNumber*—multivalued facsimile telephone number
- *postalAddress*—multivalued postal address
- *street*—multivalued string

**OID:** 2.5.6.5**person****Type:** structural**Superior Class:** ndsLoginProperties**Attributes:**

- *telephoneNumber*—multivalued telephone number
- *city*—multivalued string
- *st*—multivalued string

**OID:** 2.5.6.6

## Attributes

The core LDAP classes use the following attributes (only those used by the Cisco DESS/AUTH schema are shown):

```
city
cn
description
facsimileTelephoneNumber
givenName
groupMembership
homePhone
initials
mail
mobile
pager
postalAddress
st
street
telephoneNumber
uid
UID
uniqueMember
```

### city

**Type:** multivalue directory string

**OID:** 2.16.840.1.113719.1.8.4.4

### cn

**Type:** multivalue directory string

**OID:** 2.5.4.3

### description

**Type:** multivalue directory string

**OID:** 2.5.4.13

### facsimileTelephoneNumber

**Type:** multivalue facsimile telephone number

**OID:** 2.5.4.23

**givenName****Type:** multivalue directory string**OID:** 2.5.4.42**groupMembership****Type:** multivalue dn**OID:** 2.16.840.1.113719.1.1.4.1.25**homePhone****Type:** multivalue telephone number**OID:** 0.9.2342.19200300.100.1.20**initials****Type:** multivalue directory string**OID:** 2.5.4.43**mail****Type:** multivalue directory string**OID:** 0.9.2342.19200300.100.1.3**mobile****Type:** multivalue telephone number**OID:** 0.9.2342.19200300.100.1.41**pager****Type:** multivalue telephone number**OID:** 0.9.2342.19200300.100.1.42

**postalAddress****Type:** multivalue postal address**OID:** 2.5.4.16**st****Type:** multivalue directory string**OID:** 2.5.4.8**street****Type:** multivalue directory string**OID:** 2.5.4.9**telephoneNumber****Type:** multivalue telephone number**OID:** 2.5.4.20**uid****Type:** multivalue directory string**OID:** 0.9.2342.19200300.100.1.1**uniqueMember****Type:** multivalue dn**OID:** 2.5.4.50