Organization Units

What Is an OU?

An OU is a container in the AD domain that can contain other OUs, as well as users, computers, groups, and so on. OUs are a way to organize your objects into containers based on a logical structure. The OU design enables you to assign a flexible administrative model that eases the support and management of a large, distributed enterprise. The OU design is also used for setting up security groups.

AD controls permission to create an OU. Typically, the Domain Administrator has rights to create OUs at the root of the domain, then delegates control of those OUs to other users. After the Domain Administrator delegates a user OU control, the user has permission to create the Cisco Root OU.

Related Topics

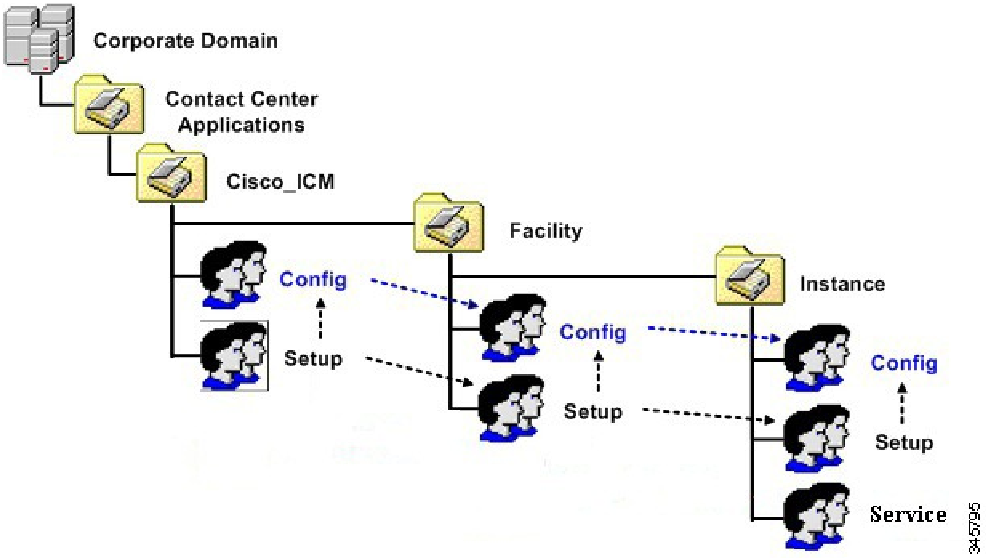
Security Groups, on page 4

OU Hierarchies

Unified ICM uses the following hierarchy of OUs:

- The Cisco Root OU (Cisco_Root)
- One or more Facility OUs
- One or more Instance OUs

Figure 1: Organizational Unit (OU) Hierarchy



All objects that Unified ICM requires are created in OUs on the domain. You can place the OU hierarchy that the Unified ICM creates at the Root of the domain, or in another OU. Servers are not placed in this OU hierarchy. You can place servers in other OUs on the domain.

Note

- The system software always uses a Cisco Root OU named “Cisco_ICM” (see preceding figure).
- The Domain Admin is a member of the Config, and Setup in the Cisco Root OU.
- Installing Unified ICM in the corporate domain is now a supported environment.

Related Topics

Security Groups and OUs, on page 4
Cisco Root OU, on page 2
Facility OU, on page 3
Instance OU, on page 3

Cisco Root OU

You can place the Cisco Root OU at any level within the domain. Software components locate the Cisco Root OU by searching for its name.

The Cisco Root OU contains one or more Facility OUs.

What is the Cisco Root OU?

- Unified ICM always uses a Cisco Root OU named “Cisco_ICM”.
- The OU containing all domain resources created by Unified ICM.
- Defines permissions for all Unified ICM instances.

- Only one Cisco Root OU can exist in each domain

For more information, see Appendix B - Moving the Cisco Root OU.

Related Topics

Create or Add Cisco Root

Facility OU

A Facility OU is a group of Instance OUs that are organizationally related or have similar management needs. Permissions defined for a Facility OU propagate to each Instance OU contained in that facility.

The Facility OU provides an administrative separation between Unified ICM instances. For example, you might have different Facility OUs for Lab and Production Unified ICM instances.

A Facility OU inherits the permissions set for the containing Cisco Root OU. You can then specify different user permissions specific to that Facility.

Note Facility OU names must be 32 characters or less.

Related Topics

Instance OU, on page 3

Cisco Root OU, on page 2

Instance OU

An Instance OU inherits the permissions set for the containing Facility OU. You can then specify different user permissions specific to that instance.

Unified ICM Instance OU

A Unified ICM instance is a single installation of the system software. It consists of several components (including the CallRouter, the Logger, Administration & Data Server, and Peripheral Gateways), some of which might be duplexed.

An Instance OU:

- Is the representation of a Unified ICM instance.
    - Each Unified ICM instance has an associated Instance OU.
- Defines permissions for that instance as part of that Instance OU.

  An Instance OU inherits the permissions set for the containing Facility OU; you can then specify different user permissions specific to that Instance.
- Is named by the user according to the following rules:
    - Limited to 5 characters

- Alphanumeric characters only
- Can not start with a numeric character
- Some instance names are reserved (local and sddsn)

Related Topics

Facility OU, on page 3

Security Groups

Security Groups and OUs

Each OU in the OU hierarchy has associated security groups.

Security groups permissions are inherited down the chain in the OU hierarchy. For example, users added to a security group for a Facility OU have the privileges of that security group for all Instance OUs contained in that Facility OU.

Each OU has the following security groups:

- Config Security Group
- Setup Security Group

In addition to the preceding list, Instance OUs also contain the Service Security Group.

Warning Microsoft limits the number of cascading groups in the OU hierarchy. For more information, see Microsoft *Active Directory Maximum Limits - Scalability* article at http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx.

Warning Users who are local administrators for the server automatically can perform configuration tasks. Therefore, only users who are members of the Setup Security Group must be local administrators.

Security Groups Described

A security group is a collection of domain users to whom you grant a set of permissions to perform tasks with system software.

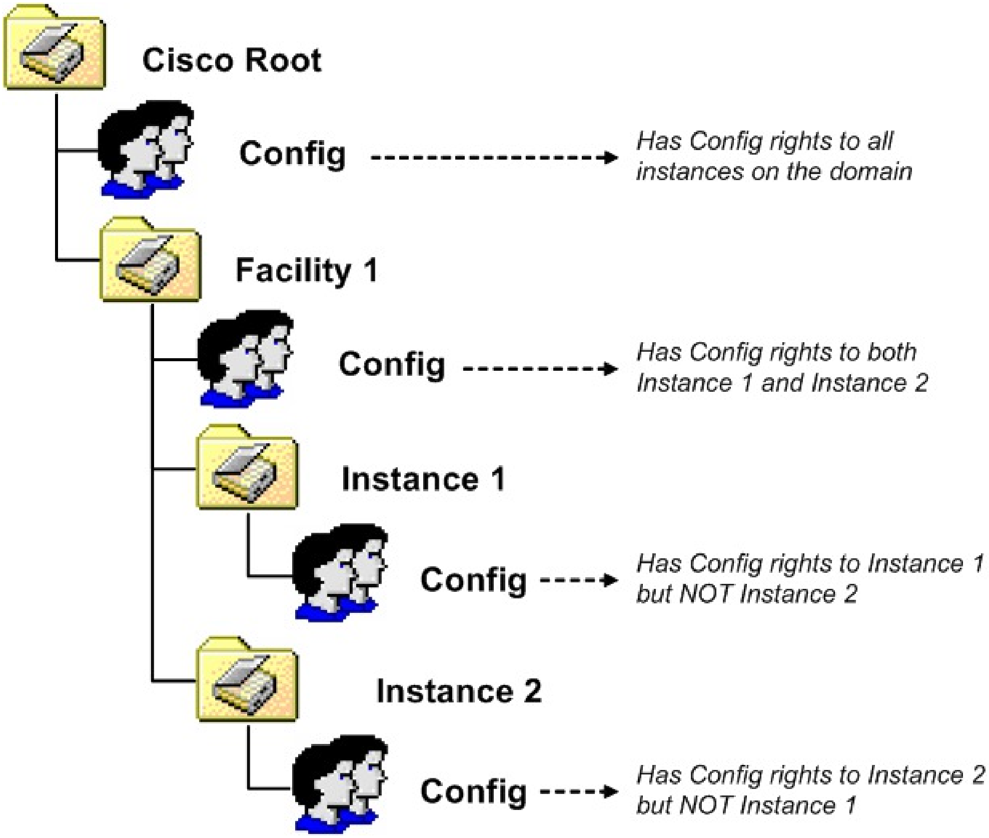
For each security group, you add domain users, who are granted privileges to the functions controlled by that security group. Users are given membership in the security groups to enable permission to the application. You can create these users in other OUs in this domain, or in any trusted domain.

Note The user who creates the Cisco Root OU automatically becomes a member of the Setup Security Group for the Cisco Root OU. In effect, this user is granted privileges to all Unified ICM tasks in the domain.

Security Groups:

- Similar groups at each level of the hierarchy allow users to be granted permission to multiple Instances.
- Are nested so that:
  - A similar group from the Parent OU is a member of each group.

Figure 2: Security Group Nesting


Cisco Root
Config
Has Config rights to all instances on the domain
Facility 1
Config
Has Config rights to both Instance 1 and Instance 2
Instance 1
Config
Has Config rights to Instance 1 but NOT Instance 2
Instance 2
Config
Has Config rights to Instance 2 but NOT Instance 1

- Use AD Domain Local Security Groups.

Related Topics

Add Users to Security Group

Security Group Names and Members

The function names of the security groups are Setup, Config, and Service. Group names must be unique in AD. Combining the names of levels of the hierarchy with the function name helps allow a unique name to be generated.

Names of the security groups created by OUs at various levels include:

- Root: `Cisco_ICM_<function>`
- Facility: `<Facility>_<function>`

- Instance: `<Facility>_<Instance>_<function>`

NetBIOS names truncate if needed and random digits are appended.

Security Group Members:

- You can add any user from a trusted domain to a group.
- Group nesting allows for groups outside the OU hierarchy.

Config Security Group

The Config Security Group controls access privileges to the common Unified ICM configuration tasks.

Domain users whom you added to a Config Security Group have access to the following applications at that point in the OU hierarchy and below:

- Configuration Manager

Note Config users can only perform AD operations using the User List tool (provided they have AD permissions to do so). Members of the Setup Group automatically have the permissions required to use the User List tool.

- Script Editor
- Internet Script Editor
- Database Access
  - SQL Permission granted to the Configuration group instead of to individual users. Database access is given explicitly to the Instance level group. Group nesting gives this access to Facility and Root configuration members.

Added to the GeoTelGroup role on the Administration & Data Server DB.

Note For Administration & Data Server DBs only. Not for Logger DBs and HDSs.

Setup Security Group

The Setup Security Group controls rights to run:

- Installation and Setup Tools
- Configuration Manager

Users who are members of the Setup Security Group can:

- Install instances and software components.

- Add users to security groups.
- Create service accounts.
- Manage OUs, groups, users, and permissions.

Note The Setup Security Group is automatically made a member of the Config for that Unified ICM instance.

The Setup group at each level is given AD permissions to the parent OU.

Figure 3: Setup Security Group permissions

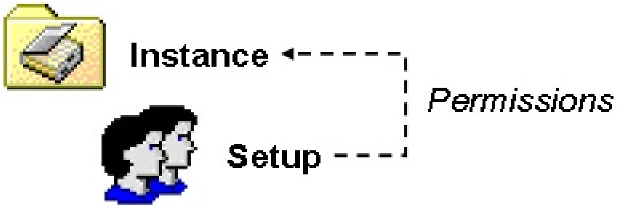


Table 1: Setup Security Group AD permissions

Tasks	OU Hierarchy Level
Delete Subtree	Child objects only
Modify Permissions	Child objects only
Create/Delete OU Objects	This object and all child objects
Create Group Objects	Child objects only
Read/Write Property	Group objects
Special: Create/Delete User Objects	This object and all child objects

For more information see the chapter Service Account Manager.

OU Hierarchies and Security

OUs are nested as described in the preceeding section, with the Root OU containing Facility OUs, which contain Instance OUs. For Unified ICM, the Cisco Root OU is the “Cisco_ICM” OU. As OUs have associated security groups, the nesting of OUs allow the nesting of access rights. Members of a security group have all the access rights granted to that same security group at lower levels in the hierarchy.

Examples:

If you make a user a member the Root Setup security group (see Root Setup Security Group Member Permissions/Access Rights following), that user has the following permissions/access rights:

- Permissions/access rights in the Root Setup security group.

  This also grants permissions/access rights for this user in the:

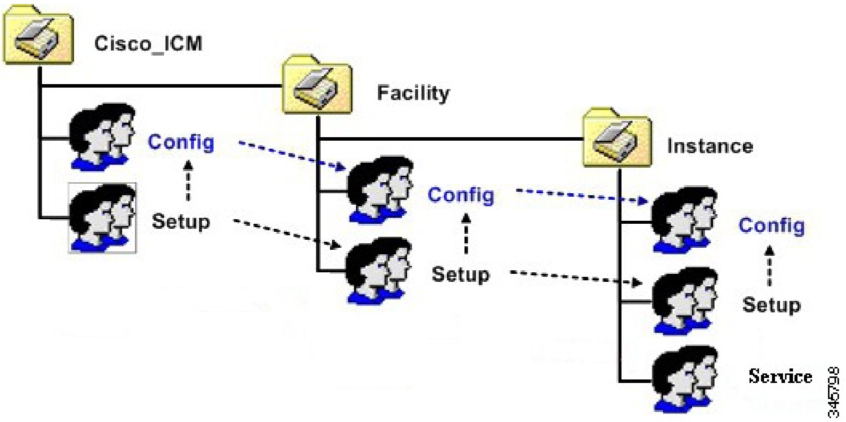
  - Facility Setup group
  - Instance Setup group

- Permissions/access rights in the Root Config security group.

  This also grants permissions/access rights for this user in the:

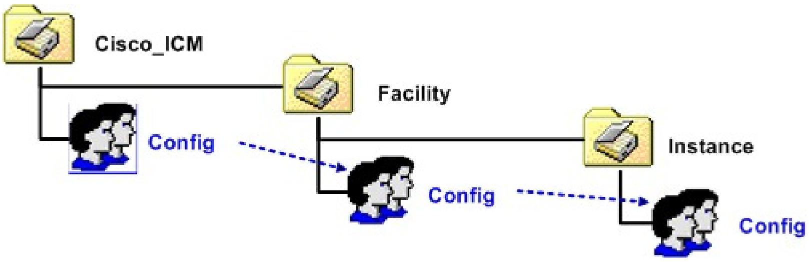
  - Facility Config group
  - Instance Config group

Figure 4: Root Setup Security Group Member Permissions/Access Rights



Making a user a member of the Root Config security group grants permissions/access rights in that security group as well as the Facility and the Instance Config security groups.

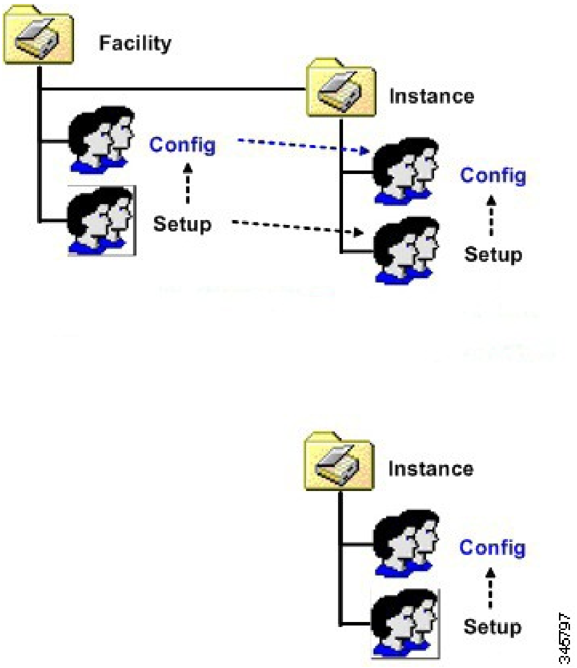
Figure 5: Root Config Security Group Member Permissions/Access Rights



Members of a Facility security group have all the permissions/access rights granted to Instance OUs nested within that Facility. However, members of those Instance OUs security groups do not necessarily have the permissions/access rights granted to their containing Facility OU.

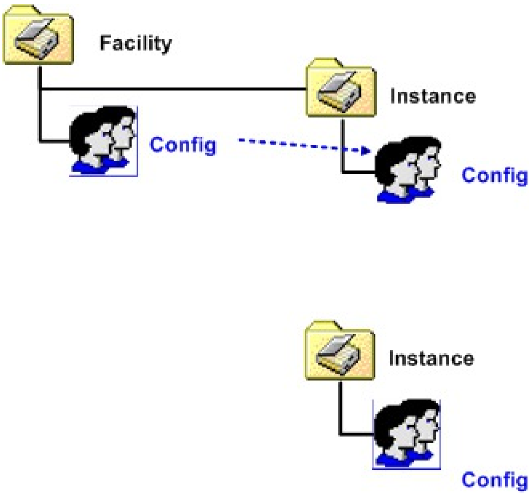
A member of the Instance Setup security group is granted permissions/access rights only to the Instance level security groups (Setup and Config).

Figure 6: Facility/Instance Setup Security Group Member Permissions/Access Rights



In the following illustrations, a member the Facility Config security group has permissions/access rights to that security group and the Instance Config security group. However, a member of the Instance Config security group only has permissions/access rights to that security group.

Figure 7: Facility/Instance Config Security Group Member Permissions/Access Rights



This hierarchy allows you to define security with maximum flexibility. For example, you can grant permissions/access rights at the Facility OU level, so those users have access to a set of instances. You can then define permissions for instance administrators at the Instance OU level, and those users would not have access to the other instances.

Note You cannot move an Instance from one Facility to another.

Related Topics

Instance OU, on page 3

Service Security Group

The Service Security Group is a security group generated automatically for Instance OUs. It exists at the Instance level only. The Service Security Group controls access between the system software components.

Note The Service Security Group is not exposed to users for the Domain Manager. You do not have to perform any tasks related to it.

The group has a SQL login and is a member of the GeoTelAdmin role on the following databases:

- Logger SideA DB
- Logger SideB DB
- Administration & Data Server DB
- HDS
- Outbound Option DB

Service Logon Accounts

- You do not have to randomly generate passwords. You can provide passwords and save them in AD or on the local machine, or save them on both.
- Passwords are 64 characters long and include:
    - English upper case characters (A..Z)
    - English lower case characters (a..z)
    - Base 10 digits (0..9)
    - Non-alphanumeric characters (! @ # % ^ & * ( ) [ ] { } ` ~ - + ? . , ; : ' < >)
- Are added to local Administrators group.
- Are given rights to Logon as a Service.
- DNS names are comprised of: <*Instance component machine*>

  Possible components are the:

    - Distributor (NetBIOS name is Distrib)
    - LoggerA
    - LoggerB

  - Tomcat

- NetBIOS names are comprised of: <*instance component-#####*>

  where *#####* is used to represent digits added to ensure the NetBIOS name is comprised of the full 20 characters allowed to help ensure, but not guarantee its uniqueness. The list of possible components is the same as those for the DNS names except as indicated above.