CHAPTER 1

CDAT Overview

The Cisco Distributed Administration Tool (CDAT) provides a set of web-based facilities that allow the service-provider administrator to create and maintain the subscriber, service, and policy information used by the Cisco Subscriber Edge Services Manager (Cisco SESM) and the Service Selection Gateway (SSG).

When a Cisco SESM web application uses an LDAP-compliant directory as its data repository for subscriber, service, and policy information, CDAT creates and maintains the information on users, services, and access policy that is stored in the directory. Cisco SESM and the SSG use this information for authentication of the subscriber's credentials and authorization for subscribers to access services.

An SESM web application and CDAT use the Cisco Directory Enabled Service Selection and Authorization (DESS/AUTH) programming interfaces and Role Based Access Control (RBAC) for authentication, authorization, and account and service management. With CDAT, DESS/AUTH, and RBAC, most account-management tasks are accomplished at the group level. CDAT, DESS/AUTH, and RBAC provide an out-of-the-box bulk administration model that gives the service provider a scalable management solution for services and large user populations.

The CDAT overview in this chapter includes these topics:

CDAT and the DESS/AUTH components that it uses are installed by the Cisco SESM software installation program. For information on the CDAT and the DESS/AUTH installation and configuration procedures, see the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide.*

SESM, CDAT, and DESS/AUTH

An SESM system that uses an LDAP directory as its data repository for subscriber and service information includes the following software:

- SESM
- CDAT
- DESS/AUTH

For a complete description of an SESM system, see the *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide.*

SESM

A Cisco SESM web application allows subscribers of DSL, cable, wireless, and dial-up to simultaneously access multiple services provided by different Internet service providers, application service providers, and Corporate Access Servers.

Cisco SESM software allows a service provider to create a customized web application that provides a network portal for individual subscribers. Through the Cisco SESM web-based network portals, subscribers can have simultaneous access to the Internet, corporate intranets, gaming, and other entertainment-based services. After logging on and being authenticated to the system, subscribers access their own personalized services by simply pointing and clicking. Because information in an LDAP directory can be dynamically updated, the subscriber can:

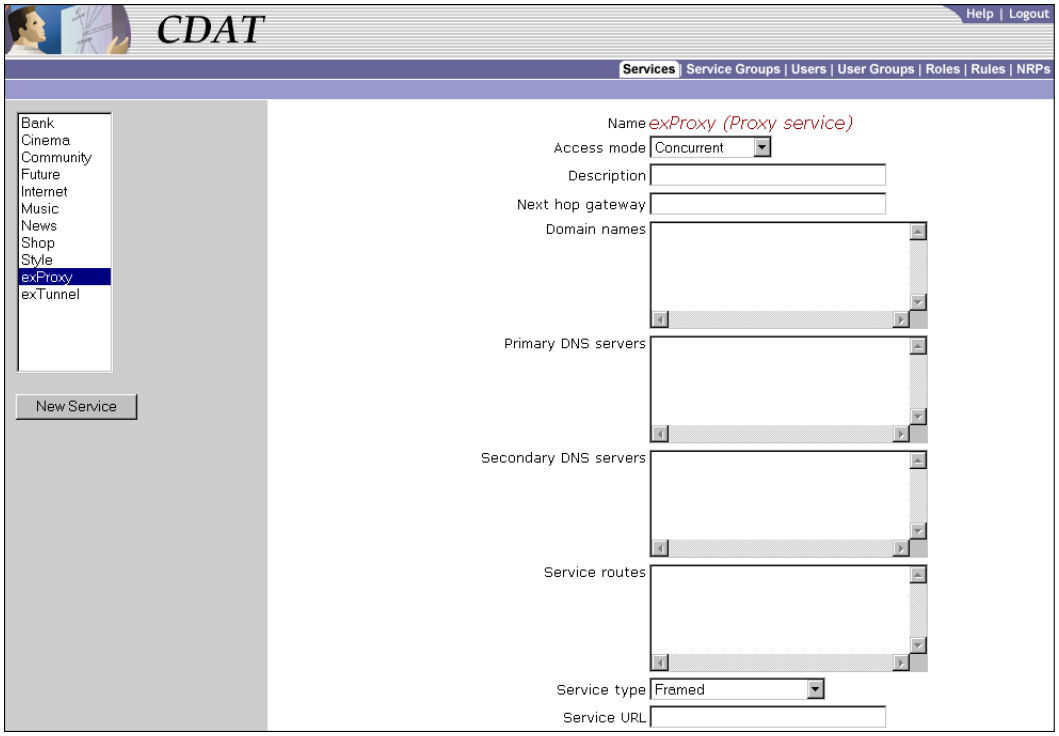
- Change the services that are subscribed
- Change account details, such as address information and passwords
- Create subaccounts for other family members

In an SESM system, *service profiles* and *subscriber profiles* contain information needed by the SESM web application and the SSG. Many of the attributes that define the service and subscriber profiles are derived from the RADIUS attributes that are used when a RADIUS server stores this information. For information on the interactions between the SSG software and the RADIUS service and subscriber profiles, see the *Cisco 6400 Feature Guide*.

CDAT

In an SESM system, CDAT is a web application that the service-provider administrator uses to create and maintain subscriber profiles, service profiles, and policy roles and rules in an LDAP directory. The CDAT web application consists of a set of windows that allow the administrator to create and update the subscriber, service, and policy objects and attributes that are stored in the directory. The CDAT expert interface allows the service-provider administrator to manage services, service groups, users, user groups, roles, rules, and Node Route Processor (NRP) information. Figure 1-1 shows part of the CDAT expert interface window for managing services.

Figure 1-1 CDAT Expert Interface

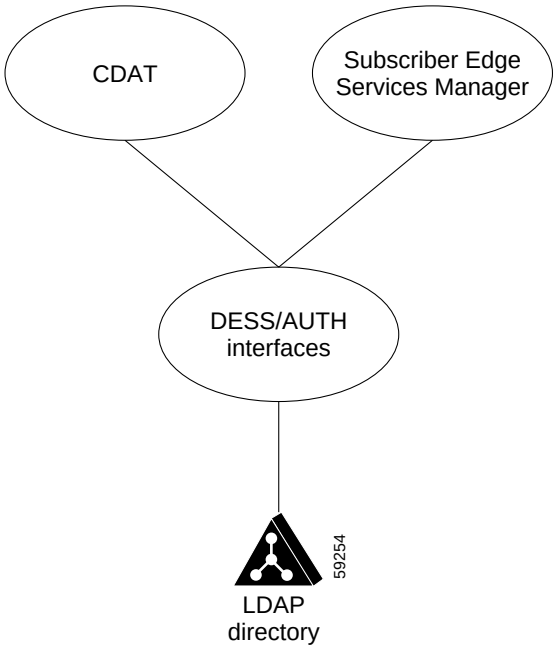


DESS/AUTH

In an SESM system, Cisco Subscriber Policy Engine (SPE) and its DESS/AUTH component provide the SESM and CDAT web applications with a set of Java class libraries and application programming interfaces for subscriber authentication, authorization, and account management. The DESS/AUTH class libraries use Lightweight Directory Access Protocol (LDAP) for directory queries. As shown in Figure 1-2, SESM and CDAT use the DESS/AUTH programming interfaces to access one or more LDAP directories where the subscriber, service, and policy information is stored.

DESS/AUTH uses a data model that is scalable and data-store independent. The subscriber, service and policy information is stored in an LDAP-compliant directory such as Novell Directory Services eDirectory. The service-provider administrator installs DESS/AUTH schema extensions in each LDAP directory that is used with SESM. For fault tolerance, the directories are typically partitioned and replicated.

Figure 1-2 DESS/AUTH Interfaces to an LDAP Directory



After the service-provider administrator uses CDAT to enter service and subscriber information into the LDAP directory and the subscriber logs on to the SESM web application, the SESM software obtains the subscriber's account and service information using the DESS/AUTH interfaces. Services for a subscriber can be dynamically subscribed or unsubscribed. If the subscriber chooses a service to subscribe to, the service is immediately available for selection.

Role Based Access Control

DESS/AUTH employs Role Based Access Control (RBAC) for subscriber authentication and authorization to services. With RBAC, the service provider manages access to resources at a level that corresponds closely to the business requirements of the application. For example, with SESM, the business requirements dictate that access to service subscription be controlled.

RBAC allows management of subscribers at the group level. Subscribers with common service and management requirements can be managed as a group. This approach is in contrast to managing each subscriber individually, a model that adds significant overhead to subscriber and service management.

When the service-provider administrator creates a subscriber, the administrator assigns the subscriber to a user group. Each user group is then made an occupant of one or more roles. The roles define the privileges that are permitted to occupants of that role. For a subscriber, the privileges usually involve authorization to subscribe to and unsubscribe from services.

Thus for the Cisco SESM, RBAC provides role-based access to services. RBAC privileges for a user group of subscribers usually also include permission to update certain account information such as passwords and to create subaccounts.

The RBAC data model can be quite complex. CDAT user interfaces for RBAC are designed specifically for creating and managing subscriber, service, and access policy information. CDAT removes much of the complexity by providing web-based user interfaces to simplify subscriber and service management.

RBAC Terminology

The service-provider administrator needs to understand some SESM and RBAC-related terms in order to use CDAT to manage subscriber and service information. The following terms are used for the objects that the administrator can manage using CDAT.

- *User*—An entity for which the administrator has created a user account in an LDAP directory. In the CDAT context, users are, in general, either subscribers or administrators.
  - A *subscriber* uses an SESM web application to subscribe to and select services.
  - An *administrator* manages the objects and attributes in the LDAP directory. With SESM and CDAT, administrators have varying responsibilities and, therefore, varying privileges. For information on the categories of administrators, see the "Creating and Updating Users and User Groups" section on page 2-19.
- *User group*—A set of users. The resources that a user group has access to can be managed at the group level. For example, the set of users in a user group of subscribers can be given access to a new service or service group.
- *Resource*—Something to which access needs to be controlled. With CDAT, resources include services, LDAP directory objects and attributes, and LDAP directory containers.
- *Service*—A resource that a subscriber can subscribe to or unsubscribe from.
- *Service group*—A set of services. A user group of subscribers can given access to the services in a service group.
- *Role*—A set of associated privileges. User groups can be made occupants of one or more roles. A role may be granted multiple privileges.
- *Rule*—The conditions under which a role is associated with one or more specified resources. With a rule, the administrator also defines the resources that can be accessed by role occupants and specifies the roles affected by the rule.

CDAT-RBAC Example

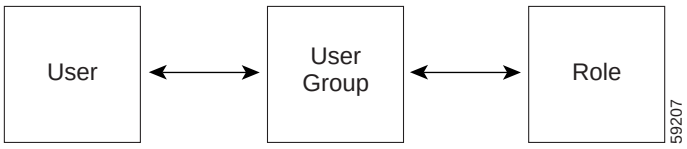
The following is a simplified example of how an administrator manages service, subscriber, and policy objects using CDAT. In this simple scenario, the service-provider administrator creates subscribers and controls at the group level the services that the subscribers can access. The administrator uses CDAT initially to create the following subscriber and service objects in an LDAP directory:

- Users (subscribers)
- A user group to which the subscribers are made members
- Services

Users, User Groups, and Roles

After creating users, a user group, and services, the administrator uses CDAT to define a role granting subscribe privileges and makes the user group of subscribers a role occupant. The subscribers now have the privileges associated with the role. Figure 1-3 shows the relationship between the users, the user group, and the role.

Figure 1-3 Users, User Groups, and Roles



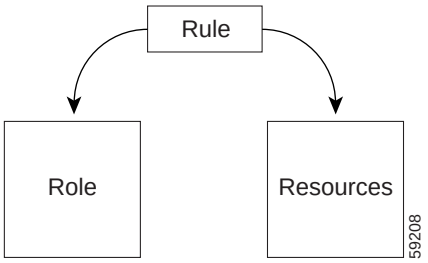
The administrator makes a user a member of a user group and makes the user group an occupant of a role that has subscribe privileges.

Rules

Roles and rules institute a service provider's policies. Each rule defines the set of conditions under which a role is associated with one or more resources, such as services. The service-provider administrator next uses the CDAT expert interface to define a rule specifying that the role with subscribe privileges is affected by the rule. The rule also lists the resources (services) that role occupants can access. Figure 1-4 shows how a rule links a role and one or more resources.

Figure 1-4 Rules

A rule associates the role with one or more resources (services).



After a framework of users, user groups, services, roles, and rules is established, the main service-provider administrative tasks are creating users and adding users to user groups. With RBAC and CDAT, no user-by-user access control modifications need to be made. Bulk administration of users, services, and privileges makes service and subscriber provisioning simple and fast.

Bulk Provisioning

SESM subscriber, service, and policy objects that exist in an LDAP directory can be exported to an LDAP Directory Interchange Format (LDIF) file and then imported into another LDAP directory where the DESS schema extensions have been installed. The classes and attributes that you can import include those for any object created with CDAT: services, service groups, users, user groups, roles, rules, and NRPs.

Bulk provisioning for a new set of subscribers can also be accomplished through the use of an LDIF file. The user accounts for a set of subscribers can be created in an LDIF file, which is an ASCII text file that can be edited with a text editor or written to with a program or script that the service provider creates. The sample LDIF files located in the *install_dir*\dess-auth\schema\samples directory provide examples of the DESS/AUTH format for entries in the LDIF file. For information on the DESS/AUTH classes and attributes, see Appendix B, "DESS/AUTH Schema Extensions."

To convert an existing set of RADIUS-formatted subscriber profiles and service profiles for use with an LDAP directory, the service provider must translate the RADIUS profiles (for example, from a MERIT RADIUS file) to the DESS/AUTH format for entries in an LDIF file. The translation can be accomplished by a program or script that the service provider creates. The LDIF file can then be imported into an LDAP directory where the DESS schema extensions have been installed.

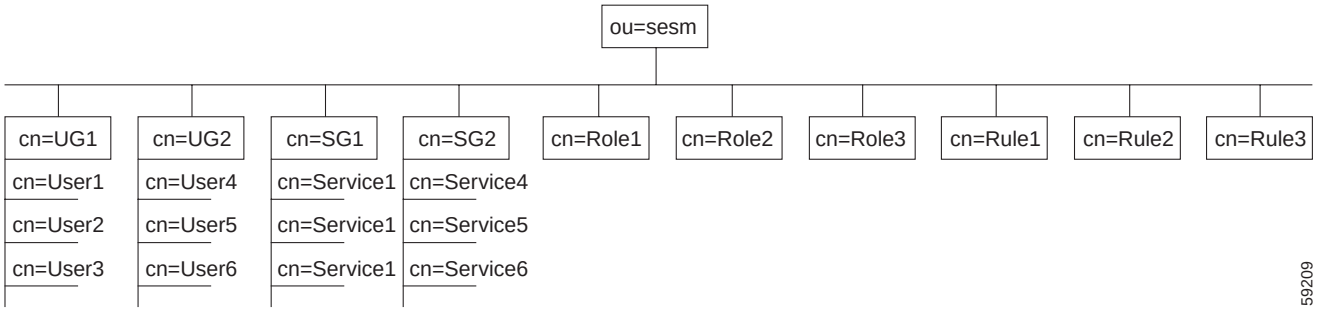
For information on LDAP directory import and export facilities such as **ldapmodify**, see the documentation from the directory vendor.

Directory Tree Structure

The directory tree structure currently used by CDAT makes use of multivalued attributes, rather than organizational units, for user groups and service groups. When the administrator creates a user group or service group, CDAT creates the group as an object having multivalued attributes. Figure 1-5 shows how a directory tree can use multivalued attributes for user groups and service groups. The sample directory tree contains the following objects:

- Two user groups (UG1 and UG2)
- Two service groups (SG1 and SG2)
- Three roles
- Three rules

Figure 1-5 Directory Tree Structure for CDAT



The structure of the underlying LDAP objects created by CDAT is a design choice and not a requirement. CDAT, not the service-provider administrator, creates the structure beneath the Organizational Unit (in this example, ou=sesm). With CDAT, the structure of the underlying LDAP objects is transparent to the administrator though an administrator could view the structure with an object-management tool like Novell Console One.

Learning about CDAT and DESS/AUTH

Table 1-1 shows where you can find more information about specific CDAT topics.

Table 1-1 CDAT Reading Path

For information on this topic	Read this
Overview of CDAT and RBAC	Chapter 1, "CDAT Overview" in this document
Installing and configuring CDAT including: • Configuring logging and debugging for CDAT • Installing the DESS/AUTH schema extensions and the sample RBAC objects (predefined roles and rules) into an LDAP directory	*Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide*
Using the CDAT expert interface	Chapter 2, "CDAT Expert Interface" in this document
Configuring the Service Selection Gateway (SSG)	*Cisco 6400 Feature Guide* *Cisco 6400 Command Reference* *Cisco 6400 Software Setup Guide*
Understanding the predefined roles and rules	Appendix A, "Predefined Roles and Rules" in this document
Understanding the DESS/AUTH schema	Appendix B, "DESS/AUTH Schema Extensions" in this document
Understanding the translations that the RADIUS-DESS Proxy (RDP) server performs for service-profile attributes	Appendix C, "RDP Service-Profile Translation" in this document

If you want general information on Role Based Access Control, the RBAC/Web has information on the use of RBAC in other contexts at:

`http://hissa.nist.gov/project/rbac.html`

For information on your LDAP directory, see the documentation from the directory vendor.