



## CDAT Overview

---

The Cisco Distributed Administration Tool (CDAT) provides a set of web-based facilities that allow the service-provider administrator to perform two different sets of tasks:

- Remote managing and monitoring of Cisco Subscriber Edge Services Manager (Cisco SESM) applications
- Managing subscriber, service, and policy information used by Cisco SESM and the Service Selection Gateway (SSG)



Note

---

This guide focuses on the second set of tasks (managing subscriber, service, and policy information) and provides only a brief overview of the remote management and monitoring capabilities of CDAT. For information on configuring and using the remote management and monitoring capabilities of CDAT, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

---

## Remote Managing and Monitoring of SESM Applications

CDAT provides remote management and monitoring for the attributes of SESM applications

### Remote Managing

CDAT allows the deployment administrator to monitor and change the configuration attributes in a running SESM application. It also provides a way to optionally store changes in the application configuration files so that the changes persist across application restarts.

From the CDAT web-based GUI interface, administrators can view and change values for most attributes in the configuration files for SESM portals, RADIUS Data Proxy (RDP), Cisco Security Policy Engine (SPE), and CDAT. The tool does not permit changes to attributes if the change could disrupt the application. The application port, for example, cannot be changed.

Each SESM application has its own instance of a management console, known as the *Agent View*. From the CDAT home page ([Figure 1-1](#)), you can access the Agent Views for all running SESM applications. An application's Agent View lists all of the management interfaces (MBeans) for the running application. The management interface is the set of information and controls that a management application needs to operate on the resource.

Figure 1-1 CDAT Home Page



Using CDAT for remote configuration, the deployment administrator can perform the following actions on attribute values:

- View current attribute values for the running application, including many read-only attributes useful for application monitoring.
- Apply changes to most Read/Write attributes. Applied changes take immediate effect on the running application.
- Store changes in the application's configuration file. Stored changes persist for future restarts of the application.
- Undo (revert) changes sequentially from the most recent store to the first store made in the session.

For information on configuring and using the remote management capabilities of CDAT, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

## Remote Monitoring

Each SESM application's management interfaces (MBeans) include read-only attributes that contain metrics, counters, and descriptions. Using CDAT, deployment administrators can view these read-only attributes to:

- Monitor SESM web portals to ensure that they are responding to HTTP requests
- Monitor RDP to ensure that it is responding to RADIUS requests
- Obtain descriptions and formatted array values
- Collect memory and activity metrics

For information on configuring and using the remote monitoring capabilities of CDAT, see the *Cisco Subscriber Edge Services Manager Solutions Guide*.

# Managing Subscriber, Service, and Policy Information

CDAT allows the service-provider administrator to create and maintain the subscriber, service, and policy information used by the Cisco Subscriber Edge Services Manager 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 in LDAP mode and CDAT use the Cisco Security Policy Engine (SPE) and Role Based Access Control (RBAC) for authentication, authorization, and account and service management. With CDAT, SPE, and RBAC, most account-management tasks are accomplished at the group level. CDAT, SPE, 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:

- [SESM, CDAT, and SPE, page 1-3](#)
- [Role Based Access Control, page 1-5](#)
- [Bulk Provisioning, page 1-8](#)
- [Directory Tree Structure, page 1-8](#)
- [Learning about CDAT and SPE, page 1-9](#)

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

## SESM, CDAT, and SPE

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

- SESM
- CDAT
- SPE

For a complete description of an SESM system, see the *Cisco Subscriber Edge Services Manager 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 Service Selection Gateway documentation that is available on Cisco Connection Online.

## 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 1-2](#) shows part of the CDAT expert interface window for managing services.

*Figure 1-2 CDAT Expert Interface*

The screenshot displays the CDAT Expert Interface for configuring a service. The interface includes a navigation menu on the left with categories like Bank, Cinema, Community, Future, Internet, Music, News, Shop, Style, exProxy (selected), and exTunnel. A 'New Service' button is located below the menu. The main content area shows the configuration for the selected service, 'exProxy (Proxy service)'. The configuration fields include:

- Name: exProxy (Proxy service)
- Access mode: Concurrent (dropdown)
- Description: (text input)
- Next hop gateway: (text input)
- Domain names: (list box)
- Primary DNS servers: (list box)
- Secondary DNS servers: (list box)
- Service routes: (list box)
- Service type: Framed (dropdown)
- Service URL: (text input)

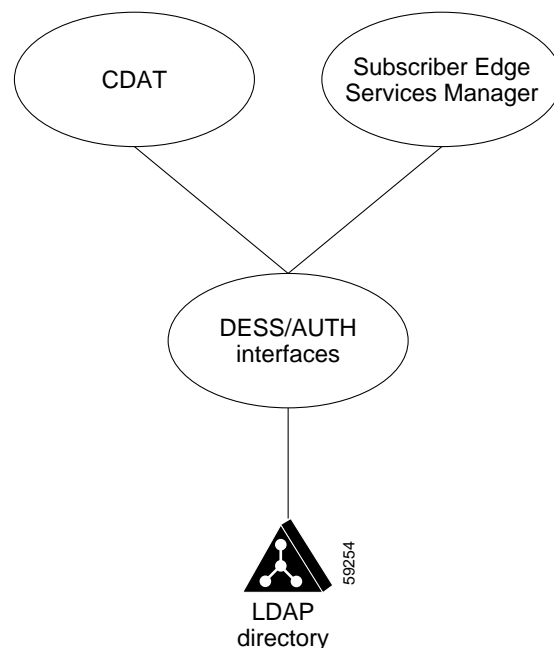
The interface also features a 'Help | Logout' link in the top right corner and a vertical ID number '59255' on the right side.

## SPE

In an SESM system, Cisco Security Policy Engine (SPE) and its Directory Enabled Service Selection and Authorization (DESS/AUTH) component provide the SESM and CDAT 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 1-3](#), 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.

SPE and DESS/AUTH use 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 or Sun ONE iPlanet Directory Server. The service-provider administrator installs SPE schema extensions in each LDAP directory that is used with SESM. For fault tolerance, the directories are typically partitioned and replicated.

*Figure 1-3 DESS/AUTH Interfaces to an LDAP Directory*



After the service-provider administrator uses CDAT to enter service, subscriber, and policy 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

SPE 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 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 2-25](#).
- *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 be 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 and RBAC. 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

### CDAT-RBAC Example: 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 1-4](#) shows the relationship between the users, the user group, and the role.

*Figure 1-4 Users, User Groups, and Roles*



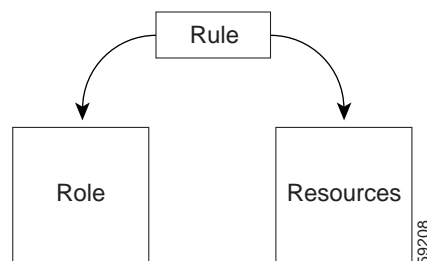
The administrator makes a user a member of a user group and makes the user group an occupant of a role that has subscribe privileges.

### CDAT-RBAC Example: 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 1-5](#) shows how a rule links a role and one or more resources.

*Figure 1-5 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 SPE 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 SPE format for entries in the LDIF file. For information on the SPE classes and attributes, see [Appendix B, “SPE 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 SPE 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 SPE 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

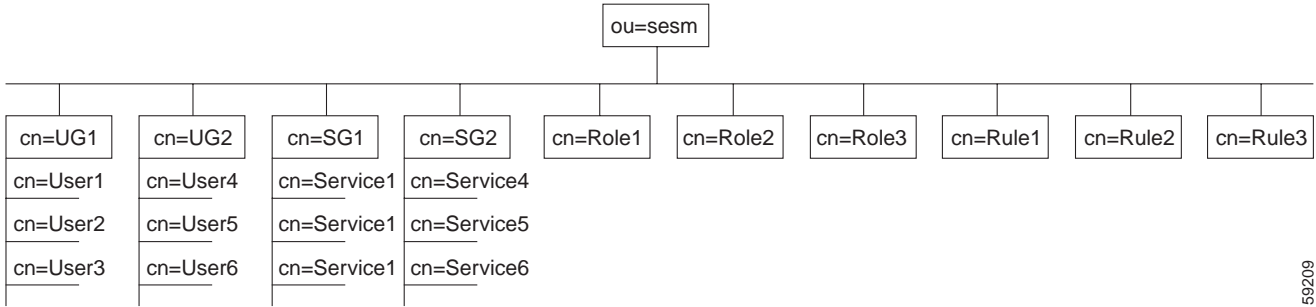
The directory tree structure currently used by CDAT makes use of multivalued attributes, rather than organizational units, for user groups and service groups. When the administrator creates a user group or service group, CDAT creates the group as an object having multivalued attributes.

[Figure 1-6](#) 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 1-6 CDAT Directory Tree Structure



59209

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 SPE

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	<a href="#">Chapter 1, “CDAT Overview”</a> in this document
Installing and configuring CDAT including: <ul style="list-style-type: none"> <li>• Configuring CDAT for remote managing and monitoring of SESM applications</li> <li>• Configuring CDAT for managing subscriber, service, and policy information</li> <li>• Installing the SPE schema extensions and the sample RBAC objects (predefined roles and rules) into an LDAP directory</li> </ul>	<i>Cisco Subscriber Edge Services Manager Installation and Configuration Guide</i>
Using CDAT for remote managing and monitoring of SESM applications	<i>Cisco Subscriber Edge Services Manager Installation and Configuration Guide</i>
Using the CDAT expert interface for managing subscriber, service, and policy information	<a href="#">Chapter 2, “CDAT Expert Interface”</a> in this document
Configuring the Service Selection Gateway (SSG)	<i>Service Selection Gateway</i> and <i>Cisco Subscriber Edge Services Manager Installation and Configuration Guide</i>
Understanding the predefined roles and rules	<a href="#">Appendix A, “Predefined Roles and Rules”</a> in this document

*Table 1-1 CDAT Reading Path (continued)*

For information on this topic	Read this
Understanding the SPE schema extensions	<a href="#">Appendix B, “SPE Schema Extensions”</a> in this document
Understanding the translations that the RADIUS Data Proxy (RDP) server performs for service-profile attributes	<a href="#">Appendix C, “RDP Service-Profile Translation”</a> 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.