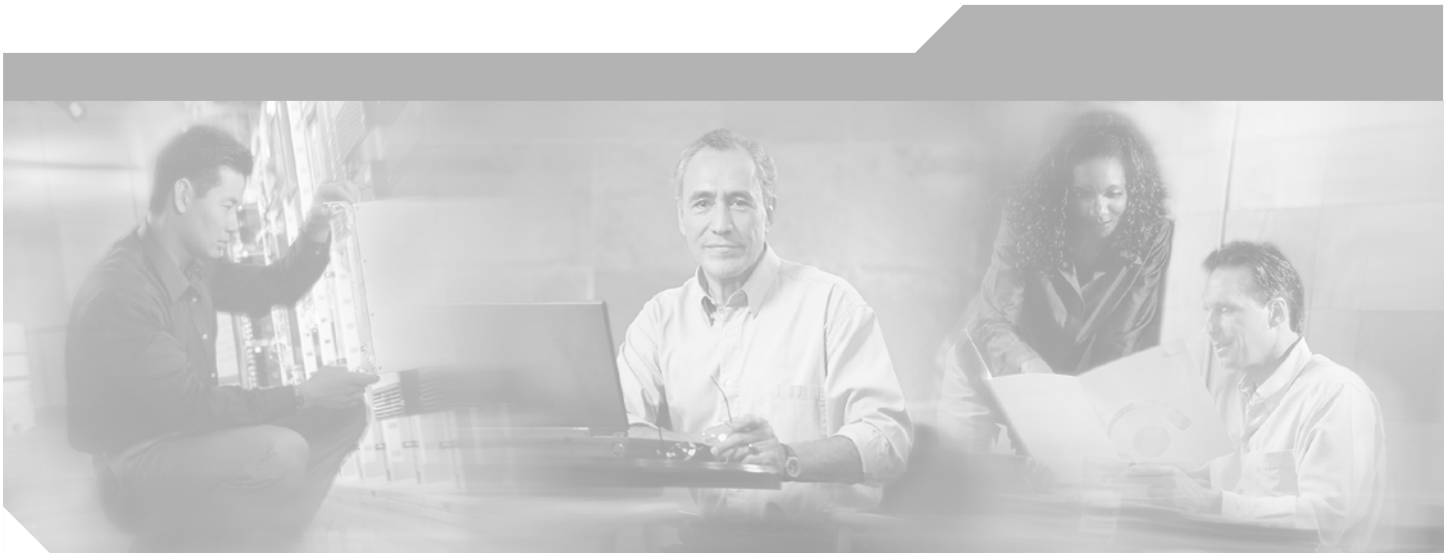


Cisco Distributed Administration Tool Guide

SESM Release 3.1(5) and SPE Version 1.11
August 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-2064-02

Cisco Distributed Administration Tool Guide

CONTENTS

About This Guide

This preface has information about the *Cisco Distributed Administration Tool Guide* and contains the following sections:

- Document Objectives
- Audience
- Document Organization
- Document Conventions
- Related Documentation
- Obtaining Documentation
- Obtaining Technical Assistance

Document Objectives

This guide explains how to use the Cisco Distributed Administration Tool (CDAT) to create and maintain the subscriber, service, and policy information used by the Cisco Subscriber Edge Services Manager (Cisco SESM). The guide documents the CDAT software that is part of Cisco SESM Release 3.1(5). The guide also provides information on the predefined roles and rules and Directory Enabled Service Selection and Authorization (DESS/AUTH) schema extensions.

Note 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*.

Audience

This guide is intended for service-provider administrators who are responsible for creating and maintaining the subscriber, service, and policy information in an LDAP directory. Another audience is service-provider network administrators who are responsible for configuring services on network devices.

Document Organization

This guide includes the chapters shown in the following table:

Chapter	Title	Description
Chapter 1	CDAT Overview	Provides an overview of the CDAT facility and Role Based Access Control (RBAC).
Chapter 2	CDAT Expert Interface	Describes how to use the CDAT expert interface.
Appendix A	Predefined Roles and Rules	Explains the predefined roles and rules that can be installed with the SPE software.
Appendix B	SPE Schema Extensions	Describes the LDAP directory schema extensions that are installed with the SPE software.
Appendix C	RDP Service-Profile Translation	Provides information on the translation that the RADIUS Data Proxy (RDP) server performs for the service-profile attributes that CDAT creates.
Index		

Document Conventions

The following conventions are used in this guide:

- **Boldface** font is used for commands and keywords.
- *Italic* font is used for elements such as a file name for which you supply a value.

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

The following documents available on Cisco Connection Online are relevant to CDAT:

- *Release Notes for the Cisco Subscriber Edge Services Manager Release 3.1(5)*
- *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*
- *Cisco Subscriber Edge Services Manager Web Developer Guide*
- *Cisco Subscriber Edge Services Manager Solutions Guide*
- *Service Selection Gateway*

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.

- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

CHAPTER 1

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:

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:

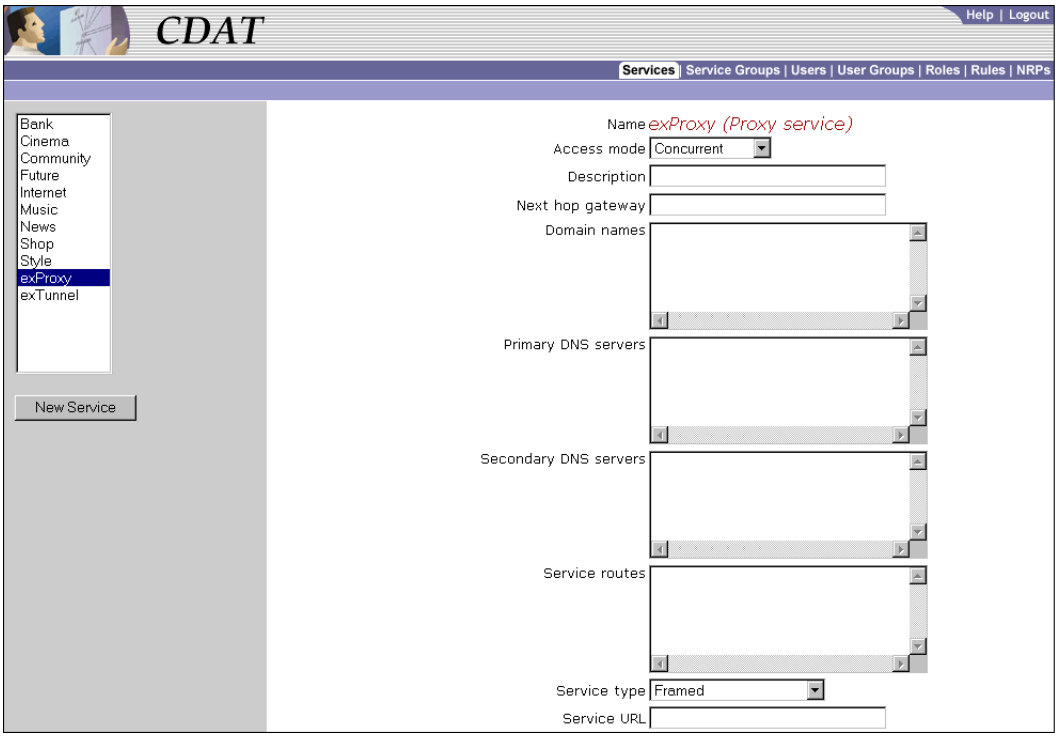
- Change the services that are subscribed
- Change account details, such as address information and passwords
- Create subaccounts for other family members

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



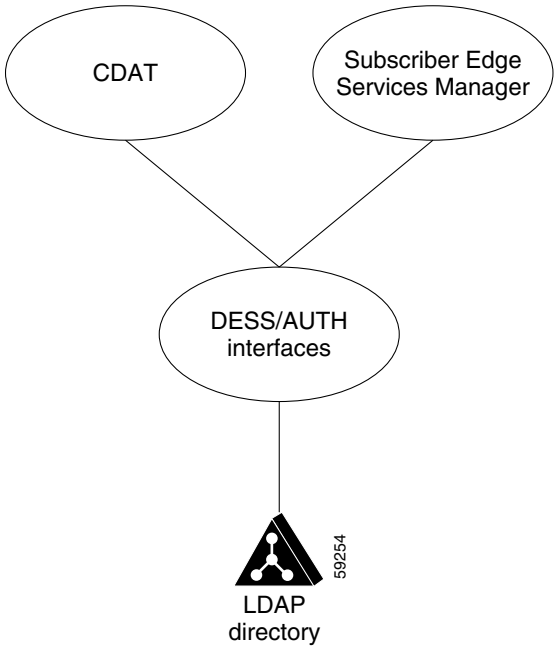
SPE

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 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 2-25.
- *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 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

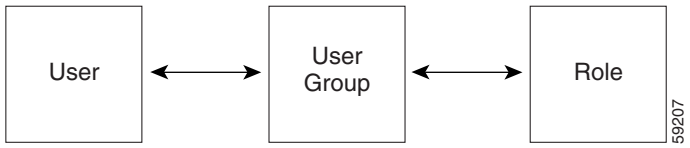
The following is a simplified example of how an administrator manages service, subscriber, and policy objects using CDAT and RBAC. In this simple scenario, the service-provider administrator creates subscribers and controls at the group level the services that the subscribers can access. The administrator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

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



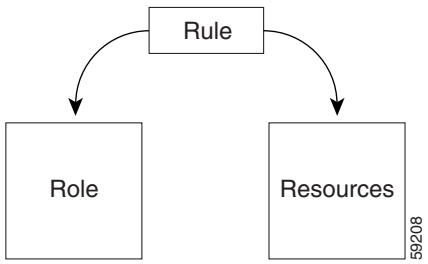
The administrator makes a user a member of a user group and makes the user group an occupant of a role that has subscribe privileges.

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.

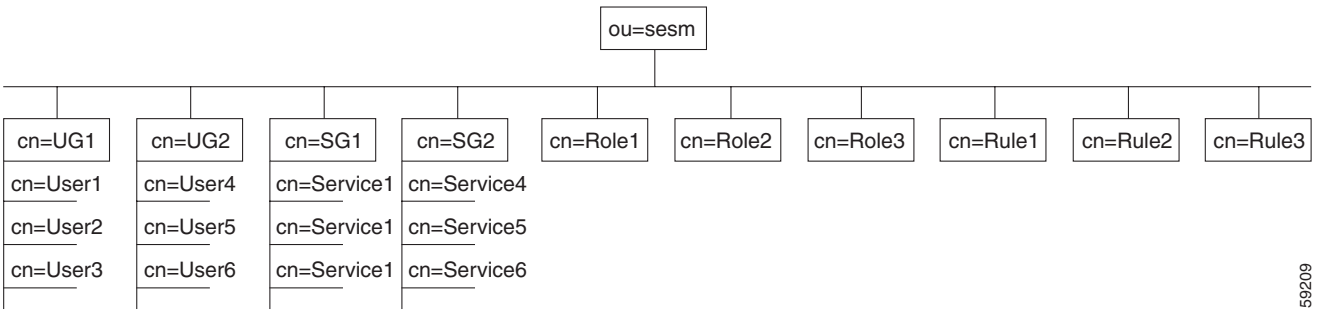
Directory Tree Structure

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



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	Chapter 1, "CDAT Overview" in this document
Installing and configuring CDAT including: • Configuring CDAT for remote managing and monitoring of SESM applications • Configuring CDAT for managing subscriber, service, and policy information • Installing the SPE schema extensions and the sample RBAC objects (predefined roles and rules) into an LDAP directory	*Cisco Subscriber Edge Services Manager Installation and Configuration Guide*
Using CDAT for remote managing and monitoring of SESM applications	*Cisco Subscriber Edge Services Manager Installation and Configuration Guide*
Using the CDAT expert interface for managing subscriber, service, and policy information	Chapter 2, "CDAT Expert Interface" in this document
Configuring the Service Selection Gateway (SSG)	*Service Selection Gateway* and *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*
Understanding the predefined roles and rules	Appendix A, "Predefined Roles and Rules" in this document
Understanding the SPE schema extensions	Appendix B, "SPE Schema Extensions" in this document
Understanding the translations that the RADIUS Data 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.

CDAT Expert Interface

The CDAT expert interface allows the service-provider administrator to create and maintain the objects and attributes for services, service groups, users, user groups, roles, rules, and Node Route Processor (NRP) information. Before using the CDAT expert interface, read the following:

- Role Based Access Control, page 1-5
- Using the CDAT Expert Interface: An Example, page 2-1
- Getting Started with the CDAT Expert Interface, page 2-3

The CDAT expert interface consists of a set of windows that allow the objects representing services, subscribers, and policy roles and rules to be created and maintained. The following sections describe how to use the CDAT expert interface to define service, subscriber, and policy information:

- Creating and Updating Services and Service Groups, page 2-11
- Creating and Updating Users and User Groups, page 2-25
- Creating and Updating Roles, page 2-41
- Creating and Updating Rules, page 2-48
- Creating and Updating NRP Information, page 2-51

In addition to creating services, subscribers, and other objects with CDAT, the SSG software must be correctly configured for the services that you create. For information on configuring services on the SSG, see the Service Selection Gateway documentation that is available on Cisco Connection Online (www.cisco.com).

Using the CDAT Expert Interface: An Example

As a simple example of the tasks that an administrator performs when using the CDAT interface, consider the tasks needed to create a user with a set of privileges to access certain resources.

Because the steps outlined below start from the very beginning and assume that no user groups, roles, or rules exist, the tasks may seem a bit complicated. After becoming familiar with RBAC and CDAT, these tasks become fairly intuitive. More importantly, this set of tasks is only performed once—when the directory objects are created for the first time.

Creating Services, Users, User Groups, Roles, and Rules

The following example outlines the steps that you perform to create a user who is a subscriber to a set of "Gold" services. The steps for this task are as follows:

1. With the Services window, create one or more services (the Gold services that Gold subscribers can access).
2. With the User Groups window, create a user group (GoldSubscriberGroup) for the users who will be granted access to the Gold services.
3. With the Users window, create the user (Joan) and make the user a member of the user group GoldSubscriberGroup.
4. With the Roles window, create a role (GoldSubscriberRole). The role defines the privileges the members of the GoldSubscriberGroup have.
   a. Define the role's privileges to include the rights to subscribe to and unsubscribe from Gold services.
   b. Make the user group GoldSubscriberGroup a subject (occupant) of the role GoldSubscriberRole.
5. With the Rules window, create a rule (GoldSubscriberRule). The rule will grant, to a specified role (GoldSubscriberRole), the privileges for a set of resources. For a Gold subscriber, the set of resources includes the Gold services.
   a. Specify the set of resources (the Gold services) that are defined for the rule.
   b. Associate the role GoldSubscriberRole with the rule GoldSubscriberRule.

When you complete the preceding steps, the privileges to subscribe to or unsubscribe from the set of Gold services are granted to the user group GoldSubscriberGroup because it is a subject of the GoldSubscriberRole. The user Joan has the privileges defined by the GoldSubscriberRole because she is a member of the GoldSubscriberGroup. The GoldSubscriberRule is applied to the specified services (the Gold services) and it associates GoldSubscriberRole with these services.

Administering Large Numbers of Users

The greatest benefit to using CDAT is that it allows for bulk administration of users. Because the preceding example started from the beginning and created all needed objects for granting a subscriber the privileges to access a set of services, the steps might seem a bit complicated.

However, once these objects (a user group, a role for the group, and a rule granting privileges to resources) are in place, creating a thousand or ten thousand additional subscribers who are members of the GoldSubscriberGroup is simple and involves two steps for each subscriber:

1. Create the user—the new subscriber.
2. Specify that the user is a member of the GoldSubscriberGroup.

In addition to granting access to resources, you can perform other service-provider administration tasks at the group level. For example, because you have already defined the underlying structure of user groups, roles, and rules, adding or removing resources (services) that group members can access, and modifying the set of privileges for group members can be accomplished at the user group level.

With RBAC and CDAT, no user-by-user access control modifications need to be made. Bulk administration of users, services, and privileges makes subscriber provisioning simple and fast.

Getting Started with the CDAT Expert Interface

This section provides some information about getting started with the CDAT expert interface:

For information on installing, configuring, and starting CDAT, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*

Using CDAT for the First Time to Manage an LDAP Directory

This section describes the following:

Note Before using CDAT, make sure that cookies are enabled in your browser. CDAT requires a browser that allows cookies.

Logging into CDAT for the First Time

To log in to CDAT for the first time to manage an LDAP directory, use the `admin` user name and the password of the directory administrator for the Organization and Organizational Unit where SESM is located. This is the user name and password that were specified when the directory was installed.

Note During the directory installation and the CDAT installation, the directory administrator must be specified as the `admin` user ID.

To use the `admin` user name as the first-time CDAT administrator, you must do the following when installing the directory server and the CDAT software:

1. When you install the directory server, set up an `admin` user with the needed permissions to access and create objects in the directory container (Organization Unit and Organization) where the SPE schema extensions and initial RBAC objects will be installed.
2. When you install the CDAT software, select **Install RBAC** to install the initial RBAC objects. When you select **Install RBAC**, the CDAT installation software *expects to find* an `admin` user ID so that it can grant that user the needed administrator privileges.

After you logged into CDAT as the `admin` user, you should create a CDAT administrator user who belongs to a user group that has the administrative privileges to set up the objects and attributes for services, subscribers, policy roles and rules, and so on. Because the `admin` user is a directory administrator for the SESM container, that administrator can create roles, rules, and user groups for CDAT administrators to whom the `admin` user can grant differing privilege levels.

After you install the RBAC objects, you can use the SUPERVISOR_ROLE and SUPERVISOR_RULE when defining a user group for administrators. For information on the privileges that are needed by a CDAT administrator, see the "Creating and Updating Roles" section on page 2-41.

Installing CDAT Sample Data

The CDAT sample data is contained in one LDIF file, DESSusecasedata.ldf file, which is located in the *install_dir*\dess-auth\schema\samples directory.

Note A differently formatted DESSusecasedata.ldf file is installed depending on the operating system. For example, the Windows-specific sample data file contains DOS-format line endings. To install a Windows sample data file on a directory server on UNIX, or a UNIX sample data file on a directory server on Windows, use a file-format conversion utility, such as **dos2unix** or **unix2dos**, to convert the DESSusecasedata.ldf file to the required format.

You use the **ldapmodify** command to install the DESSusecasedata.ldf sample data. The examples that follow show the **ldapmodify** command line that is used for NDS eDirectory and for iPlanet Directory Server.

NDS eDirectory Example

For the following eDirectory example, assume that:

- 192.10.68.12 is the address of the server where the directory is located.
- 389 is the port number where the directory server listens.
- The directory administrator (with the password "cisco") is defined as follows in the NDS directory server configuration file:
  - Admin Name and Context: cn=admin.ou=sesm.o=cisco
- The following container exists in the directory:
  - Tree Name: sesm
  - Context: ou=sesm.o=cisco

The following **ldapmodify** command installs the sample data:

```
ldapmodify -h 192.10.68.12 -p 389 -c -v -D "cn=admin,ou=sesm,o=cisco" -w cisco
     -f DESSusecasedata.ldf
```

iPlanet Directory Server Example

For the following iPlanet example, assume that:

- 192.10.68.12 is the address of the server where the directory is located.
- The administrator (with the password "cisco") with the required permissions to create and modify objects in the SESM container is defined as follows in the iPlanet configuration:
  - name: uid=admin,ou=sesm,o=cisco
- The following container exists in the directory:
  - Tree Name: sesm
  - Context: ou=sesm.o=cisco

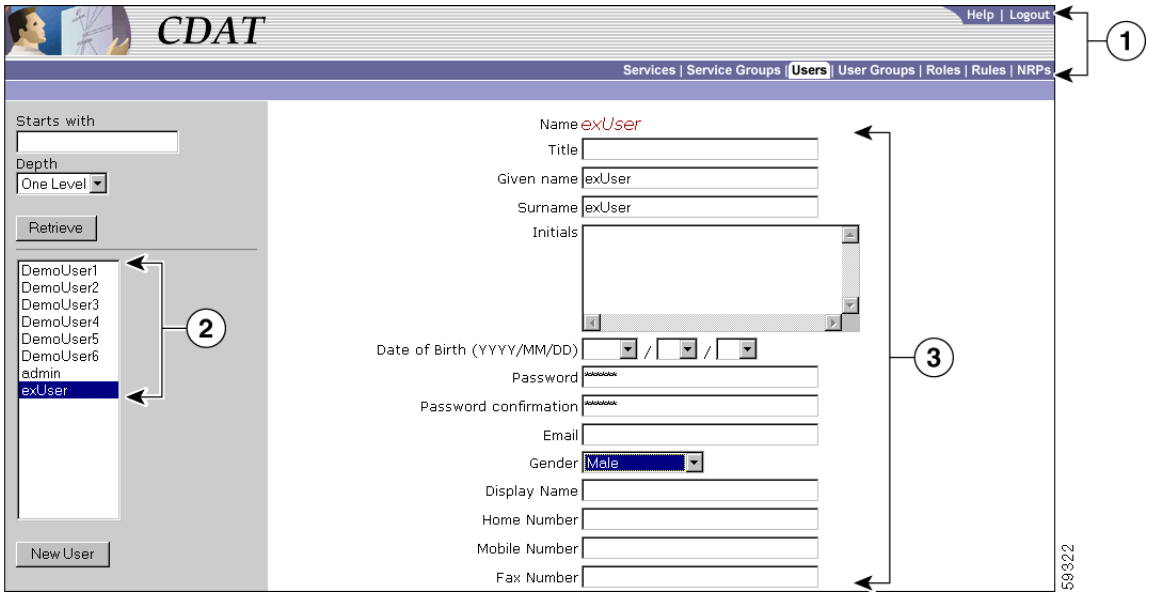
The following **ldapmodify** command installs the sample data:

```
ldapmodify -h 192.10.68.12 -c -v -D “uid=admin,ou=sesm,o-cisco” -w cisco
```

Using the CDAT Expert Interface

The CDAT expert interface allows you to create or update information for services, service groups, users, user groups, roles, rules, and NRPs. Figure 2-1 shows the Users window of the expert interface.

Figure 2-1 CDAT Expert Interface: Object Management Window



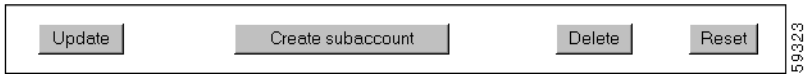
1	Navigation Bar
2	Navigation List
3	Object Details

In the CDAT expert interface, each object-management window contains these areas:

- **Navigation Bar**—Click a tab (for example, **Services**) to display the top-level management window for that task.
  - Click **Help** to display CDAT Help.
  - Click **Logout** to end the CDAT session.
- **Navigation List**—Click an object name in the list to display the attributes for that object. Or click the **New** button (for example, **New User**) to create a new object. The Users window has two additional navigation-list controls that let you choose the objects that CDAT displays in the list:
  - The Starts with box allows you to enter all or part of the name for user objects that CDAT displays.
  - The Depth box allows you to display user accounts in nested directory containers. It is not currently used.
  - Click the **Retrieve** button to start the search for the user objects specified.
- **Object Details**—For the current object selected in the Navigation List or for a new object created with the New button, CDAT displays the object's attributes. In the Object Details area, you can define attributes for a new object or modify attributes for an existing object.

The bottom of the Object Details area contains a set of buttons. Figure 2-2 shows the buttons that appear at the bottom of the Users window.

Figure 2-2 CDAT Expert Interface Buttons



The buttons shown in Figure 2-2 perform the following actions:

- **Update**—Submits the information that you have specified. CDAT modifies the LDAP directory attributes for the object and, if successful, displays the updated attributes.
- **Create subaccount** (Users window only)—Creates a subaccount user object.
- **Delete**—Deletes the object from the LDAP directory.
- **Reset**—For each attribute where you have modified an existing value, resets the value to what it was before the modification.

Defining Local RADIUS Attributes

The Local RADIUS Attribute box allows you to specify standard RADIUS attribute names and Cisco SSG vendor-specific attributes, including Cisco attribute-value pairs (Cisco AV pairs). The Local RADIUS Attributes box appears in the following CDAT windows:

- Users
- User Groups
- Services
- Service Groups
- NRPs

Tip The Local RADIUS Attribute box allows you to define an attribute and value that *does not* appear in the boxes (fields) of a CDAT window. For example, the Users window does not have a box for a RADIUS attribute Calling-Station Id. You can enter this attribute in the Local RADIUS Attributes box. As another example, most Cisco AV pairs do not appear in the boxes of a CDAT window. You can enter Cisco AV pairs in the Local RADIUS Attributes box.

For information on RADIUS attributes that appear in the boxes of the Services window, see Appendix C, "RDP Service-Profile Translation."

Using Predefined RADIUS Attributes

CDAT and other SESM applications internally predefine the standard RADIUS attributes and the Cisco SSG vendor-specific attributes (VSAs).

- Table 2-1 lists the predefined, standard RADIUS attribute names.
- Table 2-2 shows the predefined Cisco SSG VSAs.

You can use these predefined RADIUS attributes in subscriber and service profiles whether or not they are defined in an attribute dictionary. (With CDAT and LDAP mode, the attribute dictionary is in the RADIUSDictionary MBean used by the RDP application.)

Table 2-1 Standard RADIUS Attributes Predefined in SESM Applications

RADIUS Attribute Names[1]		
USER_NAME	SESSION_TIMEOUT	ACCT_LINK_COUNT
USER_PASSWORD	IDLE_TIMEOUT	ACCT_INPUT_GIGAWORDS
CHAP_PASSWORD	TERMINATION_ACTION	ACCT_OUTPUT_GIGAWORDS
NAS_IP_ADDRESS	CALLED_STATION_ID	EVENT_TIMESTAMP
NAS_PORT	CALLING_STATION_ID	CHAP_CHALLENGE
SERVICE_TYPE	NAS_IDENTIFIER	NAS_PORT_TYPE
FRAMED_PROTOCOL	PROXY_STATE	PORT_LIMIT
FRAMED_IP_ADDRESS	LOGIN_LAT_SERVICE	LOGIN_LAT_PORT
FRAMED_IP_NETMASK	LOGIN_LAT_NODE	ARAP_PASSWORD
FRAMED_ROUTING	LOGIN_LAT_GROUP	ARAP_FEATURES
FILTER_ID	FRAMED_APPLETALK_LINK	ARAP_ZONE_ACCESS
FRAMED_MTU	FRAMED_APPLETALK_NETWORK	ARAP_SECURITY
FRAMED_COMPRESSION	FRAMED_APPLETALK_ZONE	ARAP_SECURITY_DATA
LOGIN_IP_HOST	ACCT_STATUS_TYPE	PASSWORD_RETRY
LOGIN_SERVICE	ACCT_DELAY_TIME	PROMPT
LOGIN_TCP_PORT	ACCT_INPUT_OCTETS	CONNECT_INFO
REPLY_MESSAGE	ACCT_OUTPUT_OCTETS	CONFIGURATION_TOKEN
CALLBACK_NUMBER	ACCT_SESSION_ID	EAP_MESSAGE
CALLBACK_ID	ACCT_AUTHENTIC	MESSAGE_AUTHENTICATOR
FRAMED_ROUTE	ACCT_SESSION_TIME	ARAP_CHALLENGE_RESPONSE
FRAMED_IPX_NETWORK	ACCT_INPUT_PACKET	ACCT_INTERIM_INTERVAL
STATE	ACCT_OUTPUT_PACKETS	NAS_PORT_ID
CLASS	ACCT_TERMINATE_CAUSE	FRAMED_POOL
VENDOR	ACCT_MULTI_SESSION_ID	

1. A hyphen (-) can replace the underscore (_) in RADIUS attribute names. The attribute names are not case-sensitive.

Table 2-2 Cisco SSG VSAs Predefined in SESM Applications

RADIUS Attribute	Vendor ID	Subattribute	Name[1]	Type
26	9	1	CISCO-AV	String
26	9	250	ACCOUNT-INFO	String
26	9	251	SERVICE-INFO	String
26	9	252	COMMAND-CODE	BINARY
26	9	253	CONTROL-INFO	String

1. The hyphen (-) and underscore (_) are interchangeable in RADIUS attribute names. The attribute names are not case-sensitive.

To specify one of the predefined RADIUS attributes in CDAT's Local RADIUS Attributes box, use the following form:

ATTRIBUTE_NAME:*attribute_value*

ATTRIBUTE_NAME is one of the predefined RADIUS attributes, and *attribute_value* is the value given for the attribute. A colon (:) separates the two elements. Two examples follow:

```
CALLING_STATION_ID:978123456

CISCO-AV:ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21
```

Using Dynamically Defined Attributes

In the Local RADIUS Attributes box, you can also dynamically define a new attribute when you first use the attribute in a profile. This feature is intended only for testing, demonstration, and development purposes. With CDAT, use the dynamic attribute feature only in the following circumstances:

- The SESM portal is running in Demo mode.
- The SESM portal is running in LDAP mode in a testing or development environment.

For information on dynamically defining a new attribute, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*

Other CDAT Expert Interface Considerations

Some other considerations that you should be aware of when using the CDAT expert interface are:

Name Space

All objects created with CDAT share the same name space. You cannot create a CDAT object (service, service group, user, user group, role, rule, or NRP) using the same name as an object of any of these types that already exists. If you try to create an object using a name already in use, CDAT displays a message that the object already exists and asks you to choose a new name.

Visibility of and Access to Objects

When a user logs into CDAT, the objects that CDAT displays and the objects and attributes that the user can create, delete, and modify are directly related to the user groups that the CDAT user is a member of and to the following:

- The privileges that the user has been granted as determined by the role occupancy of the user's user groups.
- The resources that the user has access to as determined by the rules that are associated with the roles.

As an example, assume a user does not have Cisco_Azn_Super privilege for managing roles and rules. If this user logs in, CDAT does not display any roles or rules in the Roles and Rules windows. To see and manage roles and rules using CDAT, this user must a member of a user group that has Cisco_Azn_Super privilege and must have access to the resources of the container Organization Unit under which the roles and rules reside.

User Passwords

CDAT and the DESS/AUTH software store the user password in Secure Hash Standard encrypted form. After a password is defined for a user account, CDAT displays each password field as a 25-character string, regardless of the length of the defined password. The password encryption does not allow the user or the CDAT administrator to clear the password. Once a password exists, attempting to enter an empty string for the password results in an exception. No update of the password occurs.

When a subaccount is created, the initial password is set to the user name for the subaccount. The password fields in CDAT display a 25-character string because the password is stored in an encrypted form.

Attribute Values and Inheritance

Some of the attributes that are in effect for a user or service profile are affected by inheritance.

When you define a service, service group, user, or user group, you can specify some attribute values at both the group level and the individual member level. When certain attribute values are specified at the user group or service group level, they are inherited by individual users and services that are group members. Table 2-3 lists the CDAT inheritable attributes.

Table 2-3 Inheritable Attributes

Inheritable Attribute	Where Used
Idle Timeout	Services, Service Groups, Users, and User Groups
Local RADIUS attributes	Services, Service Groups, Users, and User Groups
Session Timeout	Services, Service Groups, Users, and User Groups
Allow Create Sub-Account	Users and User Groups
Enable Single Sign-On	Users and User Groups
Home URL	Users and User Groups
Maximum Number of Sub-Accounts	Users and User Groups
Pool name	Users and User Groups
Primary Service	Users and User Groups
Service Filters	Users and User Groups
TCP Redirection Attributes	Users and User Groups

When a value for an inheritable attribute is specified for an individual user or service, that value takes precedence over a value that is specified at the group level or container level.

For example, you can specify Idle Timeout and Session Timeout values for a service and for a service group.

- If a timeout value is defined only at the service group level, individual services that are members of the group inherit that timeout value.

- If a timeout value is defined at both the service level and the service group level, the value specified at the service level has precedence.

To simplify the use of inheritable user and user group attributes, you should define user attributes at the individual user level only when an attribute is specific to the user. You should define all other attributes at the group level. Individual group members then inherit the group value.

CDAT Configuration Attributes

CDAT configuration attributes affect the behavior of the CDAT web application (for example, the port number where the web server listens for HTTP requests for CDAT). The configuration attributes also allow you to configure CDAT logging, debugging, and the management console. Other configuration attributes can affect the results that an SESM web application sees when it retrieves profile information from the LDAP directory.

Configuration attributes that affect the behavior of CDAT are defined in the cdat.jetty.xml file located in the *install_dir*/jetty/config directory, and the cdat.xml file located in the *install_dir*/cdat/config directory. Configuration attributes in the cdat.xml file include:

- sessionTimeout—The maximum period of inactivity allowed during a CDAT login, after which the user is logged out. The default value is 600 seconds.
- queryMaxResults—The maximum number of results to return for any directory query. The default value is 100.
- maxVariables—The maximum number of page/page instance variables allowed for each CDAT session. This number affects how many pages can be visited before their state is lost. The default value is 40.
- queryTimeout—The timeout for directory queries. The default value is 0 (infinite), and no timeout is in effect.

The CDAT management console is password protected. The management console's password is defined by the AuthInfo attribute in the cdat.xml file. In a production deployment, changing this password is a common-sense security precaution.

For detailed information on the CDAT configuration files and attributes, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*

RADIUS Data Proxy Configuration Attributes

RADIUS Data Proxy (RDP) configuration attributes can, in some cases, affect the results that an SESM web application sees when it retrieves account profile information. For example, if you use CDAT to make a change to a user profile defining a new account password, the change may not be immediately visible to an SESM web application because the RDP caches profile data. With the default values, it may take as long as 20 minutes for a user profile change to become visible to a SESM web application.

Tip During development and testing, restarting the RDP after modifying account profile data causes the change to be immediately visible in the SESM web application.

Configuration attributes that affect the caching behavior of RDP are defined in the config.xml file located in the *install_dir*/dess-auth/config directory. Configuration attributes in the config.xml file include:

- cacheExpireInterval—The interval after which the cache attempts to expire objects. The default value is 600 seconds.

- cacheObjectTimeout—The amount of time before cached objects time out. The default value is 600 seconds.

For detailed information on the RDP configuration files and attributes, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide.*

Creating and Updating Services and Service Groups

Many of the attributes that you define when creating a new service with CDAT are used by the Service Selection Gateway (SSG). The SSG connects the subscriber to the service or provides status information. The SSG is the enforcement point for authentication and service-specific policies such as session timeout, idle timeout, next-hop table, and other Internet Protocol (IP) attributes. The SSG also sends messages to the Cisco SESM web application regarding authentication failures or changes in the state of the SSG as a result of enforcement decisions (such as session timeout).

SSG Considerations for Service Creation

The following sections provide information on some of the SSG functionality that you can configure when creating a new service with CDAT.

Service Classes

When creating a new service with CDAT, you specify one of these service classes:

- Passthrough—The SSG can forward traffic through any interface via normal routing or a next-hop table. Because Network Address Translation (NAT) is not performed for this type of traffic, overhead is reduced. Passthrough service is ideal for standard Internet access.
- Proxy—When a subscriber requests access to a proxy service, the SSG will proxy the Access-Request to the RADIUS server. If the subscriber is successfully authenticated, the subscriber is connected to the service. During remote authentication, the SSG may perform NAT as follows:
  - If the RADIUS server assigns an IP address to the subscriber, the SSG performs NAT between the assigned IP address and the subscriber's real IP address.
  - If the RADIUS server does not assign an IP address, NAT is not performed.

  When a subscriber selects a proxy service, there is another user name and password prompt. After authentication, the service is accessible until the user logs out from the service, logs out from the Cisco SESM web application, or is timed out.
- Tunnel—When a subscriber selects a service via the Cisco SESM web application, the NRP acts as an L2TP access concentrator (LAC) and sends the PPP session through the service-specific L2TP tunnel. If the tunnel does not already exist, the NRP-LAC creates the proper tunnel to the L2TP network server (LNS).

Packet Filtering

The SSG uses IOS access control lists (ACLs) to prevent users, services, and passthrough traffic from accessing specific IP addresses and ports. The ACLs can be configured for services and users by means of Cisco AV pairs.

- Services—When an ACL attribute is added to a service profile, all users of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

- Users—When an ACL attribute is added to a user profile, it will apply globally to all of the user's traffic.

Service Access Order

When users are accessing multiple services, the SSG must determine the services for which the packets are destined. To do this, the SSG uses an algorithm to create a service access order list. This list is stored in the user's host object and contains services that are currently open and the order in which they are searched.

The algorithm that creates this list orders the open services based on the size of the network. Network size is determined by the subnet mask of the Service Route attribute (specified with Service routes box in Services window). A subnet that contains more hosts implies a larger network. If networks are the same size, the services will be listed in the order in which they were last accessed.

When creating services, be sure to define as small a network as possible. If there is overlapping address space, packets might be forwarded to the wrong service.

Next Hop Gateway

The Next hop gateway attribute in a service profile specifies the next hop key for a service. Each SSG uses its own next-hop table that associates this key with an actual IP address. Note that this attribute overrides the IP routing table for packets destined to a service. With CDAT, you use the NRPs window to create a next hop gateway table. For information on creating a next-hop table with CDAT, see "Creating and Updating NRP Information" section on page 2-51.

For information on downloading a next hop gateway table with the **ssg next-hop** command, see the *Cisco 6400 Command Reference*.

DNS Redirection

When the SSG receives a DNS request, it performs domain name matching using the Domain Name attribute from the service profiles of the currently logged-in services. For each service, you specify the Domain Name attribute in the Domain names box in the Services window.

- If a match is found, the request is redirected to the DNS server for the matched service.
- If a match is not found and the user is logged on to a service that has Internet connectivity, the request is redirected to the first service in the user's service access order list that has Internet connectivity. Internet connectivity is defined as a service containing a Service Route attribute of 0.0.0.0/0 (default route). The Service Route attribute is specified in the Service routes box in the Services window.
- If a match is not found and the user is not logged on to a service that has Internet connectivity, the request is forwarded using the normal routing methods specified in the client's TCP/IP stack.

Fault Tolerance for DNS

The SSG can be configured to work with a single DNS server, or two servers in a fault-tolerant configuration. Based on an internal algorithm, DNS requests will be switched to the secondary server if the primary server begins to perform poorly or fails.

Session Timeout and Idle Timeout Attributes

The Session Timeout and Idle Timeout attributes can be used in either a user or service profile. In a user profile, the attribute applies to the user's session. In a service profile, the attribute individually applies to each service connection.

In a dial-up networking or bridged (non-PPP) network environment, a user might disconnect from the NAS and release the IP address without using the SESM web application to log out from the SSG. If this happens, the SSG will continue to allow traffic to pass from that IP address, and this might be a problem if the IP address is obtained by another user.

The SSG provides two mechanisms to prevent this problem:

- Idle Timeout attribute—Specifies the maximum time a session or connection can remain idle before it is disconnected.
- Session Timeout attribute—Specifies the maximum time a host or service object can remain active in any one session.

Concurrent or Sequential Service Access Mode

For each service, you specify an access mode in the Access mode box in the Services window. SSG services can be configured for concurrent or sequential access. Concurrent access allows users to log on to this service while simultaneously connected to other services. Sequential access requires that the user log out of all other services before accessing a service configured for sequential access.

Concurrent access is recommended for most services. Sequential access is ideal for services for which security is important, such as corporate intranet access, or for which there is a possibility of overlapping address space.

Hierarchical Policing

SSG allows subscribers to choose one or more types of services. Each type of service has its own bandwidth requirements. For example, assume an ISP has two types of services, regular and premium. The regular service is cheaper for customers but is allocated less bandwidth per customer than the premium service, which provides more bandwidth and a higher quality connection. SSG, therefore, requires a mechanism to ensure bandwidth is distributed properly for customers using different types of services.

Traffic policing is the concept of limiting the transmission rate of traffic entering or leaving a node. In SSG, traffic policing can be used to allocate bandwidth between subscribers and between services to a particular subscriber to ensure all types of services are allocated a proper amount of bandwidth. SSG uses per-user and per-session policing to ensure bandwidth is distributed properly between subscribers (per-user policing) and between services to a particular subscriber (per-session policing). Because these policing techniques are hierarchical in nature (bandwidth can be first policed between users and then policed again between services to a particular user), this complete feature is called SSG Hierarchical Policing.

In a user or service profile, the Q attribute for Quality of Service (QoS) is used to define per-user or per-session policing. For per-user policing, the format used in the Local RADIUS Attributes box of CDAT's Users window is as follows:

```
Account-Info:QU;upstream-token-rate;upstream-normal-burst;
[upstream-excess-burst];D;downstream-token-rate;
downstream-normal-burst;[downstream-excess-burst
```

For per-session policing, the format used in the Local RADIUS Attributes box of CDAT's Services window is as follows:

Service-Info:QU;*upstream-token-rate*;*upstream-normal-burst*;
[upstream-excess-burst];**D**;*downstream-token-rate*;
downstream-normal-burst;*[downstream-excess-burst]*

The following example shows how to define per-user policing in a user profile using the Local RADIUS Attributes box in the Users window:

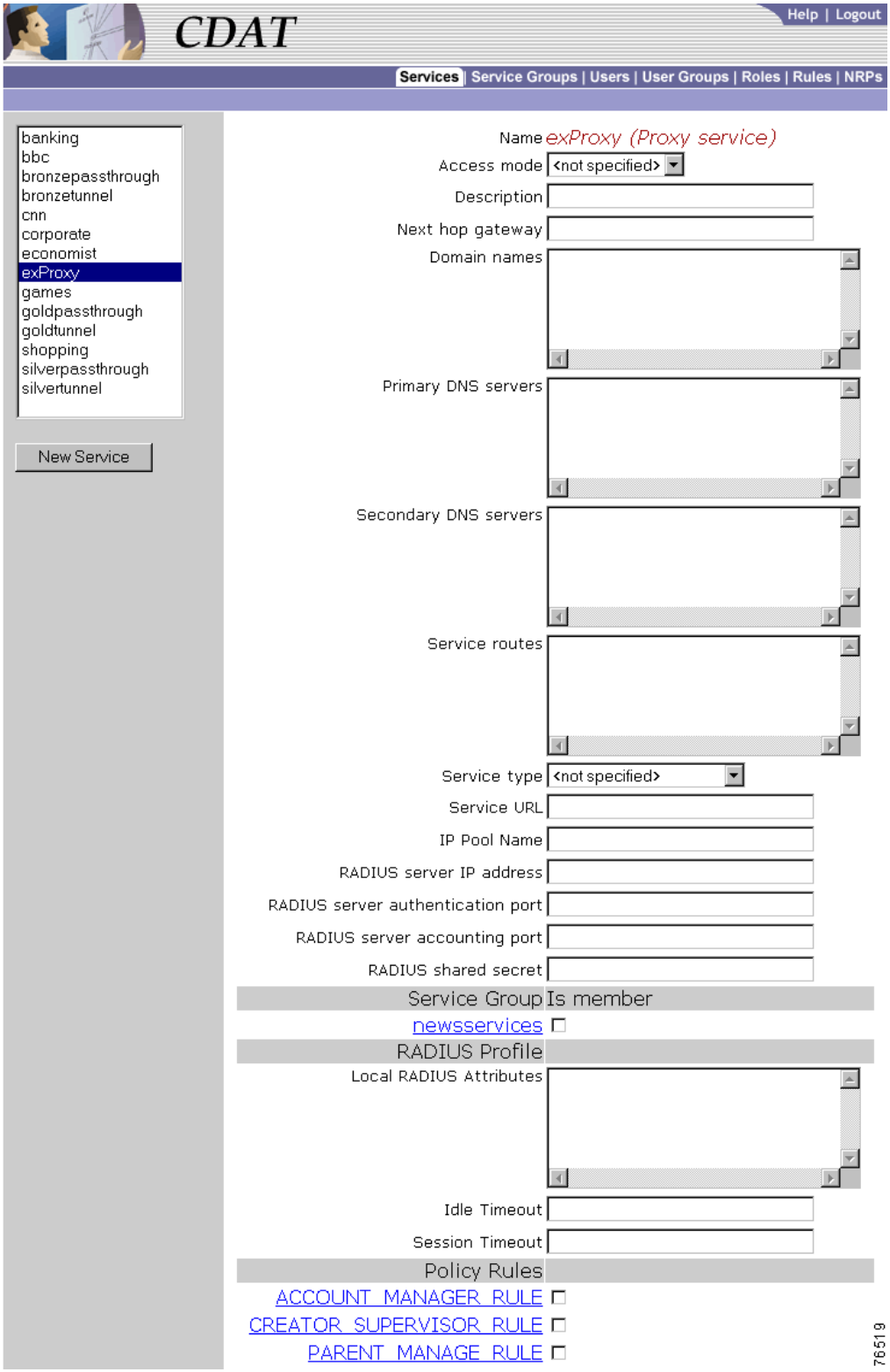
```
ACCOUNT_INFO:QU;16000;8000;16000;D;24000;12000;24000
```

For more information on SSG Hierarchical Policing, see the document *Service Selection Gateway Hierarchical Policing* on Cisco Connection Online (www.cisco.com).

Services Window

To create a service or update the attributes of an existing service, use the Services window (Figure 2-3).

Figure 2-3 Services Window for a Proxy Service



When you first create a service, you click New Service and specify the following:

Name (Required)

Name of the service. This attribute is used for accounting purposes. If the service does not have a description specified (the Description attribute), an SESM web application uses the specified name in the subscriber's service list when no description is available in the resource bundle or service profile.

Allowed values: A text string.

Example: Internet Service

Service class (Required)

Indicates whether the service is a passthrough service, proxy service, or tunnel service.

Allowed values:

- Passthrough—Passthrough service.
- Proxy—Proxy service.
- Tunnel—Tunneled service.

For information on service classes, see the "Service Classes" section on page 2-11.

For a new or existing service, you can specify the following attributes:

Access mode (Required)

Defines whether the user is able to log on to this service while simultaneously connected to other services (concurrent) or whether the user cannot access any other services while using this service (sequential).

Allowed values:

- Sequential—Sequential access mode.
- Concurrent—Concurrent access mode.

Description (Optional)

Gives a description of the service. An SESM web application (for example, New World Service Provider) uses this description in the subscriber's service list when icons are not used for services in the list.

Allowed values: A text string.

Example: My Company Intranet

Next hop gateway (Optional)

Specifies the next-hop key for this service. Each SSG uses its own next-hop gateway table that associates this key with an actual IP address. For information on the next-hop gateway table, see the "Next Hop Gateway" section on page 2-12 and the "Creating and Updating NRP Information" section on page 2-51.

Allowed values: A text string with the next hop key.

Example: service1nexthop

Domain names (Optional)

Specifies one or more domain names that get DNS resolution from the DNS server(s) specified in Primary DNS servers and Secondary DNS servers. For information on domain name matching, see the "DNS Redirection" section on page 2-12.

Allowed values: One or more domain names, each on a separate line.

Example: cisco.com
cisco-sales.com

Primary DNS servers (Required)

Specifies the primary DNS server for this service.

Allowed values: An IP address in dotted-decimal notation.

Example: 192.168.1.2

Secondary DNS servers (Optional)

Specifies the secondary DNS server for this service. If primary and secondary servers are specified, the SSG sends DNS requests to the primary DNS server until performance is diminished or it fails (failover). It then sends DNS requests to the secondary DNS server.

Allowed values: An IP address in dotted-decimal notation.

Example: 192.168.1.4

Service routes (Required)

Specifies the IP address and subnet mask of the networks or the hosts where the service is located. There can be multiple service routes for a service. For more information, see the "Service Access Order" section on page 2-12.

Allowed values: An IP address and subnet mask, separated by a semicolon. If more than one IP address and subnet mask are specified, you enter each service route on a separate line.

ip_address;subnet mask

An Internet service is typically specified as 0.0.0.0;0.0.0.0 in the service profile.

Example: 192.168.1.128;255.255.255.240

Service type (Required)

Specifies the level of service.

Allowed values: Currently, this attribute must be Outbound.

Service URL (Optional)

Gives the URL for this service. Depending on whether the SESM web application uses frames, the URL can appear in the address bar in a new browser window. When you enter the service URL, an H or U character must precede the URL. For example:

Hhttp://www.BestVideo.com

OR

Uhttp://www.BestVideo.com

If the SESM web application does not use frames, H and U have the same effect: When the subscriber selects the service, it is displayed in a new browser window, and the specified URL appears in the new window's address bar.

If the SESM web application does use frames, the behavior is as follows:

- With H, the service is displayed in a frame in the current browser window. Because the service is displayed in a frame of the containing application's frames, the specified URL is not displayed.
- With U, the service is displayed in a new browser window, and the specified URL appears in the new window's address bar.

Allowed values: A fully qualified URL preceded by the character H or U.

Example: Uhttp://www.BestVideo.com

IP Pool Name (Optional for PPP)

Specifies the name of the address pool from which to get the IP address for the service. If a service is defined as a primary service, the service must have the name of an address pool defined. For information on address pools and primary services, see the "Primary Service and Address Pool for a PPP Subscriber" section on page 2-25.

Allowed values: A text string.

Example: Blue

Proxy Service Attributes

For a proxy service, you specify the following attributes that provide information for the RADIUS server that the Service Selection Gateway (SSG) uses to authenticate access to this proxy service:

RADIUS server IP address (Required for a proxy service)

Specifies the IP address of the RADIUS server.

Allowed values: An IP address in dotted-decimal notation.

Example: 172.31.5.96

RADIUS server authentication port (Required for a proxy service)

Specifies the RADIUS server port number for authentication requests.

Allowed values: A UDP port number.

Example: 1812

RADIUS server accounting port (Required for a proxy service)

Specifies the RADIUS server port number for accounting requests.

Allowed values: A UDP port number.

Example: 1813

RADIUS shared secret (Required for a proxy service)

Specifies the secret key that the RADIUS server shares with proxy clients. The key must match the shared secret on the RADIUS server.

Allowed values: The shared secret key.

Example: sharedsecret

Tunnel Service Attributes

For a Layer 2 Tunnel Protocol (L2TP) tunnel service and virtual private dial network (VPDN), you specify the following attributes. For information on configuring L2TP and configuring the L2TP network server (LNS), see the *Service Selection Gateway* document.

Tunnel identifier (Required for a tunnel service)

Specifies the name of the tunnel. The name must match the tunnel ID specified in the L2TP network server VPDN group.

Allowed values: A tunnel ID (name).

Example: Service1Tunnel

Tunnel IP address (Required for a tunnel service)

Specifies the IP address of the home gateways (LNSs) to receive the L2TP connection.

Allowed values: An IP address in dotted-decimal notation.

Example: 10.1.1.1

Tunnel password (Required for a tunnel service)

Specifies the secret (password) used for L2TP tunnel authentication.

Allowed values: The secret (password).

Example: ourSecretPw

Tunnel password confirmation (Required for a tunnel service)

Specifies the secret (password) used for L2TP tunnel authentication. Used by CDAT to ensure that the password was correctly entered.

Allowed values: The secret (password) that was entered in the preceding Tunnel password box.

Example: ourSecretPw

Tunnel type (Required for a tunnel service)

Specifies that the tunnel type is L2TP. With an SESM tunnel service, the value must be l2tp.

Allowed values: l2tp to indicate an L2TP tunnel type. The value is case sensitive.

Example: l2tp (The first character is the lowercase letter l.)

Service Group is Member

CDAT displays the service groups that are currently defined. You indicate whether this service is a member of a service group by checking or unchecking the checkbox for the service group.

RADIUS Profile

Note RADIUS attributes can be specified at the service and the service group level. Service and service group RADIUS attributes are inherited. The set that applies to a service are all RADIUS attributes specified for the service and all RADIUS attributes specified for any service groups of which the service is a member. Therefore, a common-sense strategy is to specify RADIUS attributes at the individual service level and not at the service-group level.

Local RADIUS Attributes

Specifies one or more RADIUS attributes and values that apply to the service but that do not appear in the boxes of the Services window. These can be standard RADIUS attribute names or Cisco SSG vendor-specific attributes, including Cisco attribute-value pairs (Cisco AV pairs). For information on RADIUS attributes, see RFC 2865.

Tip The Local RADIUS Attributes box allows you to define an attribute that *does not* appear in the boxes of a CDAT window. For example, most Cisco AV pairs cannot be specified in the boxes of a CDAT window. For a list of the RADIUS attributes that correspond to the boxes of the Services window, see Appendix C, "RDP Service-Profile Translation."

Allowed values: Most standard RADIUS attribute names or Cisco SSG vendor-specific attributes are predefined in CDAT. For a list of the predefined RADIUS attributes, see the "Defining Local RADIUS Attributes" section on page 2-6.

To specify one of the predefined RADIUS attributes, use the following form:

ATTRIBUTE_NAME:*attribute_value*

ATTRIBUTE_NAME is one of the predefined RADIUS attributes, and *attribute_value* is the value given for the attribute. A colon (:) separates the two elements. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

Example:

```
CISCO-AV:ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21
```

Cisco AV Pairs for Service Profiles. With CDAT, the most common format for an AV pair is as follows:

```
CISCO-AV:protocol:attribute=value
```

The preceding format has these elements:

- `CISCO-AV` is required and indicates this is a Cisco AV pair.
- *protocol* is typically AIRNET, IP, IPX, OUTBOUND, RSVP, SHELL, SIP, VOIP, or VPDN.
- *attribute* is one of the attributes listed in Table 2-4.
- *value* is a value (for example, string, IP address, or integer) appropriate for the attribute. In the attribute descriptions that follow, the allowed values are indicated.

In the AV pair format, spaces are not allowed around the colon (`:`) and equal sign (`=`) characters. In some cases, spaces are allowed between items within *value*. For example, spaces separate some of the parts of an access control list:

```
CISCO-AV:ip:addr=10.2.3.4
```

Table 2-4 lists the Cisco AV pairs that are supported by the Cisco SESM and SSG software for service profiles when DESS/AUTH is used.

Table 2-4 Cisco AV Pairs for Service Profiles

Attribute Format	Description
acl=x	ASCII number representing a connection access list. Used only when service=shell. For example: shell:acl=115.
addr=x	A network address. Used with service=slip, service=ppp, and protocol=ip. Contains the IP address that the remote host should use when connecting via SLIP or PPP/IP. For example, addr=10.2.3.4.

Table 2-4 Cisco AV Pairs for Service Profiles (continued)

Attribute Format	Description

addr-pool=x	Specifies the name of a local address pool from which to get the address of the remote host (Cisco SESM web client). Used with service=ppp and protocol=ip.
	
	Note that addr-pool works in conjunction with local pooling. It specifies the name of a local pool, which must be preconfigured on the network access server. Use the **ip local pool** command to declare local pools. For example:
	
	`ip address-pool local`
	`ip local pool Blue 10.0.0.1 10.0.0.10`

inacl#<*n*>	ASCII access list identifier for an input access list to be installed and applied to an interface for the duration of the current connection. Use with service=ppp and protocol=ip and with service=ppp and protocol=ipx. Per-user access lists do not work with ISDN.
inacl=x	ASCII identifier for an interface input access list. Use with service=ppp and protocol=ip. Per-user access lists do not work with ISDN.
interface-config=x	Specifies user-specific interface configuration information with Virtual Profiles. The information that follows the equal sign (=) can be any Cisco IOS interface configuration command.
ip-addresses=x	List of possible IP addresses, separated by spaces, that can be used for the end-point of a tunnel. Use with service=ppp and protocol=vpdn.
min-links=<*n*>	Sets the minimum number of links for MLP.
outacl#<*n*>	ASCII access list identifier for an interface output access list to be installed and applied to an interface during the current condition. Use with service=ppp and protocol=ip, and with service=ppp and protocol=ipx. Per-user access lists do not work with ISDN.
outacl=x	ASCII identifier for an interface output access list. Use with service=ppp and protocol=ip, and with service=ppp and protocol=ipx. Contains an IP output access list for SLIP or PPP/IP (for example, outacl=4). The access list itself must already be configured on the router. Per-user access lists do not work with ISDN.
pool-def#<*n*>	Defines IP address pools on the NAS. Use with service=ppp and protocol=ip.
pool-timeout=x	In conjunction with pool-def, defines IP address pools on the NAS. During IPCP address negotiation, if an IP pool name is specified for a user (see the addr-pool attribute), a check is made that the named pool is defined on the NAS. If it is, the pool is consulted for an IP address. Use with service=ppp.
protocol=x	A protocol that is a subset of a service. Currently supported protocols are atalk, bap, bridging, ccp, cdp, deccp, ip, ipx, lat, lcp, multilink, nbf, osicp, pad, rlogin, telnet, tn3270, vines, vpdn, xns, xremote, and unknown.
proxyacl#<*n*>	Allows users to configure the downloadable user profiles (dynamic ACLs) by using the authentication proxy feature so that users can have the configured authorization to permit traffic going through the configured interfaces.

Table 2-4 Cisco AV Pairs for Service Profiles (continued)

Attribute Format	Description
route=x	Specifies a route to be applied to an interface. Use with service=slip, service=ppp, and protocol=ip. During network authorization, you can use this attribute to specify a per-user static route as follows: `route="dst_address mask [gateway]"` This indicates a temporary static route to be applied. The *dst_address*, *mask*, and *gateway* must be in dotted-decimal notation, with the same meanings as in the **ip route** configuration command on a NAS. If *gateway* is omitted, the peer's address is the gateway. The route is deleted when the connection terminates.
route#<*n*>	Like route, this attribute specifies a route to be applied to an interface, but these routes are numbered, allowing you to use multiple routes. Use with service=ppp and protocol=ip, and with service=ppp and protocol=ipx.
service=x	The service. Specify a service attribute to request authorization or accounting of that service. Values are slip, ppp, arap, shell, tty-daemon, connection, and system. *This attribute is required.*

Idle Timeout (Optional)

Specifies the maximum time, in seconds, that a session or connection can remain idle before it is disconnected. The default is no timeout.

Allowed values: A number of seconds.

Note When a non-PPP user, such as in a bridged networking environment, disconnects from a service without logging off, the connection remains open and the user will be able to reaccess the service without going through the logon procedure. This is because no direct connection (PPP) exists between the subscriber and the SSG. To prevent non-PPP users from being logged on to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout attributes.

Session Timeout (Optional)

Specifies the maximum time, in seconds, that a host or service object can remain active in any one session. The default is no timeout.

Allowed values: A number of seconds.

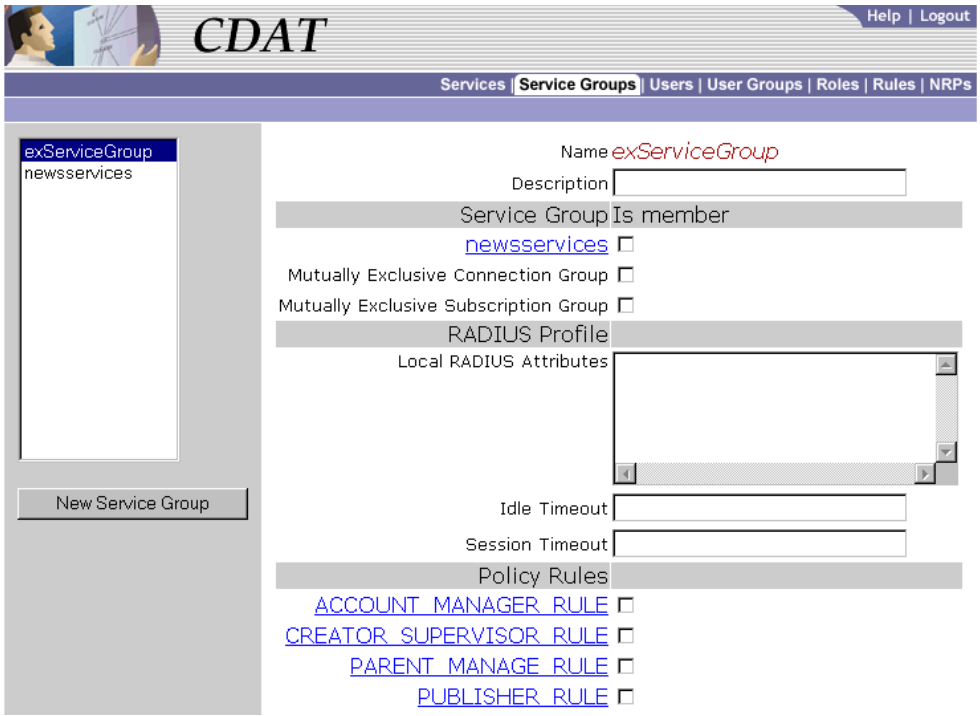
Policy Rules

CDAT displays the policy rules that are currently defined. You can indicate whether this service is a resource associated with a rule by checking or unchecking the checkbox for the rule. For information on rules, see the "Creating and Updating Rules" section on page 2-48.

Service Groups Window

To create a service group or update the attributes of an existing service group, use the Service Groups window (Figure 2-4). When creating a service group, you can make a service a member of the group by choosing the group in the Service Group Is member section of the Services window.

Figure 2-4 Service Groups Window



When you first create a service group, you click New Service Group and specify the following:

Name (Required)

Name of the service group.

Allowed values: A text string.

Example: Gold Services Group.

For a new or existing service group, you can specify the following attributes:

Description (Optional)

Gives a description of the service group.

Allowed values: A text string.

Example: A group of services for Gold subscribers.

Service Group is Member

CDAT displays the other service groups that are currently defined. You indicate whether this service group is a member of another service group by checking or unchecking the checkbox for the other service group.

Mutually Exclusive Connection Group

Indicates whether the service group is a mutually-exclusive connection group in which the subscriber can connect to only one service in the group at any one time.

Mutually Exclusive Subscription Group

Indicates whether the service group is a mutually-exclusive subscription group in which the subscriber can subscribe to only one service in the group at any one time.

RADIUS Profile

Note RADIUS attributes can be specified at the service and the service group level. Service and service group RADIUS attributes are inherited. The set that applies to a service are all RADIUS attributes specified for the service and all RADIUS attributes specified for any service groups of which the service is a member. Therefore, a common-sense strategy is to specify RADIUS attributes at the individual service level and not at the service-group level.

Local RADIUS Attributes (Optional)

Specifies one or more RADIUS attributes and values that apply to the service group but that do not appear in the boxes of the Service Groups window. These can be standard RADIUS attribute names or Cisco SSG vendor-specific attributes, including Cisco attribute-value pairs (Cisco AV pairs). For information on RADIUS attributes, see RFC 2865.

Allowed values: Most standard RADIUS attribute names or Cisco SSG vendor-specific attributes are predefined in CDAT. For a list of the predefined RADIUS attributes, see the "Defining Local RADIUS Attributes" section on page 2-6.

To specify one of the predefined RADIUS attributes, use the following form:

ATTRIBUTE_NAME:*attribute_value*

ATTRIBUTE_NAME is one of the predefined RADIUS attributes, and *attribute_value* is the value given for the attribute. A colon (:) separates the two elements. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

Example:

```
CISCO-AV:ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21
```

Cisco AV Pairs for Service Group Profiles. The Cisco AV pairs that are supported by the Cisco SESM and SSG software for service groups are the same as for services. For information on this set of AV pairs and the format used to specify them, see Table 2-4 and the "RADIUS Profile" section on page 2-19.

Idle Timeout (Optional)

Specifies the maximum time, in seconds, that a session or connection for services in the service group can remain idle before it is disconnected. The default is no timeout.

Allowed values: A number of seconds.

Note When a non-PPP user, such as in a bridged networking environment, disconnects from a service without logging off, the connection remains open and the user will be able to reaccess the service without going through the logon procedure. This is because no direct connection (PPP) exists between the subscriber and the SSG. To prevent non-PPP users from being logged on to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout attributes.

Session Timeout (Optional)

Specifies the maximum time, in seconds, that a host or service object for services in the service group can remain active in any one session. The default is no timeout.

Allowed values: A number of seconds.

Policy Rules

CDAT displays the policy rules that are currently defined. You can indicate whether this service group is a resource associated with a rule by checking or unchecking the checkbox for the rule. For information on rules, see the "Creating and Updating Rules" section on page 2-48.

Creating and Updating Users and User Groups

In CDAT, a user can be any one of the following:

- A *subscriber* is a customer of the service provider who subscribes to services.
- A *publisher* is a service-provider administrator who creates services and grants access to services.
- An *account manager* is a service-provider employee who creates subscriber accounts.
- An *administrator* is a service-provider administrator who can create any object (users, user groups, services, service groups, roles, and rules), add, modify, or delete any attribute, and assign access privileges to any object.

For each category of user, the CDAT administrator creates an account for the user with the Users window. In addition, the CDAT administrator must create one or more user groups for each category of user because roles and privileges are specified for user groups, not individual users.

For the CDAT administrator, creating a user who has access to resources (services or objects and attributes in the LDAP directory) involves these steps:

1. Create a user group with the User Groups window.
2. Create a role with the Roles window and make the user group a subject (occupant) of the role. The role defines the privileges that user group members have.
3. Create a rule with the Rules window and associate the role with the rule. The rule will grant the privileges associated with specified roles to a set of resources defined in the rule. For a subscriber, the set of resources includes one or more services.
4. Create the user with the Users window and make the user a member of one or more user groups.

Creating user groups, roles, and rules is usually done once when the initial set of objects is being defined. Once these objects are defined, creating a user who actually has access to resources typically requires only Step 4.

Primary Service and Address Pool for a PPP Subscriber

When you define a user account for a subscriber to connect through a PPP connection, you can also define a primary service for the subscriber.

Note IP address allocation for PPP subscribers is a deployment consideration. If a primary service or a local address pool or both are not defined in the user profile of a PPP subscriber, a local address pool name for a service may be defined on the network access server (NAS).

A user account for a PPP subscriber can have one primary service from which the SSG software determines an IP address range (sometimes called a *local address pool*). The user receives a primary IP address from this address range. This primary-service addressing mechanism allows the subscriber's IP address to be associated with a primary service, which is usually the subscriber's Internet service. If the subscriber switches to another ISP (primary service), the IP address range from which subscriber's address is obtained changes to the address pool of the new ISP.

- When you define a user, the primary service for the user account is specified with the Primary Service box of the Users window.
- When you define a primary service, the name of the address pool from which to get the IP address is specified with the IP Pool Name box in the Services window. For example:

  IP Pool Name Blue

The IP Pool Name attribute specifies the name of a local address pool. On the NAS, the deployer must use the **ip local pool** command to define the range of addresses for the local address pool.

Primary Service Example

As an example of the primary-service addressing mechanism, assume the following:

- A user account for a PPP subscriber defines the user's Primary Service to be Internet-Blue.
- The service definition for Internet-Blue defines the IP Pool Name to be Blue.
- The NAS is configured with **ip local pool** command so that the local pool Blue uses a specified range of IP addresses.

With the preceding conditions in place, the IP address for the user whose primary service is Internet-Blue is taken from the local pool of addresses defined on the NAS for the local address pool Blue.

Primary Service and Local Address Pool Precedence

CDAT allows you to define a primary service at the user and user group level. In addition, you can also define a local address pool at the user and user group level. The precedence for these definitions is as follows (item 1 having the highest precedence):

1. Pool name in the Users window
2. Primary Service in the Users window
3. Pool name in the User Groups window
4. Primary Service in the User Groups window

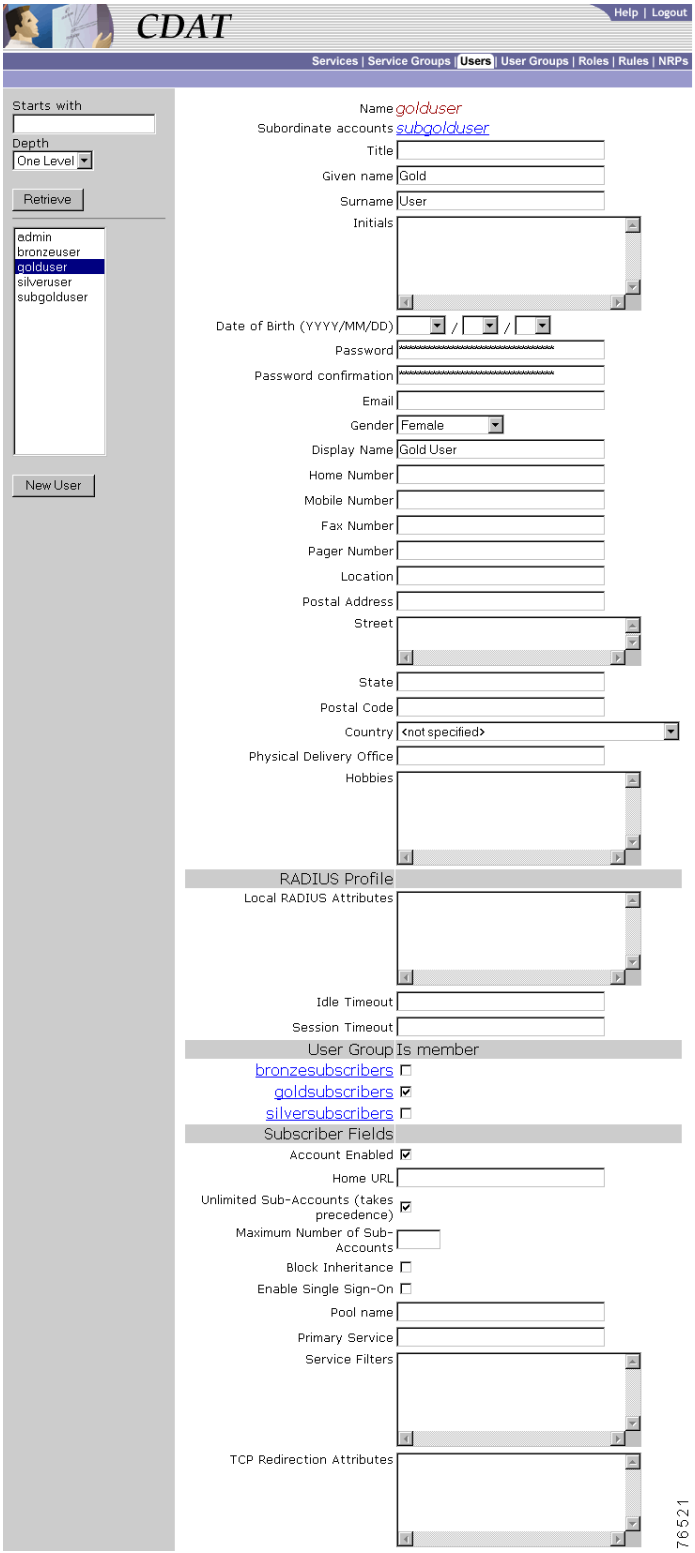
Note When a Pool name and Primary Service are specified in the Users or User Groups window, this local address pool name takes precedence over any pool name defined for the user's primary service (IP Pool Name in the Services window).

Users Window

To create a subscriber or administrator account or to update information in an existing subscriber or administrator account, use the Users window (Figure 2-5). Service subscriptions and service-group subscriptions are not shown in the figure.

After a subscriber account is created, you can use the Create subaccount button (at the bottom of the Users window) to create a subaccount. The attributes that define a subaccount are identical to the attributes for a parent account.

Figure 2-5 Users Window



When you first create a user, you click New User and specify the following:

Name (Required)

Name of the user.

Allowed values: A text string

Example: Terry Connor

If the user has subaccounts, CDAT displays the following:

Subordinate accounts

Shows subaccounts that have been created for this user account. This is a read-only field.

For a new or existing user, you can specify the following attributes:

User Information (Optional)

The first set of boxes in the Users window specifies information about the user. The user information is derived from the X.500 user schema for use with LDAP. The following attributes appear in the user-information block:

- Title
- Given name
- Surname
- Initials
- Date of Birth
- Password
- Password confirmation
- Email
- Gender
- Display Name
- Home Number
- Mobile Number
- Fax Number
- Pager Number
- Location
- Postal Address
- Street
- State
- Postal Code
- Country
- Physical Delivery Office
- Hobbies

Note A password must contain at least one character (letter or number).

RADIUS Profile

Note RADIUS attributes can be specified at the user and the user group level. User and user group RADIUS attributes are inherited. The set that applies to a user are all RADIUS attributes specified for the user and all RADIUS attributes specified for any user groups of which the user is a member.

Local RADIUS Attributes (Optional)

Specifies one or more RADIUS attributes and values that apply to the user but that do not appear in the boxes of the Users window. These can be standard RADIUS attribute names or Cisco SSG vendor-specific attributes, including Cisco attribute-value pairs (Cisco AV pairs). For information on RADIUS attributes, see RFC 2865.

Allowed values: Most standard RADIUS attribute names or Cisco SSG vendor-specific attributes are predefined in CDAT. For a list of the predefined RADIUS attributes, see the "Defining Local RADIUS Attributes" section on page 2-6.

To specify one of the predefined RADIUS attributes, use the following form:

ATTRIBUTE_NAME:*attribute_value*

ATTRIBUTE_NAME is one of the predefined RADIUS attributes, and *attribute_value* is the value given for the attribute. A colon (:) separates the two elements. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

Example:

```
CALLING-STATION-ID:123456789
```

Cisco AV Pairs for User Profiles. The Cisco AV pairs that are supported by the Cisco SESM and SSG software for user profiles are for upstream access control lists and downstream access control lists.

Upstream and Downstream Access Control Lists

An upstream access control list (ACL) is defined with the inacl AV pair and specifies an access control list to be applied to upstream traffic coming from the user. A downstream access control list is defined with the outacl AV pair and specifies an access control list to be applied to downstream traffic going to the user. Either type of access control list can be an IOS standard access control list or an extended access control list. When you specify an AV pair in the Local RADIUS Attributes box, the syntax is as follows:

CISCO-AV:ip:inacl[#*number***]={***standard-access-control-list* **|** *extended-access-control-list***}**

CISCO-AV:ip:outacl[#*number***]={***standard-access-control-list* **|** *extended-access-control-list***}**

Syntax Description

number	Access list identifier.
standard-access-control-list	Standard access control list.
extended-access-control-list	Extended access control list.

Note The SESM web portal application uses extended access control lists for its firewall functionality. The SSG does not allow a mix of standard and extended access control lists.

The following guidelines apply when you use ACLs for firewall functionality in an SESM web portal application and its My Firewall page:

- The range of ACL numbers reserved for use in *deployer-imposed* firewalls is 100 to 109.
- The range of ACL numbers reserved for use in *subscriber-imposed* firewalls (the SESM web portal's My Firewall page) is 110 to 196.
- ACLs whose numbers are in the range 100 to 109 will have higher priority than any ACLs created by subscribers using the My Firewall page.
- The numbers indicate priority in the ACL evaluation. ACLs with the lowest numbers are analyzed first. The order is important because ACL processing stops when the first match occurs.

For more information on ACLs and SESM firewalls, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Examples

```
CISCO-AV:ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21

CISCO-AV:ip:outacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 21
```

There can be multiple instances of upstream and downstream access control lists within user profiles. Use one AV pair attribute for each access control list statement. Multiple attributes can be used for the same ACL. Multiple attributes will be downloaded according to the number specified and executed in that order.

Idle Timeout (Optional and for Subscribers Only)

Specifies the maximum time, in seconds, that a session or connection can remain idle before it is disconnected. The default is no timeout.

Allowed values: A number of seconds.

Note When a non-PPP user, such as in a bridged networking environment, disconnects from a service without logging off, the connection remains open and the user will be able to reaccess the service without going through the logon procedure. This is because no direct connection (PPP) exists between the subscriber and the SSG. To prevent non-PPP users from being logged on to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout attributes.

Session Timeout (Optional and for Subscribers Only)

Specifies the maximum time, in seconds, that a host or service object can remain active in any one session. The default is no timeout.

Allowed values: A number of seconds.

User Group Is Member

CDAT displays the user groups that are currently defined. You can indicate whether the user is a member of a user group by checking or unchecking the checkbox for the group. For information on user groups, see the "User Groups Window" section on page 2-35.

Subscriber Fields

Account Enabled

Indicates whether the user account is currently enabled for authentication purposes when logging on to an SESM web portal. A subscriber with an enabled account can log on to an SESM web portal.

Home URL (For Subscribers Only)

Gives the home URL for this user's preferred Internet home page when the subscriber logs on to SESM. As shown in the following examples, when you enter the home URL, an H or U character must precede the URL. The H or U character control whether an SESM web application displays the home page in a new browser window.

Hhttp://www.MyHomePage.com

OR

Uhttp://www.MyHomePage.com

If an SESM web application does not use frames, H and U have the same effect: When the subscriber logs on to SESM, the home page is displayed in a new browser window.

If an SESM web application does use frames, the behavior is as follows when the subscriber logs on to SESM:

- With H, the home page is displayed in a frame in the current browser window.
- With U, the home page is displayed in a new browser window.

Allowed values: A fully qualified URL preceded by the character H or U.

Example: Uhttp://www.MyHomePage.com

Unlimited Sub-Accounts (Subscribers Only)

Indicates whether the number of subaccounts for this user is unlimited. By default, Unlimited Sub-Accounts is checked and the user can create an unlimited number of subaccounts.

Note If you uncheck Unlimited Sub-Accounts and specify no value for Maximum Number of Sub-Accounts, the value for subaccount-creation limits defined at the user-group level takes effect.

Maximum Number of Sub-Accounts (Optional and for Subscribers Only)

Specifies the number of subaccounts allowed for this user.

Allowed values: The value 0 or a positive number for the subaccount-creation limit.

Example: 5

Block Inheritance (For Subscribers Only)

Indicates whether subaccounts created by this user inherit service subscriptions from this user account (the parent account) or from the container.

Enable Single Sign-On (Optional)

Indicates whether the single sign-on feature applies to the user.

- For PPP subscribers—With single sign-on enabled, the Cisco SESM web application queries the SSG for the existence of a PPP connection for the host key or IP address of any request to the Cisco SESM. The Cisco SESM web application does not require additional authentication if a PPP connection already exists.

- For non-PPP subscribers—With single sign-on enabled, when an SESM session is lost (for example, due to inactivity), the SSG maintains an active edge session so that the subscriber does not need to reauthenticate.

Note For the single-sign-on feature to work in LDAP mode, the singleSignOn attribute in an SESM web portal application configuration file, such as nwsp.xml, must be set to true. For information on setting the singleSignOn attribute, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Pool name (Optional and for PPP Subscribers Only)

Specifies the name of a local address pool (IP address range) for the user. The user receives a primary IP address from this address range. For information on local address pools, see the "Primary Service and Address Pool for a PPP Subscriber" section on page 2-25.

Allowed values: A text string for a local address pool name.

Example: GoldPool

Primary Service (Optional and for PPP Subscribers Only)

Specifies the name of a primary service for this user. For information on primary services and local address pools, see the "Primary Service and Address Pool for a PPP Subscriber" section on page 2-25.

Allowed values: A text string for a primary service name.

Example: Internet-Blue

Service Filters (Optional and for Subscribers Only)

Specifies the list of services that are blocked (that is, not inherited) for this subscriber account and for all subaccounts below this subscriber account. For example, this attribute might be used to block services to which children should not be granted access.

Note When a subaccount inherits service filters, the service names do not appear in the Service Filters box of the subaccount but are applied by the DESS/AUTH software at run time.

Allowed values: One or more text strings for service names. Multiple services appear on separate lines. Service group names are not allowed.

Example: Gambling Service
Banking

TCP Redirection Attributes (Optional and for Subscribers Only)

One or more RADIUS vendor-specific attributes related to TCP redirection. For information on TCP redirection, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Allowed values: Table 2-5 describes the allowed vendor-specific attributes.

Table 2-5 TCP Redirection Attributes

Attribute	Description
RI*group*;*duration*[;*service*]	Overrides the TCP redirect configuration on the SSG for initial logon redirections. The *group* is the captive portal group to use for initial logon redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The *duration* is the duration of the captivation (in seconds). If you specify the optional *service* field, initial logon redirection occurs only when the subscriber requests connection to the named service.
RA*group*;*duration*;*frequency*[;*service*]	Overrides the TCP redirect configuration on the SSG for advertisement redirections. The *group* is the captive portal group to use for advertisement redirections for this subscriber. The group must be configured on the SSG with TCP redirect commands. The *duration* is the duration of the captivation (in seconds). The frequency is the approximate interval between redirections (in seconds). If you specify the optional *service* field, initial advertisement redirection occurs only when the subscriber requests connection to the named service.
RS	Indicates the subscriber has SMTP forwarding capability.

If more than one attribute is specified in the TCP Redirection Attributes box, enter each attribute on a separate line.

Example: RIRedirectServers;12;OnlineEducation
RS

Service and Service Group Subscriptions

For each service and service group to which the user can subscribe, CDAT displays one of the following subscription scopes:

- Available—The user has the privileges needed to subscribe to the service or service group but is currently not subscribed.
- Inherited—The user is subscribed to the service or service group through inheritance (that is, through a user group of which the user is a member).
- Local—The user is explicitly subscribed to the service or service group (as opposed to being subscribed by inheritance from a user group), or a feature of the service or service group (for example, a password) has been explicitly chosen that is different from the features defined for the user group.
- Unsubscribed—The user is subscribed to the service or service group through inheritance but has explicitly chosen to unsubscribe.

If CDAT does not display a service or service group in the Users window, the user does not have the privileges needed to subscribe to the service or group. For each service or service group to which the user has access, you can specify the following information:

Subscribe (For Subscribers Only)

Indicates whether the user is subscribed to the service or service group.

Note If the subscriber has been given subscription privileges by the administrator, the subscriber can then use the SESM account-management pages to subscribe to or unsubscribe from the service or service group if desired.

For each service to which the user has access, you can specify the following information:

Auto-logon (For Subscribers Only)

Indicates whether the user is automatically logged on to the service. With an auto-logon service, when a subscriber enters a user name and password to log on to the SESM web application, the subscriber is also automatically logged on to this service with the user name and password that were used to log into the SESM web application.

Note In the SESM web application configuration file, the auto-logon functionality is called the autoconnect feature. The autoConnect attribute in an SESM web application configuration file (for example, nwsp.xml) controls the auto-logon functionality. For information on the autoConnect attribute, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Hidden (For Subscribers Only)

Indicates whether an auto-logon service is a hidden service. An SESM web application does not display a hidden service in the subscriber's service list. If the Hidden attribute is not selected, an SESM web application does display the service in the subscriber's service list. For services that are not auto-logon, selecting the Hidden attribute has no effect.

User Groups Window

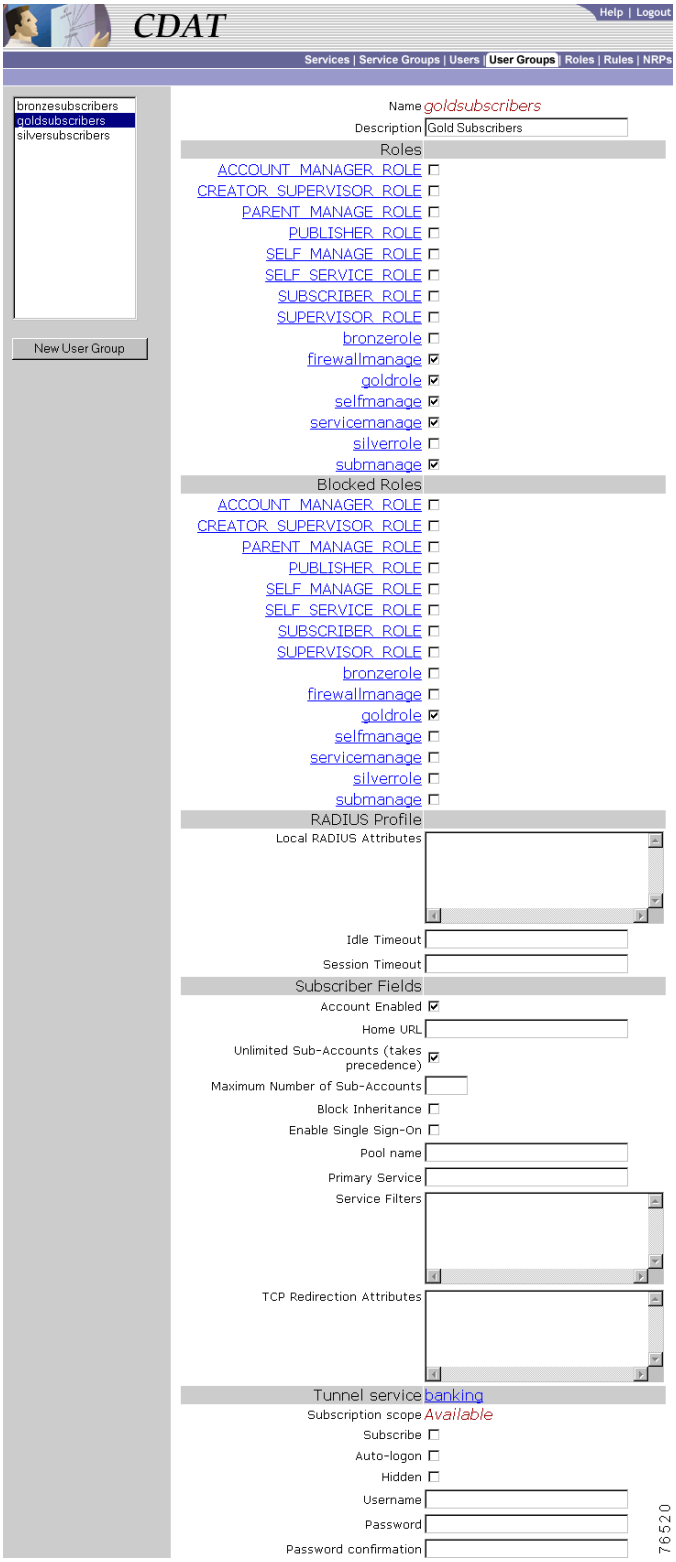
A *user group* is a set of users. With CDAT, individual users—subscribers, publishers, account managers, and administrators—must be associated with one or more user groups in order to get access to resources. After creating a user group, you can make a user a member of the group by choosing the group in the User Group Is member section of the Users window.

Privileges are granted to a user group through a role. The resources to which the user group has access are defined in a rule. With RBAC, both privileges and access to resources are managed at the group level. For example, a user group made up of subscribers can be given access at the group level to a new service.

For inheritable user and user group attributes, you should define user attributes at the individual user level only when an attribute is specific to the user. You should define all other attributes at the group level. Individual group members then inherit the group value. For more information on inheritable attributes, see the "Attribute Values and Inheritance" section on page 2-9.

To create a new user group or update the attributes of an existing user group, use the User Groups window (Figure 2-6).

Figure 2-6 User Groups Window



When you first create a user group, you click New User Group and specify the following:

Name (Required)

Name of the user group.

Allowed values: A text string.

Example: Gold Subscribers Group

For a new or existing user group, you can specify the following attributes:

Description (Optional)

Gives a description of the user group. The description is for informational purposes to help administrators identify the purpose of this user group.

Allowed values: A text string.

Roles

CDAT displays the roles that are currently defined. You can indicate whether the user group is an occupant of a role by checking or unchecking the checkbox for the role. For information on roles, see the "Roles Window" section on page 2-43.

Blocked Roles

CDAT displays the roles that are currently defined. You currently do not use the Blocked Roles attribute at the user-group level.

RADIUS Profile

Local RADIUS Attributes (Optional)

Specifies one or more RADIUS attributes and values that apply to the user group but that do not appear in the boxes of the User Groups window. These can be standard RADIUS attribute names or Cisco SSG vendor-specific attributes, including Cisco attribute-value pairs (Cisco AV pairs). For information on RADIUS attributes, see RFC 2865.

Allowed values: Most standard RADIUS attribute names or Cisco SSG vendor-specific attributes are predefined in CDAT. For a list of the predefined RADIUS attributes, see the "Defining Local RADIUS Attributes" section on page 2-6.

To specify one of the predefined RADIUS attributes, use the following form:

ATTRIBUTE_NAME:*attribute_value*

ATTRIBUTE_NAME is one of the predefined RADIUS attributes, and *attribute_value* is the value given for the attribute. A colon (:) separates the two elements. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

Example:

```
CISCO-AV:ip:inacl#101=deny tcp 192.168.1.0 0.0.0.255 any eq 23
```

Cisco AV Pairs for User Group Profiles. The Cisco AV pairs that are supported by the Cisco SESM software for user group profiles are for upstream access control lists and downstream access control lists.

Note RADIUS attributes can be specified at the user and the user group level. User and user group RADIUS attributes are inherited. The set that applies to a user are all RADIUS attributes specified for the user and all RADIUS attributes specified for any user groups of which the user is a member.

Idle Timeout (Optional and for Subscriber Groups Only)

Specifies the maximum time, in seconds, that a session or connection can remain idle before it is disconnected. The default is no timeout.

Allowed values: A number of seconds.

Note When a non-PPP user, such as in a bridged networking environment, disconnects from a service without logging off, the connection remains open and the user will be able to reaccess the service without going through the logon procedure. This is because no direct connection (PPP) exists between the subscriber and the SSG. To prevent non-PPP users from being logged on to services indefinitely, be sure to configure the Session-Timeout and/or Idle-Timeout attributes.

Session Timeout (Optional and for Subscriber Groups Only)

Specifies the maximum time, in seconds, that a host or service object can remain active in any one session. The default is no timeout.

Allowed values: A number of seconds.

Subscriber Fields

Account Enabled (For Subscriber Groups Only)

Indicates whether the user accounts for group members are currently enabled for authentication purposes when logging on to an SESM web portal. A user with an enabled account can log on to an SESM web portal.

Home URL (For Subscriber Groups Only)

Gives the home URL for the group member's preferred Internet home page when the subscriber logs on to SESM. As shown in the following examples, when you enter the home URL, an H or U character must precede the URL. The H or U character control whether an SESM web application displays the home page in a new browser window.

Hhttp://www.MyHomePage.com

OR

Uhttp://www.MyHomePage.com

If an SESM web application does not use frames, H and U have the same effect: When the subscriber logs on to SESM, the home page is displayed in a new browser window.

If an SESM web application does use frames, the behavior is as follows when the subscriber logs on to SESM:

- With H, the home page is displayed in a frame in the current browser window.
- With U, the home page is displayed in a new browser window.

Allowed values: A fully qualified URL preceded by the character H or U.

Example: Uhttp://www.MyHomePage.com

Unlimited Sub-Accounts (Subscriber Groups Only)

Indicates whether the number of subaccounts for users in the group is unlimited. By default, Unlimited Sub-Accounts is checked, and the user has the ability to create an unlimited number of subaccounts.

Maximum Number of Sub-Accounts (Optional and for Subscriber Groups Only)

Specifies the number of subaccounts allowed for this user in the group.

Allowed values: The value 0 or a positive number for the subaccount-creation limit.

Example: 5

Block Inheritance (Not Currently Used)

Not used and ignored if chosen.

Enable Single Sign-On

Indicates whether the single sign-on feature applies to the users.

- For PPP subscribers—With single sign-on enabled, the Cisco SESM web application queries the SSG for the existence of a PPP connection for the host key or IP address of any request to the Cisco SESM. The Cisco SESM web application does not require additional authentication if a PPP connection already exists.
- For non-PPP subscribers—With single sign-on enabled, when an SESM session is lost (for example, due to inactivity), the SSG maintains an active edge session so that the subscriber does not need to reauthenticate.

Note For the single-sign-on feature to work in LDAP mode, the singleSignOn attribute in an SESM web portal application configuration file, such as nwsp.xml, must be set to true. For information on setting the singleSignOn attribute, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Pool name (Optional and for PPP Subscriber Groups Only)

Specifies the name of a local address pool (IP address range) for users in the group. For information on local address pools, see the "Primary Service and Address Pool for a PPP Subscriber" section on page 2-25.

Allowed values: A text string for a local address pool name.

Example: GoldPool

Primary Service (Optional and for PPP Subscriber Groups Only)

Specifies the name of a primary service for users in the group. For information on primary services and local address pools, see the "Primary Service and Address Pool for a PPP Subscriber" section on page 2-25.

Allowed values: A text string for a primary service name.

Example: Internet-Blue

Service Filters (Optional and for Subscriber Groups Only)

Specifies the list of services that are blocked (that is, not inherited) for group member accounts and for all subaccounts below these member accounts. For example, this attribute might be used to block services to which children should not be granted access.

Note When a subaccount inherits service filters, the service names do not appear in the CDAT Services window but are applied by the DESS/AUTH software at run time.

Allowed values: One or more text strings for service names. Multiple services appear on separate lines. Service group names are not allowed.

Example: Gambling Service
Banking

TCP Redirection Attributes (Optional and for Subscriber Groups Only)

One or more RADIUS vendor-specific attributes related to TCP redirection. For information on TCP redirection, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Allowed values: Table 2-5 describes the allowed vendor-specific attributes. If more than one attribute is specified in the TCP Redirection Attributes box, enter each attribute on a separate line.

Example: RIRedirectServers;12;OnlineEducation
RS

Service and Service Group Subscriptions

For each service and service group to which the users in the user group can subscribe, CDAT displays one of the following subscription scopes:

- Available—The user group has the privileges needed to subscribe to the service or service group but is currently not subscribed.
- Local—The user group is explicitly subscribed to the service or service group. Choosing Auto-logon is a subscription to a service.

If CDAT does not display a service or service group in the User Groups window, the user group does not have the privileges needed to subscribe to the service or service group. For each service or service group to which the user has access, you can specify the following information:

Subscribe (For Subscriber Groups Only)

Indicates whether the user group is subscribed to the service or service group.

Note If the user group of subscribers has been given subscription privileges by the administrator, the subscriber can then use the SESM account-management pages to subscribe to or unsubscribe from the service or service group if desired.

For each service to which the user has access, you can specify the following information:

Auto-logon (For Subscriber Groups Only)

Indicates whether the members of the user group are automatically logged on to the service. With an auto-logon service, when a subscriber enters a user name and password to log on to the SESM web application, the subscriber is also automatically logged on to this service with the user name and password that were used to log into the SESM web application.

Note In the SESM web application configuration file, the auto-logon functionality is called the autoconnect feature. The autoConnect attribute in an SESM web application configuration file (for example, nwsp.xml) controls the auto-logon functionality. For information on the autoConnect attribute, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

Hidden (For Subscribers Only)

Indicates whether an auto-logon service is a hidden service. An SESM web application does not display a hidden service in the subscriber's service list. If the Hidden attribute is not selected, an SESM web application does display a service in the subscriber's service list. For services that are not auto-logon, selecting the Hidden attribute has no effect.

Creating and Updating Roles

In the RBAC model, a *role* is a collection of associated privileges. With CDAT, a user group may be assigned to multiple roles. In the context of Cisco SESM and CDAT, user groups fall into the following general categories:

- *Subscribers*—User groups that may subscribe to services and, optionally, modify their own account attributes (for example, passwords and address information) and create subaccounts if it is the parent account.
- *Publishers*—User groups that may create services and assign access privileges to services.
- *Account Managers*—User groups that may create accounts.
- *Administrators*—User groups that may create any object (users, user groups, services, service groups, roles, and rules), add, modify, or delete any attribute, and assign access privileges to any object. This is a superuser role and should not be deleted.

With RBAC and CDAT, the underlying directory and SPE software determines the roles for a given user in these ways:

- Roles are assigned indirectly to a user when the user is made a user group member.
- Roles can be inherited from a container in the directory tree.
- All roles are expanded by the LDAP directory software to include parent roles.

For a subaccount, roles are inherited from the parent account as determined in the preceding ways. Service filters that are defined for the parent account also apply to the subaccount.

Predefined Roles

If the RBAC objects were installed when the SPE software was installed, a set of predefined roles will be displayed in the list of roles. For information on the predefined roles, see Appendix A, "Predefined Roles and Rules."

Subscriber Role Examples

This section provides two examples of subscriber roles and the privileges that you might grant to a subscriber.

Self-Care and Subaccount-Creation Subscriber Roles

For a subscriber who requires self-care privileges (managing account attributes such as passwords and addresses) and subaccount-creation privileges, you can use the privilege Cisco_Dess_Manage and as role occupant specify the dynamic subject Self. The dynamic subject Self defines the role occupant when the accessed resource name is the same as the subject name in the submitted privilege token. The dynamic subject Self allows a subscriber to be a role occupant only for objects and attributes that are related to the specific user account.

The predefined role SELF_MANAGE_ROLE provides an example of how you can define privileges for subscriber self-care and subaccount creation with the privilege Cisco_Dess_Manage and the dynamic subject Self. The predefined roles are optionally installed with the RBAC objects as part of the SPE software installation.

In the associated rule SELF_MANAGE_RULE that defines resources for SELF_MANAGE_ROLE, the resources are specified as the container that holds the SESM/CDAT objects. In this way, a subscriber who is a member of a group occupying the SELF_MANAGE_ROLE has access to all objects and attributes that are related to this specific subscriber account.

Service Subscription Roles

For a subscriber to subscribe to and unsubscribe from services with the SESM web application, you must grant the user the following privileges through one or more roles:

- SESMSubscribe
- Cisco_Dess_Subscribe and Cisco_Dess_Unsubscribe
- Cisco_Dess_Read

In addition, the subscriber must be associated with a role that has Cisco_Dess_Manage privilege for the dynamic subject Self, and with a rule where the resources are specified as the container that holds the SESM/CDAT objects. In this way, the user can manage all objects and attributes that are related to the specific subscriber account. For information on this type of role and rule, see the explanation of the SELF_MANAGE_ROLE and SELF_MANAGE_RULE in the "Self-Care and Subaccount-Creation Subscriber Roles" section on page 2-42.

The SESMSubscribe privilege causes the SESM web application to display the navigation-bar button (MY SERVICES) that is linked to the page that allows service subscription and unsubscription.

Tip To remove subscription privileges from a subscriber, remove the SESMSubscribe privilege so that SESM web application does not display the MY SERVICES button. *Do not remove* the privilege Cisco_Dess_Subscribe. If a subscriber does not have Cisco_Dess_Subscribe privilege, services will not be available for the SESM web application to display in the service list (where the subscriber clicks a service to connect to the service).

Firewall-related Roles

For a subscriber to deploy a firewall with the SESM web application's My Firewall page, you must grant the user the following privileges through one or more roles:

- SESMFirewall
- Cisco_Dess_Read

In addition, the subscriber must be associated with a role that has Cisco_Dess_Manage privilege for the dynamic subject Self, and with a rule where the resources are specified as the container that holds the SESM/CDAT objects. In this way, the user can manage all objects and attributes that are related to the specific subscriber account. For information on this type of role and rule, see the explanation of the SELF_MANAGE_ROLE and SELF_MANAGE_RULE in the "Self-Care and Subaccount-Creation Subscriber Roles" section on page 2-42.

Parent and Subaccount Subscriber Roles

Roles for subscribers can require that you create two or more roles that are associated with specific privileges. As an example, consider an SESM deployment that allows only the parent user account (not the subaccount users) to create subaccounts. This model could be implemented with two distinct roles: one role for the parent user and one role for the subaccount user.

As an example of this model, assume that the parent user group is GoldSubscriberParent and is associated with a GoldSubscriberParentRole having these privileges:

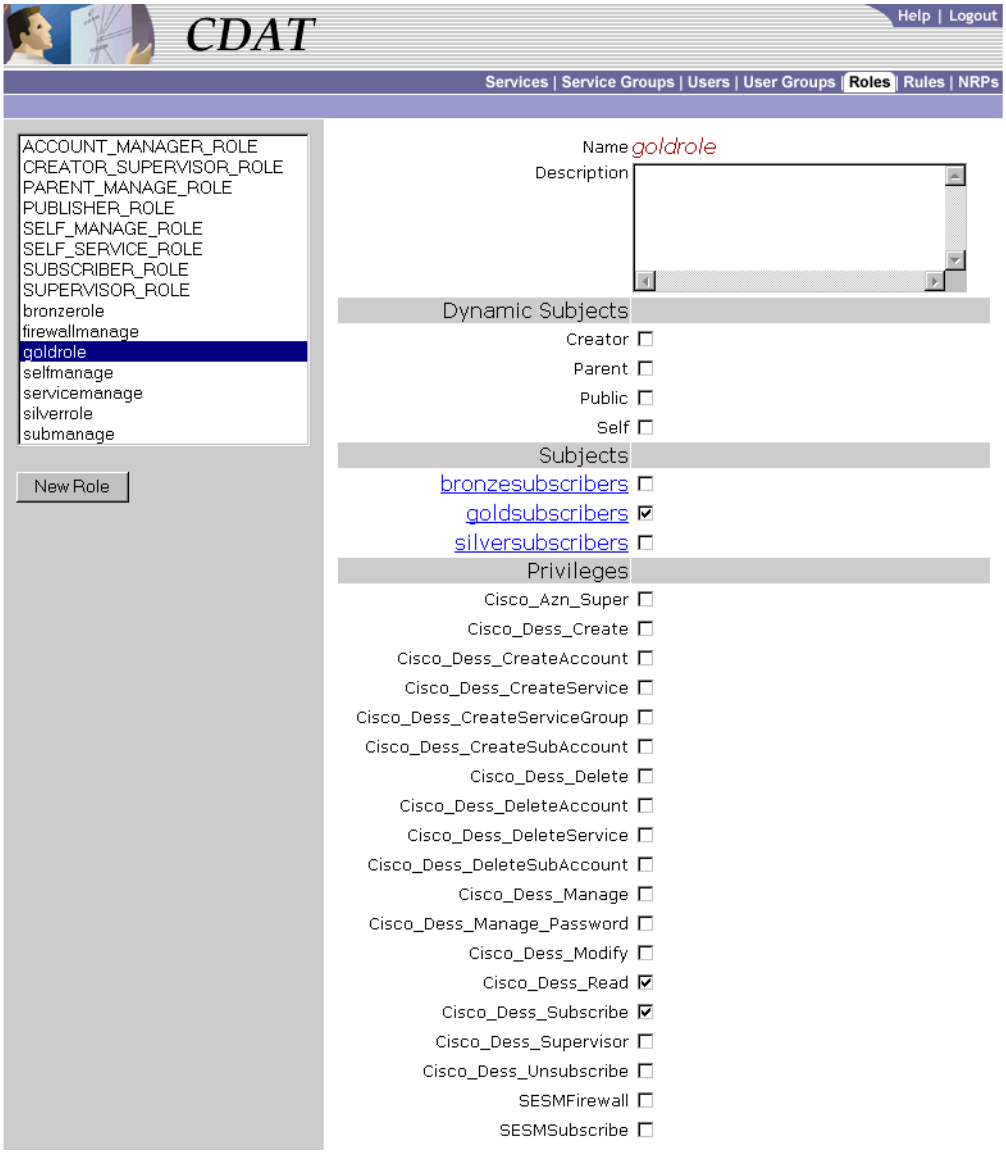
- The privileges needed for service subscription and unsubscription as described in the "Service Subscription Roles" section on page 2-42.
- Cisco_Dess_CreateSubAccount for creating subaccounts
- Cisco_Dess_DeleteSubAccount for deleting subaccounts
- Cisco_Dess_Read for reading objects and attributes (for example, for subscriber self-care)
- Cisco_Dess_Manage_Password for reading and changing passwords
- Cisco_Dess_Modify for changing attributes (for example, for subscriber self-care)

The subaccount user group is GoldSubscriberSubaccount and is associated with a GoldSubscriberSubaccountRole having all of the preceding privileges except for Cisco_Dess_CreateSubAccount and Cisco_Dess_DeleteSubaccount. Not granting these two privileges to the subaccount role makes it impossible for the subaccount user to create or delete a subaccount.

Roles Window

To create a new role or update the attributes of an existing role, use the Roles window (Figure 2-7).

Figure 2-7 Roles Window



When you first create a role, you click New Role and specify the following:

Name (Required)

Name of the role.

Allowed values: A text string.

Example: SubscriberRole

For a new or existing role, you can specify the following:

Description (Optional)

Gives a description of the role. The description is for informational purposes to help administrators when using this role.

Allowed values: A text string.

Dynamic Subjects (Optional)

Indicates dynamic subjects that will be role occupants. *Dynamic subjects* are users whose role occupancy is determined at run time. For example, the dynamic subject Self can be granted privileges at run time to objects whose creator name matches the login name specified when the user logs in to SESM or CDAT.

Dynamic subjects are as follows:

- Creator—A subject is classified as Creator if the creator name in the accessed resource is the same as the subject name in the submitted privilege token.
- Parent—A subject is classified as Parent if the parent name of the accessed resource is the same as the subject name in the submitted privilege token.
- Public—All subjects, whether authenticated or unauthenticated, are classified as Public.
- Self—A subject is classified as Self if the accessed resource name is the same as the subject name in the submitted privilege token.

Subjects (Optional)

Indicates the user groups that are occupants of this role. The user groups displayed were created with the User Groups window.

Privileges (Required)

Indicates those privileges that are associated with this role. Table 2-6 shows the privileges that can be chosen. In the table, the Who Is Granted? column indicates the category of user group that is typically granted this privilege and contains one or more of these types:

- Subscribers
- Publishers
- Account Managers
- Administrators

Table 2-6 uses the term *DESS objects* for all objects that can be created with CDAT other than roles and rules. Services, service groups, users, user groups, and NRPs are DESS objects. Roles and rules are AUTH objects. Cisco_Dess_* privileges pertain to DESS objects. Cisco_Azn_* privileges pertain to AUTH objects.

Note The SESMFirewall and SESMSubscribe privileges (shown in Table 2-6) pertain to and are enforced by an SESM web application such as NWSP. These two privileges are not DESS/AUTH privileges that are enforced by SPE.

When you use Table 2-6 to determine the privileges typically granted to a specific role, it might not be clear at first glance why a category of user groups such as administrators or subscribers is not explicitly granted certain privileges. Be aware that certain privileges may be implicitly granted by other privileges.

For example, Cisco_Dess_Supervisor (manage any DESS object) is a privilege that an administrator role is typically granted. If an administrator role has been explicitly defined to have Cisco_Dess_Supervisor privilege, you do not need to explicitly grant Cisco_Dess_Create (and many other privileges) to that role because many administrative privileges are implicit in Cisco_Dess_Supervisor.

Tip For some examples of the privileges that subscribers require, read the section "Subscriber Role Examples" section on page 2-41.

Table 2-6 Allowed Privileges for a Role

Privilege	Description	Who Is Granted?
Cisco_Azn_Super	Allows access to, creation, deletion, modification of a role or rule. Also allows assigning roles to subjects, policy rules to resources, and allows checking access on resources.	Administrators
Cisco_Dess_Create	Allows creation of user groups. Implied privileges: None	Administrators
Cisco_Dess_CreateAccount	Allows creation of users. Implied privileges: Cisco_Dess_CreateSubAccount	Account Managers
Cisco_Dess_CreateService	Allows creation of services. Implied privileges: None	Publishers
Cisco_Dess_CreateServiceGroup	Allows creation of service groups. Implied privileges: None	Publishers
Cisco_Dess_CreateSubAccount	Allows creation of subaccounts. Implied privileges: None	Subscribers
Cisco_Dess_Delete	Allows deletion of user groups. Implied privileges: None	Administrators
Cisco_Dess_DeleteAccount	Allows deletion of user accounts. Implied privileges: Cisco_Dess_DeleteSubAccount	Account Managers
Cisco_Dess_DeleteService	Allows deletion of services. Implied privileges: None	Publishers
Cisco_Dess_DeleteSubAccount	Allows deletion of subaccounts. Implied privileges: None	Subscribers
Cisco_Dess_Manage	Allows managing of DESS objects, including changing the set of attributes associated with these objects. Implied privileges: Cisco_Dess_Create, Cisco_Dess_CreateAccount, Cisco_Dess_CreateService, Cisco_Dess_CreateServiceGroup, Cisco_Dess_CreateSubAccount, Cisco_Dess_Delete, Cisco_Dess_DeleteAccount, Cisco_Dess_DeleteService, Cisco_Dess_DeleteSubaccount, Cisco_Dess_ManagePassword, Cisco_Dess_Modify, Cisco_Dess_Read, Cisco_Dess_Subscribe, Cisco_Dess_Unsubscribe	Administrators and Subscribers (with the subject Self)

Table 2-6 Allowed Privileges for a Role (continued)

Privilege	Description	Who Is Granted?
Cisco_Dess_Manage_Password	Allows reading and changing of passwords on user objects. This privilege grants modify rights to the set of attributes associated with the passwords. Implied privileges: None	Subscribers
Cisco_Dess_Modify	Allows changes to attributes for DESS objects. Implied privileges: None	Subscribers
Cisco_Dess_Read	Allows reading of DESS objects and their attributes. Cisco_Dess_Read privilege is needed for displaying services and, therefore, is needed for service subscription. For information on service-subscription privileges, see the "Service Subscription Roles" section on page 2-42. Implied privileges: None	Subscribers
Cisco_Dess_Subscribe	Allows subscription to a service. For information on service-subscription privileges, see the "Service Subscription Roles" section on page 2-42. Implied privileges: Cisco_Dess_Unsubscribe	Subscribers
Cisco_Dess_Supervisor	Allows management of DESS objects, including changing the set of attributes associated with these objects. Cisco_Dess_Supervisor and Cisco_Dess_Manage are identical. Implied privileges: Cisco_Dess_Create, Cisco_Dess_CreateAccount, Cisco_Dess_CreateService, Cisco_Dess_CreateServiceGroup, Cisco_Dess_CreateSubAccount, Cisco_Dess_Delete, Cisco_Dess_DeleteAccount, Cisco_Dess_DeleteService, Cisco_Dess_DeleteSubaccount, Cisco_Dess_Manage, Cisco_Dess_ManagePassword, Cisco_Dess_Modify, Cisco_Dess_Read, Cisco_Dess_Subscribe, Cisco_Dess_Unsubscribe	Administrators
Cisco_Dess_Unsubscribe	Allows unsubscription to a service. For information on service-subscription privileges, see the "Service Subscription Roles" section on page 2-42. Implied privileges: None	Subscribers
SESMFirewall	Allows an SESM web application to display the MY FIREWALL button that the user clicks for firewall management. For information firewall-related privileges, see the "Firewall-related Roles" section on page 2-42. Implied privileges: None	Subscribers
SESMSubscribe	Allows an SESM web application to display the MY SERVICES button that the user clicks for service subscriptions. For information on service-subscription privileges, see the "Service Subscription Roles" section on page 2-42. Implied privileges: None	Subscribers

Creating and Updating Rules

A *rule* defines the set of conditions under which a role is associated with one or more resources. User groups can be made occupants of one or more roles. In this way, an administrator can define the resources that can be accessed by members of a user group.

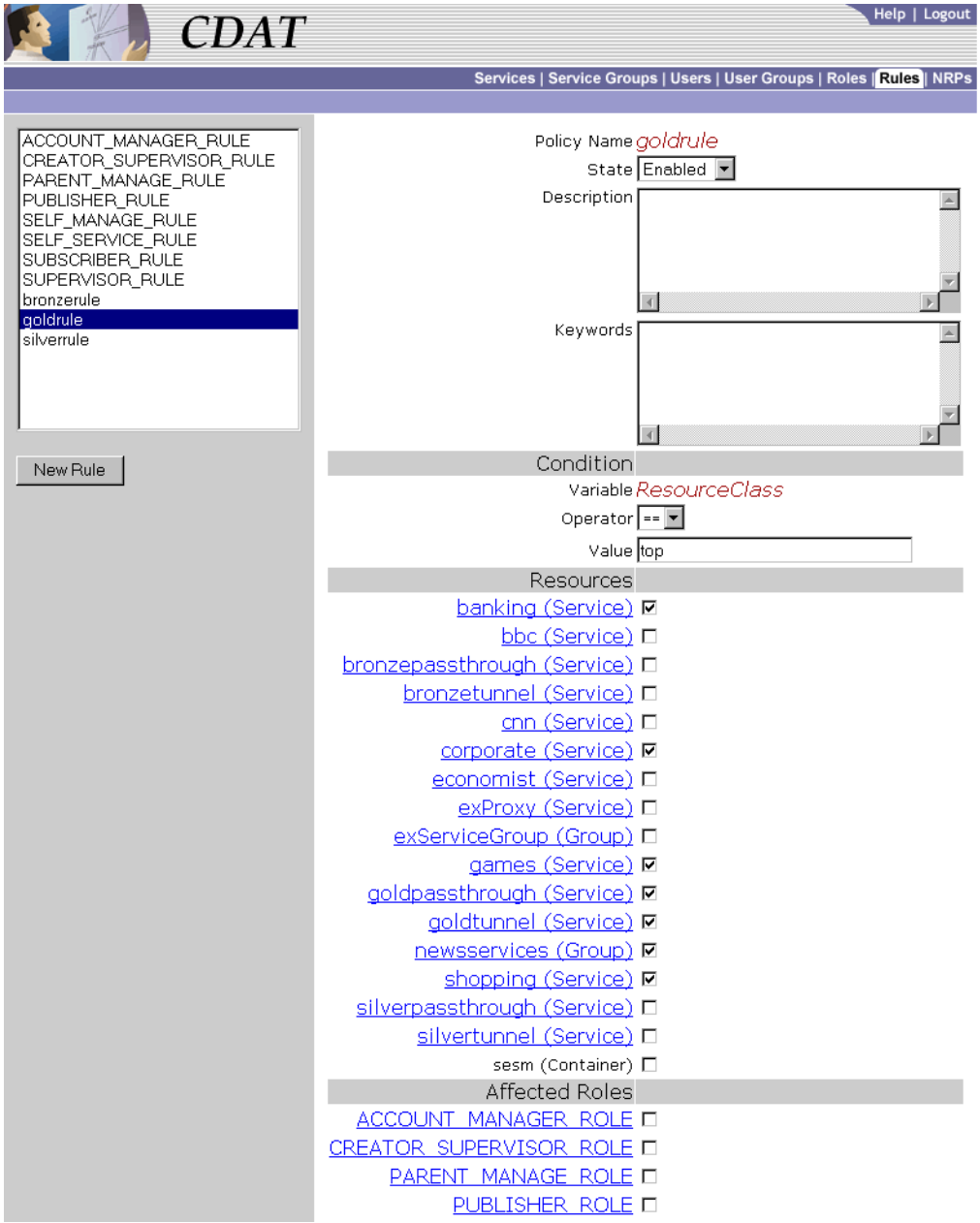
Predefined Rules

If the RBAC objects were installed when the DESS software was installed, CDAT displays a set of predefined rules in the list of rules. For information on the predefined rules, see Appendix A, "Predefined Roles and Rules."

Rules Window

To create a new rule or update the attributes of an existing rule, use the Rules window (Figure 2-8).

Figure 2-8 Rules Window



When you first create a rule, you click New Rule and specify the following:

Name (Required)

Name of the rule.

Allowed values: A text string.

Example: SubscriberRule

For a new or existing rule, you can specify the following:

State (Required)

Indicates the state of the rule: Enabled, Disabled, or Debug. This attribute is not currently used. A rule is always enabled.

Allowed values: Enabled

Description (Optional)

Gives a description of the rule. The description is for informational purposes to help administrators when using this rule.

Allowed values: A text string.

Keywords (Optional)

Specifies a keyword that helps an administrator locate the policy objects applicable to them.

Allowed values: Currently, the keyword `CISCO_AZN` indicates authorization policies and is the only keyword used.

Condition

The *condition* for a rule specifies whether the set of actions associated with the rule should be executed or not. The fields under Condition give the three elements of the rule's condition:

```
Variable Operator Value
```

For example:

```
ResourceClass==top
```

The preceding condition is the only condition currently used with Cisco SESM and CDAT. This condition always evaluates to true. Therefore, the privileges granted by the roles can be exercised. The roles chosen in Affected Roles determine the set of roles to which the rule applies.

Variable (Read Only)

Specifies a variable for the condition: an attribute that should be matched when evaluating the condition.

Allowed values: Currently, `ResourceClass` is the only variable used.

Operator (Required)

Specifies an operator for the condition.

Allowed values: Currently, the `==` operator is the only operator used.

Value (Required)

Specifies a value against which the variable is to be compared when evaluating the condition.

Allowed values: Currently, the value `top` is the only value used.

Resources (Required)

Indicates the resources (services, service groups, or containers) that will be associated with the rule. The services and service groups that CDAT displays were created with, respectively, the Services and Service Groups windows. The containers that CDAT displays were created with the object management facility used for the LDAP directory.

Affected Roles (Required)

For each role, indicates whether the role is associated with the rule.

Creating and Updating NRP Information

CDAT allows creation of NRP-related information in an NRP object. Currently, NRP-related information is for a next-hop table.

Because multiple NRP-SSGs might access services from different networks, each service profile can specify a next-hop key, which is a string identifier, rather than an actual IP address. For each service, use the Services window's Next hop gateway box to specify the next-hop key for the service.

For each NRP-SSG to determine the IP address associated with the next-hop key, each NRP-SSG downloads its own next-hop table that associates keys with IP addresses. In the NRPs window, you use the Next Hop Table box to define the entries in the next-hop table for each NRP-SSG. The name of the next-hop table is the name that you give when you click New NRP.

Using a Next-Hop Table

To create and download a next-hop table that an NRP-SSG can use to access services from different networks, do the following:

Step 1 For each service, use CDAT and the Next hop gateway box in the Services window to specify the next-hop key for the service.

Step 2 For each NRP-SSG, use CDAT to create a next-hop table.

a. In the NRPs window, click New NRP to create a next-hop table for the NRP, and specify the name for the next-hop table in the Name box. With CDAT, the next-hop table takes its name from the name of the NRP.

b. In the Next Hop Table box, define the entries in the next-hop table for the NRP-SSG. For example:

```
service3=192.168.103.3
service2=192.168.103.2
service1=192.168.103.1
Worldwide_Gaming=192.168.4.2
```

Step 3 On the RADIUS Data Proxy (RDP) server, specify the next-hop table password that will be used to access the next-hop table. The next-hop table password is specified in the \rdp\config\rdp.xml file:

```
<!-- Following attribute and type handle next hop profiles -->
<Call name="setAttribute">
<Arg>PASSWORD:nexthopcisco</Arg>
<Arg>NextHopRequest</Arg>
</Call>
```

By default, the password is nexthopcisco.

Step 4 On each NRP-SSG, use the following command to download the appropriate next-hop table:

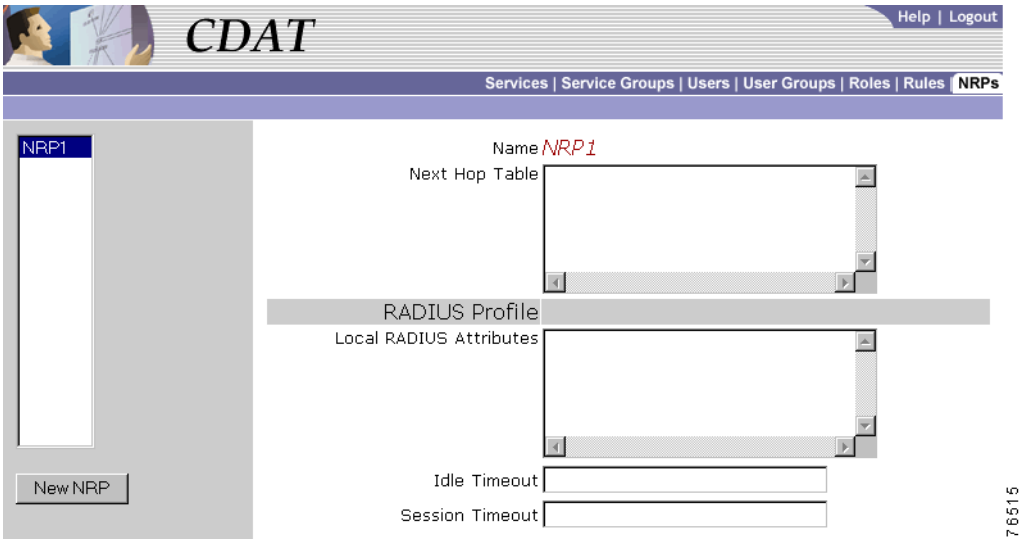
ssg next-hop download *next-hop_table_name* *next-hop_table_password*

In the preceding command, *next-hop_table_name* is the name you specified when creating the next-hop table (Step 2a). The *next-hop_table_password* is the password that is defined in the rdp.xml file (Step 3). For information on the **ssg next-hop** command, see the *Service Selection Gateway* document.

NRPs Window

To create or update information for an NRP, use the NRPs window (Figure 2-9) Currently, the only information you can create is a next-hop table.

Figure 2-9 NRPs Window



The NRPs window allows you to create a next-hop table. When you first create a next-hop table, you click New NRP and specify the following:

Name (Required)

Name of the NRP. The next-hop table takes its name from the name that you specify for the NRP object.

Allowed values: A text string.

Example: nrp1

For a new or existing next-hop table, you can specify the following:

Next Hop Table (Required)

Specifies a key and an IP address for each entry in the next-hop table.

Allowed values: A key and an IP address, separated by an equal sign. Each next-hop table entry is on a separate line:

key=ip_address

In the preceding entry, *key* is the key for the service specified with CDAT in the Next hop gateway box of the Services window. The *ip_address* is IP address of the next hop for this service.

Example:

```
service3=192.168.103.3
service2=192.168.103.2
service1=192.168.103.1
Worldwide_Gaming=192.168.4.2
```

RADIUS Profile

Local RADIUS Attributes (Not Currently Used)

Reserved for future use.

Idle Timeout (Not Currently Used)

Reserved for future use.

Session Timeout (Not Currently Used)

Reserved for future use.

Predefined Roles and Rules

A set of predefined RBAC roles and rules are installed when the SPE software is installed if the RBAC objects are chosen for installation. You can use the predefined roles and rules as models for the roles and rules that your deployment will use. This appendix explains the predefined roles and rules.

Predefined Roles

The SPE software provides the set of predefined roles described in Table A-1. You can use a predefined role as it exists or use it as a model for creating a similar role with a modified set of privileges.

Table A-1 SPE Predefined Roles

Predefined Role	Privileges	Dynamic Subject Occupants
ACCOUNT_MANAGER_ROLE	Cisco_Dess_CreateAccount Cisco_Dess_DeleteAccount Cisco_Dess_CreateSubAccount Cisco_Dess_DeleteSubAccount	None
CREATOR_SUPERVISOR_ROLE This is a superuser role and should not be deleted.	Cisco_Dess_Supervisor Cisco_Azn_Super	Creator
PARENT_MANAGE_ROLE	Cisco_Dess_Manage	Parent
PUBLISHER_ROLE	Cisco_Dess_CreateService Cisco_Dess_CreateServiceGroup Cisco_Dess_DeleteService Cisco_Dess_Subscribe	None
SELF_MANAGE_ROLE	Cisco_Dess_Manage	Self
SELF_SERVICE_ROLE	Cisco_Dess_Manage_Password Cisco_Dess_Modify Cisco_Dess_Read	Self
SUBSCRIBER_ROLE	Cisco_Dess_Subscribe	None
SUPERVISOR_ROLE	Cisco_Azn_Super Cisco_Dess_Supervisor	None

Predefined Rules

Each predefined role (Table A-1) has a corresponding a predefined rule. Table A-2 lists the predefined rules. For example, the ACCOUNT_MANAGER_ROLE is the affected role in the ACCOUNT_MANAGER_RULE. The predefined rules specify the conditions and the resources for the privileges granted by the corresponding role. For the predefined rules (for example, SUBSCRIBER_RULE) where no resources are specified, the service-provider administrator can update the rule and define resources after the RBAC objects are installed.

Table A-2 SPE Predefined Rules

Predefined Rule	Corresponding Role
ACCOUNT_MANAGER_RULE	ACCOUNT_MANAGER_ROLE
CREATOR_SUPERVISOR_RULE	CREATOR_SUPERVISOR_ROLE
PARENT_MANAGE_RULE	PARENT_MANAGE_ROLE
PUBLISHER_RULE	PUBLISHER_ROLE
SELF_MANAGE_RULE	SELF_MANAGE_ROLE
SELF_SERVICE_RULE	SELF_SERVICE_ROLE
SUBSCRIBER_RULE	SUBSCRIBER_ROLE
SUPERVISOR_RULE	SUPERVISOR_ROLE

Two of the predefined rules have resources defined: SELF_MANAGE_RULE and SUPERVISOR_RULE. In both cases, the resources are defined as the Organizational Unit container (for example, ou=sesm, o=cisco) where the CDAT/SPE objects are created. Therefore, the privileges are for all applicable resources in the sesm Organizational Unit of the cisco Organization. The sesm Organizational Unit and cisco Organization are the default values when the SESM software is installed. The installer can change these values during the SPE software installation.

SPE Schema Extensions

This appendix describes the LDAP directory schema extensions that are installed with the Cisco Security Policy Engine (SPE) software and that are used by the SPE Directory Enabled Service Selection and Authorization (DESS/AUTH) component.

Some DESS/AUTH objects may contain more attributes than are documented in this appendix. Only those attributes that are used in the current release are documented.

Cisco Schema Extensions

The SPE schema extensions include the Cisco 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; not currently used.
- *CiscoAznPrivileges*—multivalue Distinguished Name (dn); not currently used.
- *CiscoAznResourceName*—single-value case-ignore string; not currently used.
- *CiscoAznRoleList*—multivalue 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*.
- *description*—multivalue string that describes the condition

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*—multivalue 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*—multivalue 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*—multivalue case-ignore string containing a list of valid privileges
- *CiscoAznRoleOccupants*—multivalue 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-value case-ignore string which specifies a condition (filter) determining role occupancy; not currently used.
- *CiscoAznDenyRoleOccupancy*—multivalue Distinguished Name (dn) which lists users or groups to be denied occupancy; not currently used.
- *CiscoAznSuperiorRole*—single-value Distinguished Name (dn) which specifies the role object that is superior to this role (and from which privileges and occupants are inherited)
- *CiscoAznSubordinateRoles*—multivalue Distinguished Name (dn) which specifies roles that are subordinate to this role; not currently used.

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*—multivalue Distinguished Name (dn) which lists the roles occupied by this object
- *CiscoAznBlockedRoleList*—multivalue Distinguished Name (dn) which lists the roles that have been blocked for this object
- *groupMembership*—multivalue Distinguished Name (dn) which lists the user groups that the user belongs to

OID: 1.2.840.113548.3.2.6.7

CiscoAznSubordinateSubjectAux

Specifies a subordinate subject.

Type: Auxiliary

Superior Class: top

Attributes:
- *CiscoAznParentSubject*—single-value 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 RDP 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: CiscoDESSService

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:

- *C*—single-value string that specifies the ISO 3166 two-character country code of the user
- *CiscoDESSGender*—single-value integer (0 male; 1 female)
- *CiscoDESSHobbies*—multivalue case-ignore string
- *CiscoDESShomeURL*—single-value string that specifies the home URL of the user
- *CiscoDESSageGroup*—single-value string that specifies the age group of the user
- *CiscoDESStimeZone*—single-value string that specifies the time zone of the user
- *Initials*—multivalue case-ignore string that specifies the initials of the user
- *DisplayName*—multivalue case-ignore string that specifies the preferred name to be used when displaying the user's name
- *Language*—single-value string that specifies the ISO 639 2-character language code for the user

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*—multivalue string

OID: 1.2.840.113548.3.2.7.5

CiscoDESSradiusProfileAux

RADIUS attributes for a user or service.

Type: Auxiliary

Superior Class: top

Attributes:

- *CiscoDESSapplicableClassRADIUS*—single-value case-ignore string which specifies the applicable class for RADIUS 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*—multivalue 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*, *proxy*, and *tunnel* services.

Type: Abstract

Superior Class: top

Naming: Common Name (cn)

Containment: Organization (o)
Organization Unit (ou)

Attributes:

- *CiscoDESSserviceRoute*—(required) multivalue case-ignore 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 RDP translator will encode this attribute (if needed) in the following format:

```
Raddress;mask
```

- *CiscoDESSnextHopGatewayKey*—single-value case-ignore string that specifics the next-hop key for this service. The RDP translator will encode this attribute, if needed, as follows:

  G*key*

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

```
Concurrent
Sequential
```

  The RADIUS Data Proxy (RDP) translator will encode this attribute, if needed, as follows:

  M*S* or M*C*

- *CiscoDESSdomainName*—multivalue case-ignore string that specifies domain names to be resolved by the specified DNS server
- *CiscoDESSpoolName*—single-value string which specifies the name of the local address pool for the service
- *CiscoDESSprimaryDNSServer*—multivalue case-ignore string that specifies the primary DNS servers for this service. The RDP translator will encode this attribute, if needed, in the following format:

```
Dprimary;secondary;secondary
```

- *CiscoDESSserviceType*—single-value case-ignore string which specifies the level of service; must have the following value:

```
outbound
```

- *CiscoDESSserviceURL*—single-value string which specifies the URL for the service
- *CiscoDESSsecondaryDNSServer*—multivalue case-ignore string which specifies the secondary DNS servers for this service

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:

- *CiscoDESSconnectMutex*—single-value integer (0 false; 1 true) that specifies whether the service group is a mutually-exclusive connection group in which the user can connect to only one service in the group at a time
- *CiscoDESSsubscribeMutex*—single-value integer (0 false; 1 true) that specifies whether the service group is a mutually-exclusive subscription group in which the user can subscribe to only one service in the group at a time
- *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:

- *CiscoDESSaccountActive*—single-value integer (0 false; 1 true) that specifies whether the account is active
- *CiscoDESSallowCreateSubAccounts*—single-value integer that specifies whether a user can create sub-accounts
- *CiscoDESSblockServiceInheritance*—single-value integer (0 false; 1 true) that specifies whether subaccounts created by this user inherit service subscriptions from this user account (the parent account) or the container
- *CiscoDESSautoLogonService*—multivalue 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*—multivalue case-ignore string; can be used to store any application-specific information; DESS does not interpret this attribute
- *CiscoDESShomeURL*—single-value string that specifies the home URL of the user
- *CiscoDESSmaxSubAccounts*—single-value integer that specifies whether the maximum number of subaccounts allowed for this account is
- *CiscoDESSpoolName*—single-value case-ignore string; represents the name of the pool.
- *CiscoDESSprimaryService*—single-value Distinguished Name (dn); represents the primary service for the user
- *CiscoDESSserviceFilter*—multivalue Distinguished Name (dn) which lists the set of services that are blocked for (not inherited by) this user
- *CiscoDESSsubscribedServices*—multivalue Distinguished Name (dn) that specifies the services to which the user has subscribed (may be a service name or service group name)
- *CiscoDESSsubscriptionProperties*—multivalue string that specifies subscription properties of the user
- *CiscoDESStcpRedirect*—multivalue string that specifies one or more vendor-specific RADIUS attributes related to TCP redirection
- *CiscoDESSunsubscribedServices*—multivalue Distinguished Name (dn) that specifies the services to which the user has unsubscribed (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
CiscoDESSaccountActive
CiscoDESSageGroup
CiscoDESSallowCreateSubAccounts
CiscoDESSapplicableClassACL
CiscoDESSapplicableClassRadius
```

```
CiscoDESSautoLogonService
CiscoDESSblockServiceInheritance
CiscoDESSciscoAVPair
CiscoDESSclearpassword
CiscoDESSciscoAVPair
CiscoDESSconnectMutex
CiscoDESSdomainName
CiscoDESSenableSingleSignon
CiscoDESSGender
CiscoDESSgenericAttribute
CiscoDESSHobbies
CiscoDESShomeURL
CiscoDESSidleTimeout
CiscoDESSmaxSubAccounts
CiscoDESSmemberServices
CiscoDESSnextHopGatewayEntry
CiscoDESSnextHopGatewayKey
CiscoDESSpoolName
CiscoDESSprimaryService
CiscoDESSprimaryDNSServer
CiscoDESSradiusAttr
CiscoDESSradiusServer
CiscoDESSsecondaryDNSServer
CiscoDESSserviceFilter
CiscoDESSserviceRoute
CiscoDESSserviceType
CiscoDESSserviceURL
CiscoDESSsessionTimeout
CiscoDESSsubscribedServices
CiscoDESSsubscribeMutex
CiscoDESSsubscriptionProperties
CiscoDESStcpRedirect
CiscoDESStimezone
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

CiscoDESSaccountActive

Type: single-value integer

OID: 1.2.840.113548.3.1.7.39

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

CiscoDESSconnectMutex

Type: single-value integer

OID: 1.2.840.113548.3.1.7.44

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

CiscoDESSmaxSubAccounts

Type: single-value integer

OID: 1.2.840.113548.3.1.7.40

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

CiscoDESSsubscribedServices

Type: multivalue dn

OID: 1.2.840.113548.3.1.7.22

CiscoDESSsubscribeMutex

Type: single-value integer

OID: 1.2.840.113548.3.1.7.43

CiscoDESSsubscriptionProperties

Type: multivalue string

OID: 1.2.840.113548.3.1.7.41

CiscoDESStcpRedirect

Type: multivalue string

OID: 1.2.840.113548.3.1.7.42

CiscoDESStimeZone

Type: single-value directory string

OID: 1.2.840.113548.3.1.7.38

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*—multivalue case-exact string containing a set of keywords to assist directory clients in locating policy objects applicable to them. Each value of the multivalue attribute contains a single keyword.
- *cimCaption*—string containing a 1-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*—multivalue 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
policyConditionGroupNumber
policyConditionName
policyConditionNegated
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 SPE 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*—multivalue string; name of the group
- *description*—multivalue string; description of the group
- *uniqueMember*—multivalue dn

OID: 2.5.6.9

inetOrgPerson

Type: Structural

Superior Class: organizationalPerson

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

OID: 2.16.840.1.113730.3.2.2

organizationalPerson

Type: structural

Superior Class: person

Attributes:
- *facsimileTelephoneNumber*—multivalue facsimile telephone number
- *postalAddress*—multivalue postal address
- *stree*t—multivalue string

OID: 2.5.6.7

organizationalUnit

Type: structural

Superior Class: ndsLoginProperties
ndsContainerLoginProperties

Attributes:
- *facsimileTelephoneNumber*—multivalue facsimile telephone number
- *postalAddress*—multivalue postal address
- *stree*t—multivalue string

OID: 2.5.6.5

person

Type: structural

Superior Class: ndsLoginProperties

Attributes:
- *telephoneNumber*—multivalue telephone number
- *city*—multivalue string
- *st*—multivalue string

OID: 2.5.6.6

Attributes

The core LDAP classes use the following attributes. Only those attributes 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
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

RDP Service-Profile Translation

This appendix provides information on the translation that the RADIUS Data Proxy (RDP) server performs for the service-profile attributes that CDAT creates in the LDAP directory.

The content of the service profile that you create with CDAT is derived from a RADIUS service profile. When the SSG gets information about services, the SSG uses the RADIUS protocol and expects RADIUS service-profile attributes.

In an SESM system, the RDP server is a RADIUS proxy server that acts as a mediator between the SSG and the LDAP directory. For example, RDP uses the DESS programming interfaces to access service profiles in the LDAP directory. RDP translates the CDAT/DESS service-profile attributes into the RADIUS service-profile attributes that the SSG uses.

The three tables in this appendix list the CDAT-to-RADIUS translations that RDP performs for a service profile.

Note The information in this appendix may be useful to you if you are reading SSG documentation, which discusses only RADIUS attributes, and you need to know what RADIUS attribute corresponds to each CDAT attribute in a service profile.

Table C-1 shows the CDAT attributes for a service that RDP translates into standard RADIUS attributes.

Table C-1 Standard RADIUS Attributes

CDAT attribute	Standard RADIUS Attribute Sent to the SSG
Service type	Standard RADIUS attribute number 6. Service type. The value must be outbound.
Session Timeout	Standard RADIUS attribute number 27. Maximum time, in seconds, that a host or service object can remain active in any one session.
Idle Timeout	Standard RADIUS attribute number 28. Maximum time, in seconds, that a service connection can remain idle before it is disconnected.

Table C-2 shows the CDAT attributes for a service that RDP translates into RADIUS Service-Info attributes. Service-Info attributes are vendor-specific attributes (attribute number 26), vendor 9, subattribute 251.

Table C-2 Service-Info Attributes

CDAT attribute	Service-Info Attribute Sent to the SSG
Service class	**T***type* Type of service. Valid values for *type* are: • P—Passthrough service • T—Tunneled service • X—Proxy service
Access mode	**M***mode* Service mode. Valid values for *mode* are: • S—Sequential mode • C—Concurrent mode
Description	**I***description* Service description where *description* is the text string for the description.
Next hop gateway	**G***key* Next-hop key where *key* is the text string for the key.
Domain names	**O***name1[name2]...[;nameX]* Domain names where *name1*, *name2,* and so forth are the domain names.
Primary DNS servers Secondary DNS servers	**D***ip_address_1[;ip_address_2]* The primary and secondary DNS servers for this service. *ip_address1* and *ipaddress2* are the IP addresses for, respectively, the primary and secondary DNS servers.
Service routes	**R***ip_address;subnet_mask* Service routes (destinations) where the service is located. *ip_address* and *subnet_mask* are the IP address and subnet mask for a destination. Multiple instances of this attribute in a single service profile specify multiple service destinations.
Service URL	**U***url* or **H***url* Service URL where *url* is a fully qualified URL.
RADIUS server IP address RADIUS server authentication port RADIUS server accounting port RADIUS shared secret	**S***RadiusServerAddress;authPort;acctPort;secret* Remote RADIUS server information where: • *RadiusServerAddress* is the server IP address. • *authPort* is the server authentication port. • *acctPort* is the server accounting port. • *secret* is the server shared secret.

Table C-3 shows the CDAT attributes for a service that RDP translates into Cisco AVPair attributes. Cisco AVPair attributes are vendor-specific attributes (attribute number 26), vendor 9, subattribute 1.

Table C-3 Cisco AV-Pair Attributes

CDAT attribute	Cisco AVPair Sent to the SSG
Tunnel identifier	**vpdn:tunnel-id=***name* Tunnel identifier where *name* is the name of tunnel.
Tunnel IP address	**vpdn:ip-addresses=***ip_address* Tunnel IP address where *ip_address* is the address of the home gateway (LNS) to receive the L2TP connection.
Tunnel password	**vpdn:l2tp-tunnel-password=***password* Tunnel password where *password* is the password for L2TP tunnel authentication.
Tunnel type	**vpdn:tunnel-type=***type* Tunnel type where *type* is the l2tp (the only value allowed with SESM).
Pool name and IP Pool Name	**ip:addr-pool=***pool_name* Local address pool where *pool_name* is the name of the address pool.

CDAT allows the service provider to explicitly define additional Cisco AV pairs for a service using the Local RADIUS Attributes box in the Services and Service Groups windows. RDP sends these AV pairs to the SSG exactly as they are specified. For information on these AV pairs, see the "RADIUS Profile" section on page 2-19.

For more information on RADIUS profiles and the SSG, see the *Service Selection Gateway* document and the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*.

A

B

C

D

E

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X