CHAPTER 2

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 1-4
- 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 2-7
- Creating and Updating Users and User Groups, page 2-19
- Creating and Updating Roles, page 2-34
- Creating and Updating Rules, page 2-39
- Creating and Updating NRP Information, page 2-42

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.

Using the CDAT Expert Interface: An Example

As a simple example of the tasks that an administrator performs when using the CDAT interface, consider possible tasks in creating 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 and Subscriber Policy Engine Installation and Configuration Guide.*

Logging into CDAT for the First Time

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

To log in to CDAT for the first time, you need a user name and password. The administrator who logs in first needs administrative privileges to begin the work of setting up the objects and attributes for services, subscribers, policy roles and rules, and so forth.

The easiest way to create an administrator user account for CDAT is to use some DESS sample data that the SESM installation program copies onto the CDAT server machine when it installs the CDAT and DESS software. The DESS sample data creates users (including an administrator user), users groups, services, roles, and rules. The DESS sample data is located in the *install_dir*/dess-auth/schema/samples directory, and is contained in two files: DESSadmin.ldf and DESSusecasedata.ldf.

You must manually install the DESS sample data with a facility such as **ldapmodify**. For information on installing the DESS sample data, see the following file:

install_dir/dess-auth/schema/README.LDIFload.html

After the DESS sample data is successfully installed, you can use the DemoUser5 user name (password cisco) to log in to CDAT for the first time. The DemoUser5 account is an administrative account with Cisco_Dess_Supervisor and Cisco_Azn_Super privileges, which are appropriate for a superuser-type administrator. The Demo5User can access all objects in the Organization Unit and can perform all CDAT tasks: access, create, delete, and modify all objects and attributes. The Demo5User can create user accounts, roles, and rules for all users, including administrators, account managers, and publishers.

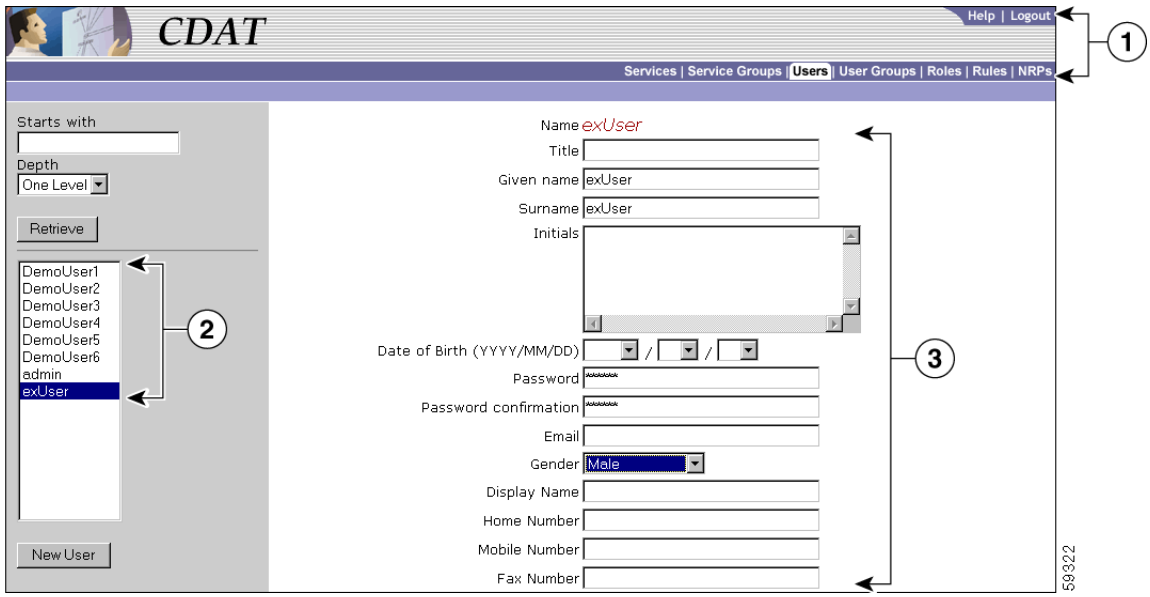
Note If your CDAT uses DemoUser5 and the other sample DESS objects, changing CDAT administrator passwords is a needed security precaution for production deployments of SESM and CDAT.

Your first task after logging in for the first time as DemoUser5 should be to change the passwords associated with all CDAT administrator user accounts, including DemoUser3 and DemoUser5. CDAT administrator user accounts are members of user groups that occupy roles with administrative privileges (for example, Cisco_Dess_Supervisor, Cisco_Dess_Manage, and Cisco_Azn_Super). With CDAT, passwords must have at least one character.

Using the CDAT Expert Interface

The CDAT expert interface (Figure 2-1) allows you to create or update information for services, service groups, users, user groups, roles, rules, and NRPs.

Figure 2-1 CDAT Expert Interface



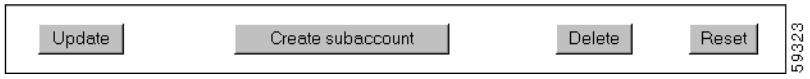
1	Navigation Bar
2	Navigation List
3	Object Details

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.

Other CDAT Expert Interface Considerations

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

- Name Space, page 2-5
- Visibility of and Access to Objects, page 2-5
- Attribute Values and Inheritance, page 2-6
- User Passwords, page 2-6
- CDAT Configuration Attributes, page 2-7

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 2-1 lists the CDAT inheritable attributes.

Table 2-1 Inheritable Attributes

Inheritable Attribute	Where Used
Idle Timeout	Services, Service Groups, Users, and User Groups
Local Generic 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

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.

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 and Subscriber Policy Engine 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 2-42.

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

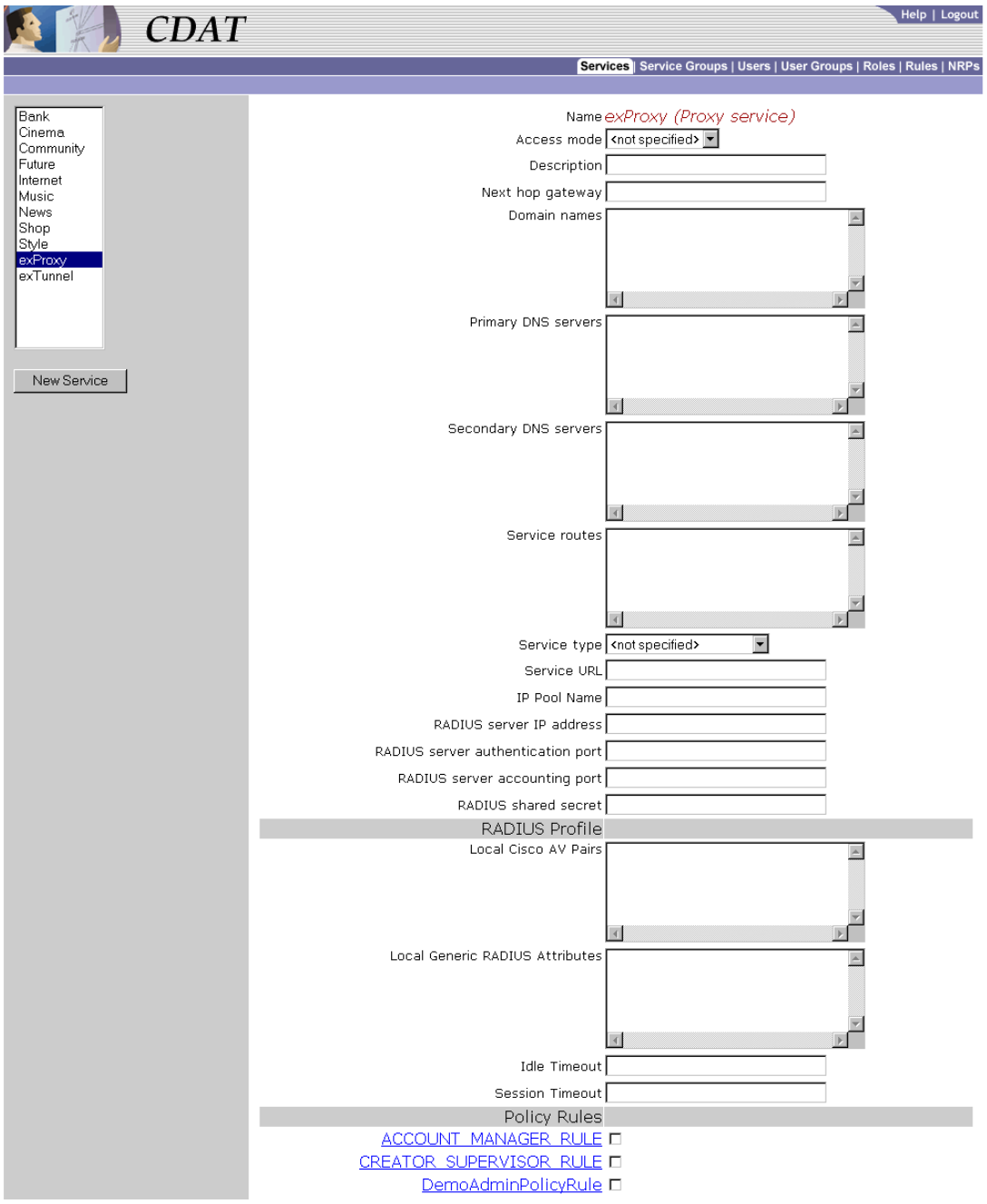
For each service, you specify an access mode in the Access mode box in the Services window. SSG services can be configured for concurrent or sequential access. Concurrent access allows users to log on to this service while simultaneously connected to other services. Sequential access requires that the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

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 icons are not used for services in the list.

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 2-7.

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 2-8 and the "Creating and Updating NRP Information" section on page 2-42.

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 2-9.

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 2-8.

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 2-20.

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 *Cisco 6400 Feature Guide*.

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

Local Cisco AV Pairs

Cisco attribute-value pairs (Cisco AV pairs) can appear as part of the service profile.

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

With CDAT, the most common format for each AV pair is as follows:

protocol:*attribute*=*value*

For use with Cisco SESM and CDAT, the preceding format has these elements:

- *protocol* is typically AIRNET, IP, IPX, OUTBOUND, RSVP, SHELL, SIP, VOIP, or VPDN.

- *attribute* is one of the attributes listed in Table 2-2.
- *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:

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

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

Table 2-2 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.

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.

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

Attribute Format	Description
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.
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.*

Local Generic RADIUS Attributes (Optional)

One or more RADIUS attributes and values that apply to the service but that do not appear in the fields of the Services window. For information on RADIUS attributes, see RFC 2865.

Allowed values: A RADIUS attribute number and a value in the form *99*:*value*, where *99* is the RADIUS attribute number. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

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.

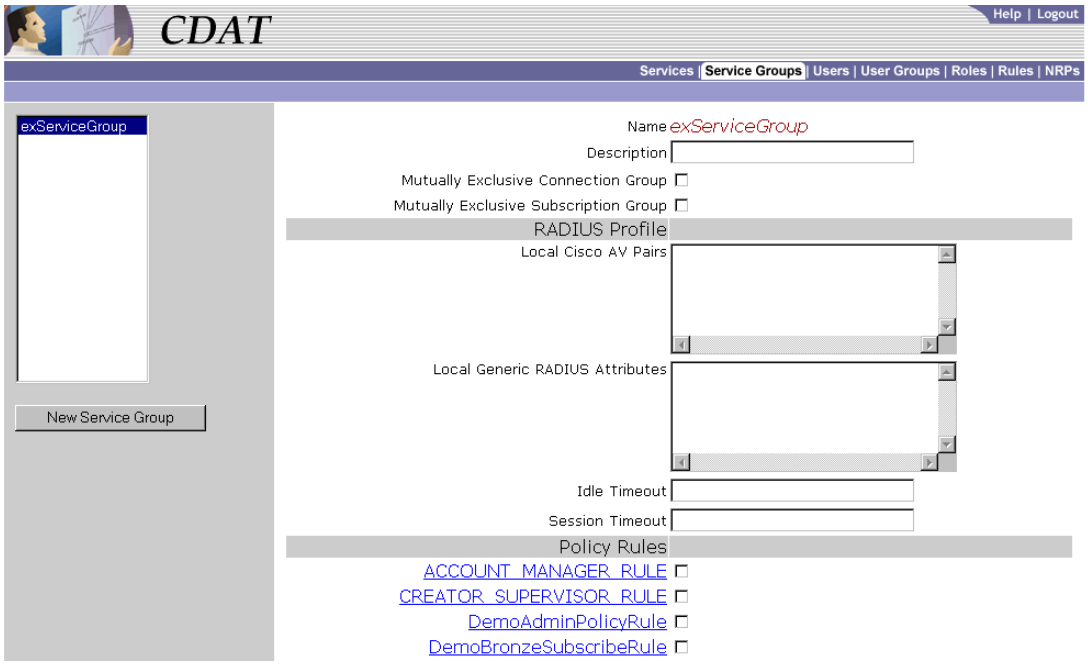
Policy Rules

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 2-39.

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.

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

Local Cisco AV Pairs (Optional)

Cisco attribute-value pairs (Cisco AV pairs) can appear as part of the service group profile. 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, see Table 2-2.

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

Local Generic RADIUS Attributes (Optional)

One or more RADIUS attributes and values that apply to all services in the group but that do not appear in the fields of the Service Groups window. For information on RADIUS attributes, see RFC 2865.

Allowed values: A RADIUS attribute number and a value in the form *99*:*value*, where *99* is the RADIUS attribute number. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

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 2-39.

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

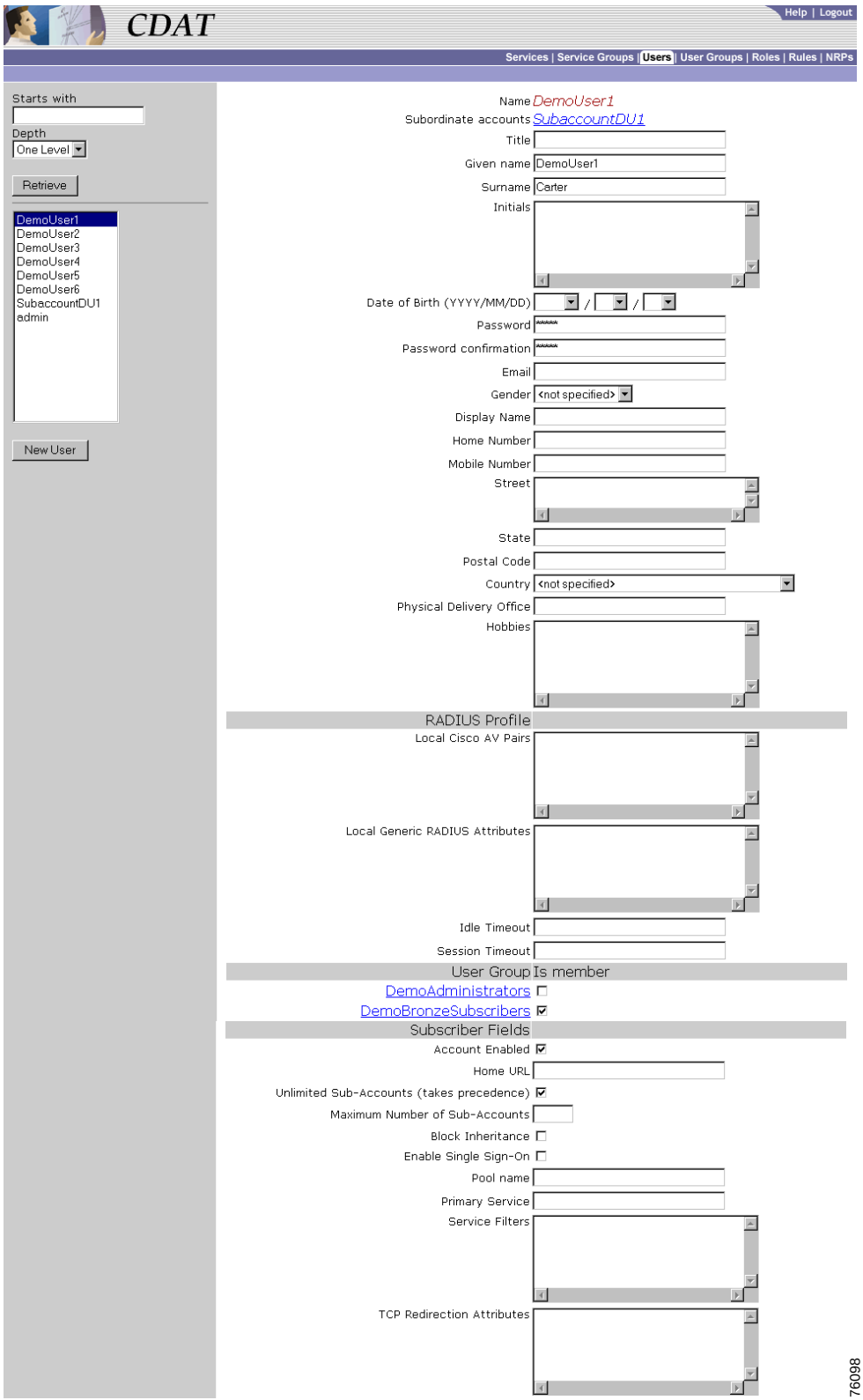
Note When a Pool name and Primary Service are specified in the Users or User Groups window, this local address pool name takes precedence over any pool name defined for the user's primary service (IP Pool Name in the Services window).

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).

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

Local Cisco AV Pairs (Optional and for Subscribers Only)

Cisco attribute-value pairs (Cisco AV pairs) can appear as part of the user profile. The Cisco AV pairs that are supported by the Cisco SESM and CDAT software for user profiles are for upstream access control lists and downstream access control lists.

Note Cisco AV pairs can be specified at the user and the user group level. User and user group AV pairs are cumulative. The set that applies to a user are all AV pairs specified for the user and all AV pairs specified for any user groups of which the user is a member.

Upstream and Downstream Access Control Lists

An upstream access control list 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. The syntax for these AV pairs is as follows:

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

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.

Examples

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

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.

Local Generic RADIUS Attributes (Optional)

One or more RADIUS attributes and values that apply to the user but that do not appear in the fields of the Users window. For example, the Users window does not have a field for a Calling-Station-Id (RADIUS attribute number 31). A Calling-Station-Id for a Mobile Subscriber ISDN (MSISDN) is required in the subscriber profile for 3-key authentication. For information on RADIUS attributes, see RFC 2865.

Allowed values: A RADIUS attribute number and a value in the form *99*:*value*, where *99* is the RADIUS attribute number. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

Example: 31:123456789

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 2-28.

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 the container.

Enable Single Sign-On (Optional and for PPP Subscribers Only)

Indicates whether the single sign-on feature applies to the user. With single sign-on enabled, the Cisco SESM web application queries the SSG for the existence of a PPP connection for the IP address of any request to the Cisco SESM. The Cisco SESM web application does not require additional authentication at the Cisco SESM if a PPP connection already exists. The Enable Single Sign-On box applies only to PPP users. For non-PPP users, choosing Enable Single Sign-On has no effect.

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 2-20.

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 2-20.

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 and Subscriber Policy Engine Installation and Configuration Guide*.

Allowed values: Table 2-3 describes the allowed vendor-specific attributes.

Table 2-3 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 Subscriptions

For each service 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 but is currently not subscribed.
- Inherited—The user is subscribed to the service through inheritance (that is, through a user group of which the user is a member).
- Local—The user is explicitly subscribed to the service (as opposed to being subscribed by inheritance from a user group), or a feature of the service (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 through inheritance but has explicitly chosen to unsubscribe.

If CDAT does not display a service in the Users window, the user does not have the privileges needed to subscribe to the service. For each service 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.

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 if desired.

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 and Subscriber Policy Engine Installation and Configuration Guide*.

User Groups Window

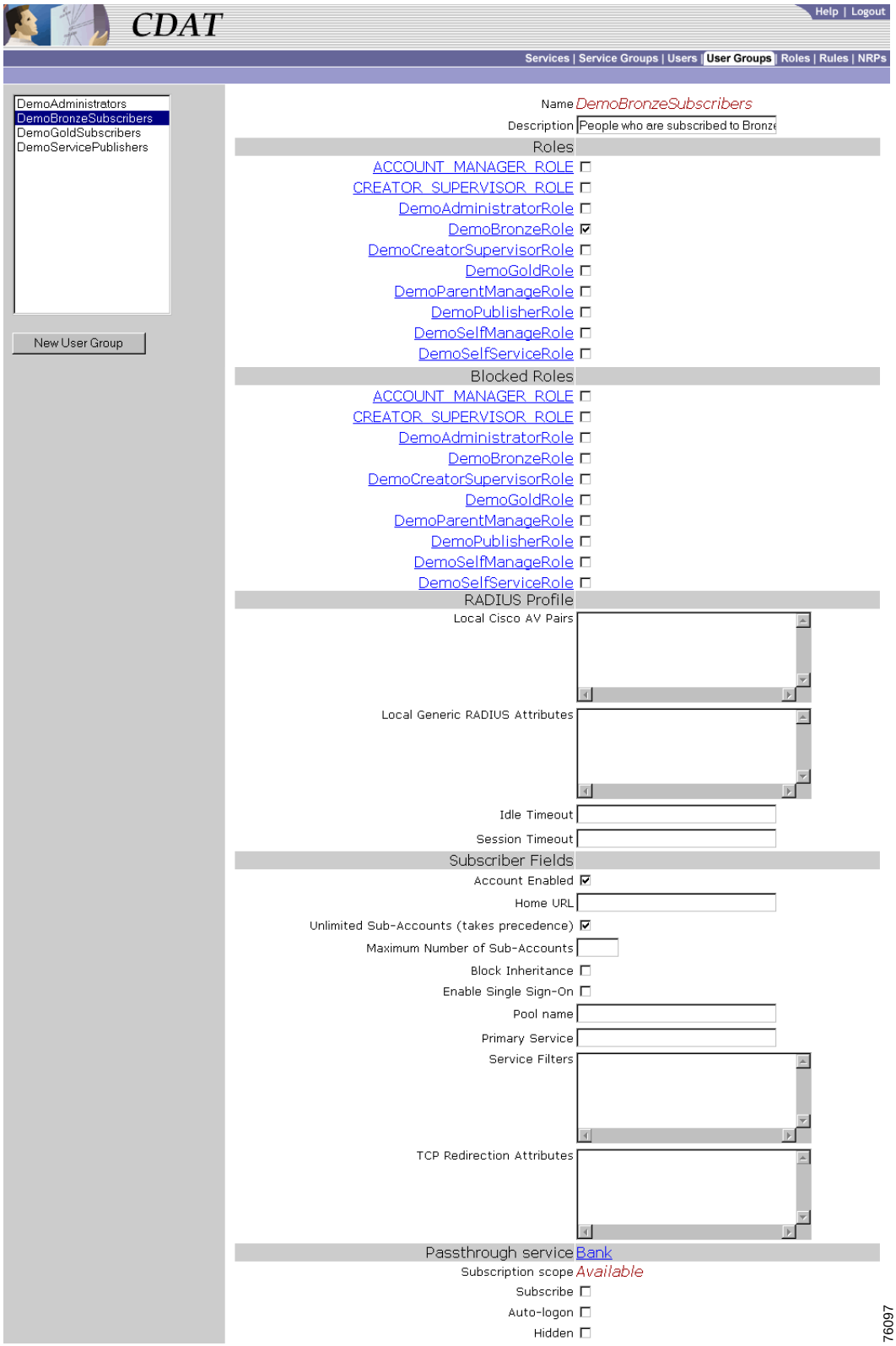
A *user group* is a set of users. With CDAT, individual users—subscribers, publishers, account managers, and administrators—must be associated with one or more user groups in order to get access to resources. After creating a user group, you can make a user a member of the group by choosing the group 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 2-6.

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 service group, you click New Service 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 2-35.

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 Cisco AV Pairs (Optional and for Subscriber Groups Only)

Cisco attribute-value pairs (Cisco AV pairs) can appear as part of the user group profile. The Cisco AV pairs that are supported by the Cisco SESM and CDAT software for user groups are for upstream access control lists and downstream access control lists. For information on these access control lists, see the "Upstream and Downstream Access Control Lists" section on page 2-24.

Note Cisco AV pairs can be specified at the user and the user group level. User and user group AV pairs are cumulative. The set that applies to a user are all AV pairs specified for the user and all AV pairs specified for any user groups of which the user is a member.

Local Generic RADIUS Attributes (Optional)

One or more RADIUS attributes and values that apply to the user group but that do not appear in the fields of the User Groups window. For information on RADIUS attributes, see RFC 2865.

Allowed values: A RADIUS attribute number and a value in the form *99*:*value*, where *99* is the RADIUS attribute number. If more than one RADIUS attribute and value are specified, enter each attribute-value pair on a separate line.

Example: 31:123456789

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 (For PPP Subscriber Groups Only)

Indicates whether the single sign-on feature applies to the users. With single sign-on enabled, the Cisco SESM web application queries the SSG for the existence of a PPP connection for the IP address of any request to the Cisco SESM. The Cisco SESM web application does not require additional authentication at the Cisco SESM if a PPP connection already exists. The Enable Single Sign-On box applies only to PPP users. For non-PPP users, choosing Enable Single Sign-On has no effect.

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 2-20.

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 2-20.

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 and Subscriber Policy Engine Installation and Configuration Guide*.

Allowed values: Table 2-3 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 Subscriptions

For each service to which the user group can subscribe, CDAT displays a subscription scope:

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

If CDAT does not display a service in the User Groups window, the user group does not have the privileges needed to subscribe to the service.

For each available service, you can specify the following information:

Subscribe (For Subscriber Groups Only)

Indicates whether the user group is subscribed to the service.

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

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 and Subscriber Policy Engine Installation and Configuration Guide*.

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 DESS/AUTH 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 DESS 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 DESS 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.

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:

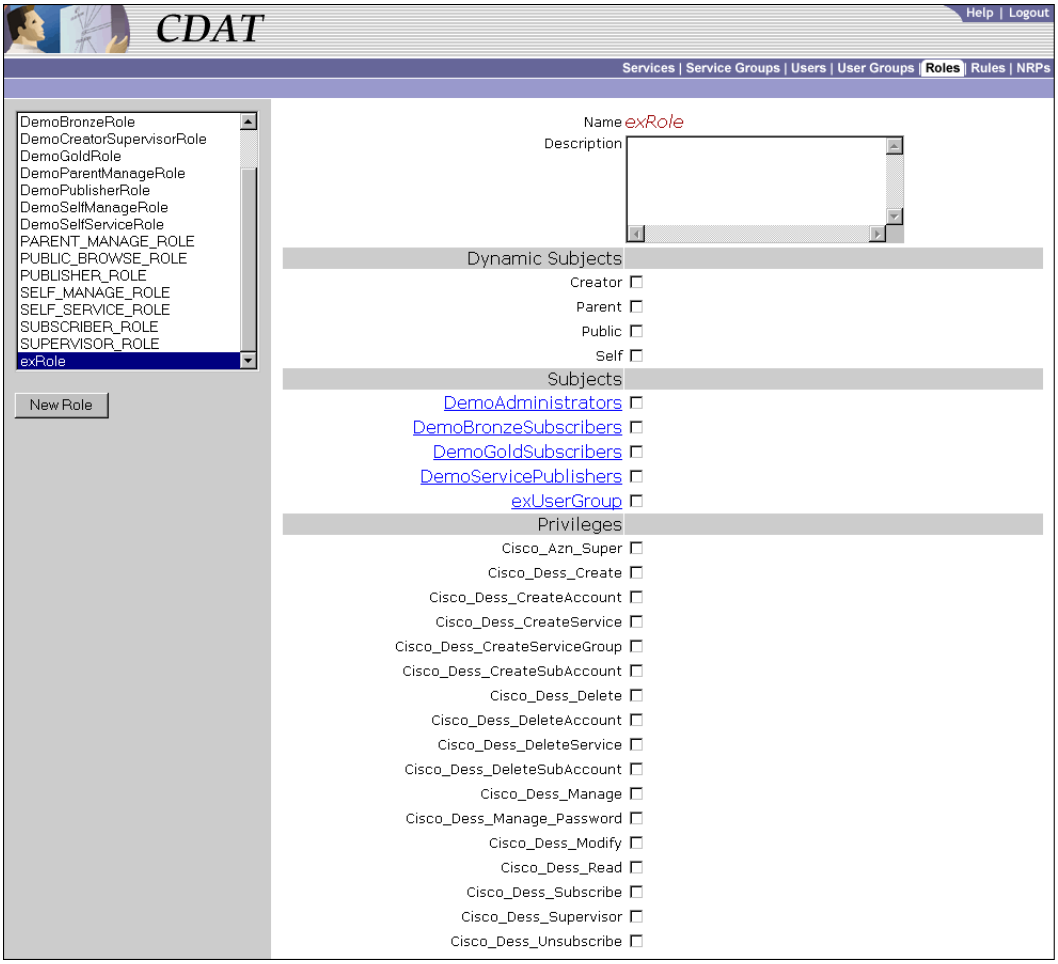
- Cisco_Dess_Subscribe for subscribing to services
- Cisco_Dess_Unsubscribe for unsubscribing to services
- Cisco_Dess_CreateSubAccount for creating subaccounts
- Cisco_Dess_DeleteSubAccount for deleting subaccounts
- Cisco_Dess_Read for reading objects and attributes (for subscriber self-care)
- Cisco_Dess_Manage_Password for reading and changing passwords
- Cisco_Dess_Modify for changing attributes (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 2-4 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 2-4 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.

When you use Table 2-4 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.

Table 2-4 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
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 (for self-care)
Cisco_Dess_Modify	Allows changes to attributes for DESS objects. Implied privileges: None	Subscribers (for self-care)

Table 2-4 Allowed Privileges for a Role (continued)

Privilege	Description	Who Is Granted?
Cisco_Dess_Read	Allows reading of DESS objects and their attributes. CDAT does not display services for a user unless the user has Cisco_Dess_Read privilege. Implied privileges: None	Subscribers (for self-care)
Cisco_Dess_Subscribe	Allows subscription to a service. In order to subscribe to a service, the user must also have Cisco_Dess_Manage privilege on the user account. 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. 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.

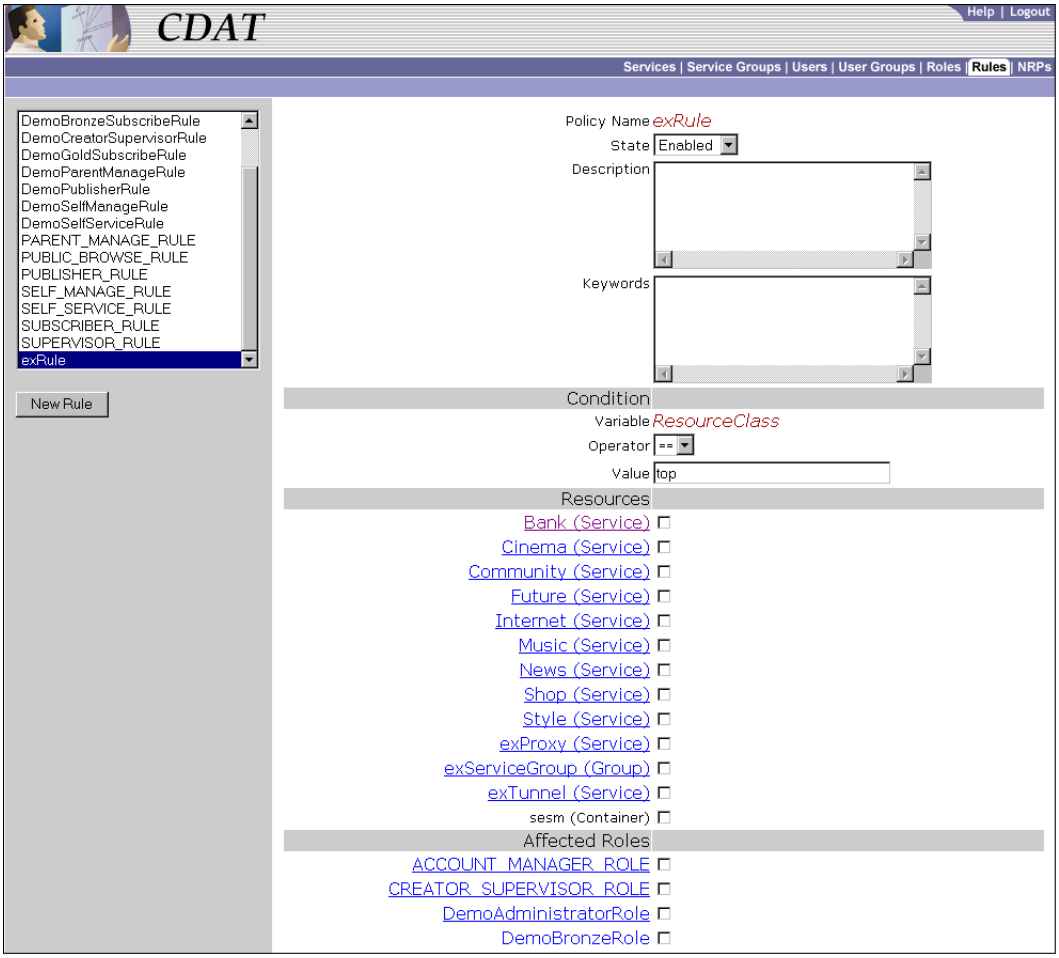
Predefined Rules

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 boxes 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/DESS 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:

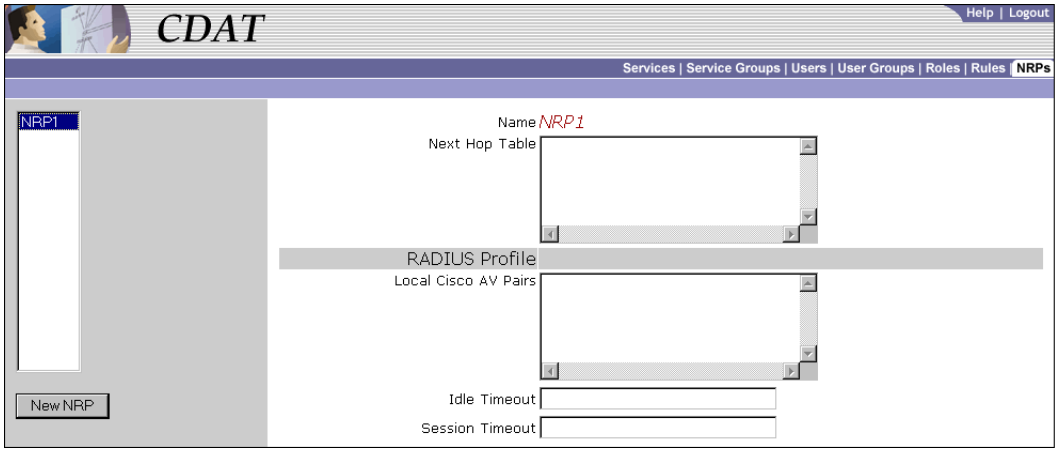
ssg next-hop download *next-hop_table_name next-hop_table_password*

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 *Cisco 6400 Command Reference*.

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
```

Local Cisco AV Pairs (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.