SESM Solutions for Subscriber Self-Care

This chapter describes SESM features that support subscriber self-care solutions. It includes the following topics:

Subscriber Self-Care Solution Description

This section describes the common characteristics of SESM self-care solutions. Topics are:

Subscriber Experiences in Self-Care Solutions

The SESM self-care solutions allow subscribers to make on-demand updates to their personal information at any time and see those changes take effect within minutes of submitting the change, with no involvement from the deployer. Subscribers can submit updates using the SESM portal. The self-care portal pages can be branded, personalized, and customized using any SESM web development features.

The NWSP portal contains pages that illustrate the following types of self-care activities:

- Updating personal account information
- Creating and provisioning subaccounts

- Building personal firewalls
- Subscribing and unsubscribing to services

See the "Supported Data Fields in a Self-Care Solution" section on page 4-4 for ways to extend the self-care examples shown in NWSP.

Security in Self-Care Solutions

The following features provide security in SESM self-care solutions:

- User authentication—A subscriber must successfully log in to the SESM portal before gaining access to any account information. The SSG performs authentication services for the SESM portal, based on subscriber profile information obtained by the RADIUS Data Proxy (RDP).
- User permissions—A subscriber must be assigned permissions that allow self-care updates. The provider administrator assigns permissions using CDAT. Permissions can be assigned to individual subscribers or to groups of users.
- Subaccount permissions—When subaccounts exist, the parent account can assign permissions to the subaccount that are more restrictive than the parent account permissions.
- Secure Socket Layer (SSL) mode—The default SESM portal configuration allows the subscriber to choose whether or not to use the SSL port. Providers can change this configuration so that the SESM web server uses only SSL listeners.

Deployment Requirements for Self-Care Solutions

This section lists the required components for self-care solutions.

Cisco Service Selection Gateway

The Cisco Service Selection Gateway (SSG) is required in the self-care solutions described in this chapter. These solutions require SSG for the following services:

- Requesting authentication—The SESM portal initiates authentication by sending an access request to SSG, which in turn sends a RADIUS access request to the RDP.
- Obtaining the subscriber profile—If the RDP reply is an access-accept, the reply includes the subscriber profile. SSG includes the subscriber profile in its reply to the SESM portal.

SSG configuration details for self-care solutions are the same as those for service selection and connection solutions. The SESM portal and RDP must be running on the SSG default network and configured to communicate with the SSG. For more information about how SESM, SSG, and RDP work together, see the "Request Processing in SESM SPE Mode Deployments" section on page 3-11.

SESM Portal

The SESM self-care solutions require that SESM portals are deployed in LDAP mode.

RADIUS Data Proxy

The RADIUS Data Proxy (RDP) is a required component in self-care solutions.

The RDP cache refresh time is directly related to the length of time subscribers must wait to see their updates take effect. Due to the possibility of just having missed a refresh, the minimum guaranteed time is double the cache refresh time. The installed default for cache refresh is 10 minutes.

LDAP Directory

The profile data that you want subscribers to update must reside in profiles on an LDAP directory. The LDAP protocol provides the features that allow for on-demand updates to profile data.

We recommend deploying a primary and a secondary directory and using the LDAP directory failover features.

Cisco Distributed Administration Tool

The Cisco Distributed Administration Tool (CDAT) is the tool for administrators to use in adding and maintaining subscriber profiles in the LDAP directory.

CDAT must have access to the LDAP directory. Multiple instances of CDAT can be installed on different systems, giving distributed administrative access to the directory.

Portal Customizations for Self-Care Solutions

The SESM portal is the subscriber interface to self-care activity. You can integrate a self-care solution with a service selection and connection solution or deploy it as a standalone solution. The NWSP application illustrates several self-care solutions as different pages in the same application:

- My Account Page
- My Firewall Page
- My Services Page
- Subaccounts Page

Service provider developers can use the SESM web developer kit to customize the portal page on which subscribers can enter or update the account information. Customizations related to self-care features might include:

- Adding or deleting self-care fields on the pages. See the "Supported Data Fields in a Self-Care Solution" section on page 4-4.
- Implementing the provider's business rules when validating the subscriber-submitted account information.

Supported Data Fields in a Self-Care Solution

SESM 3.1(5) supports the following categories of data in a subscriber profile. Developers can add any field from these categories to an SESM portal page and optionally provide access to them for on-demand updates by subscribers:

- Generic RADIUS attributes. For a list of supported attributes, see the *Cisco Subscriber Edge Services Manager Installation and Configuration Guide*. The online link to the list of generic RADIUS attribute fields that are predefined in the SESM core model is:

  http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_315/instconf/cradius.htm#xtocid5

- SPE attributes. SPE supports many of the fields in the X.500 standard user schema developed for use with LDAP. Some of the fields supported include date of birth, various address and telephone number fields, e-mail, gender, and hobbies. For a list of SPE-supported attributes, see the *Cisco Distributed Administration Tool Guide.* The online link to the SPE DESS/AUTH schema extensions is:

  http://www.cisco.com/univercd/cc/td/doc/solution/sesm/sesm_313/toolguid/appb_sch.htm#xtocid0

Subscriber Profile Requirements for Self-Care Solutions

The following requirements apply to subscriber profiles in SESM self-care solutions:

- The profile data that you want the subscriber to maintain must reside on an LDAP directory.
- The service provider must create the initial profile for each subscriber.

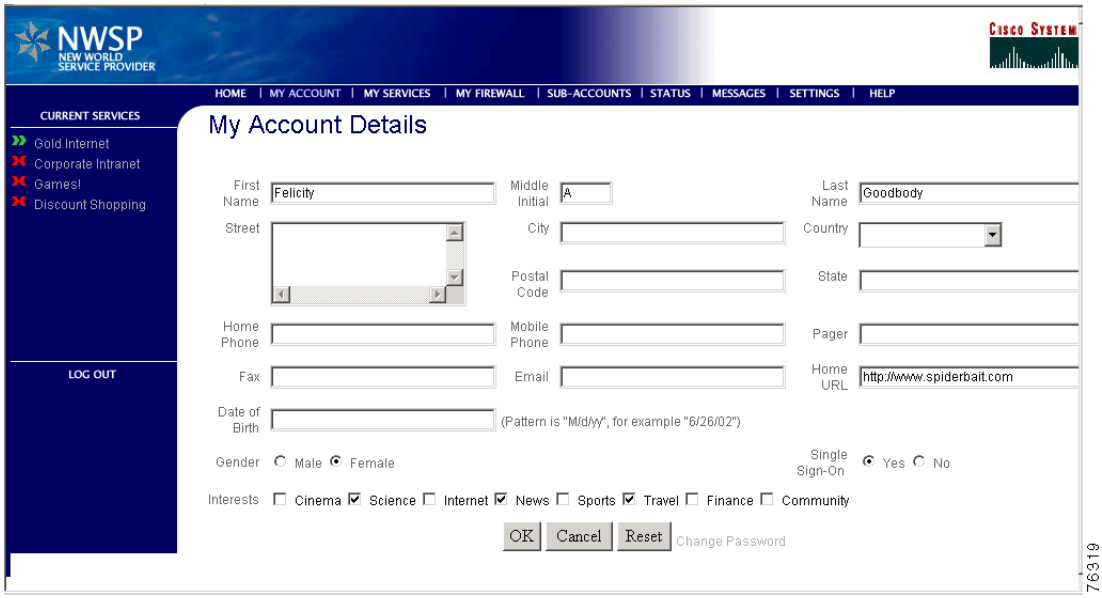
Service provider administrators use the Cisco Distributed Administration Tool (CDAT) to add subscriber profiles to the LDAP directory. Administrators use CDAT to:

- Add a new subscriber.
- Enter subscriber profile information. Required information includes an initial SESM user name and password for logging into the SESM portal. Other optional information can be entered by the administrator in CDAT, or left to the subscriber to fill in later using the self-care features in the SESM portal.
- Assign permissions that allow the subscriber to perform self-care activities. Permissions can be inherited from roles that are assigned to groups of users. User groups, roles, and permissions are Security Policy Engine (SPE) concepts and are explained in the *Cisco Distributed Administration Tool Guide*.

Personal Account Maintenance

Figure 4-1 shows the My Account Page in NWSP. See the "Supported Data Fields in a Self-Care Solution" section on page 4-4 for other supported fields that you might want to add to a personal account maintenance page.

Figure 4-1 NWSP My Account Page



The initial display of the My Account Details page reflects the contents of the subscriber profile. After subscribers enter or update their personal details, they can go back to the My Account Details page in about 20 minutes to see the changes. In Demo mode, the changes are *not* recorded in the profile.

Personal Firewalls

The SESM personal firewall feature provides a way for subscribers to restrict or permit traffic to and from their connection by making choices on a web portal page. The portal page presents a list of applications that are available for firewall protection. The SESM deployer configures the list of applications using the Firewall MBean.

Deployers can also configure firewall controls for subscribers which cannot be changed by the subscriber. Administrators use CDAT to configure these controls.

The underlying technology for the SESM personal firewall feature is extended access control lists (ACLs) added as attributes in subscriber profiles in an LDAP directory.

The ACLs are stored in the subscriber profiles as standard RADIUS attribute with number 26 (vendor specific attribute), subattribute number 1 (Cisco AV-pair). A subscriber profile might have many ACL entries, which together determine which traffic is permitted and denied on the connection.

The ACLs are added to the profile in two ways:

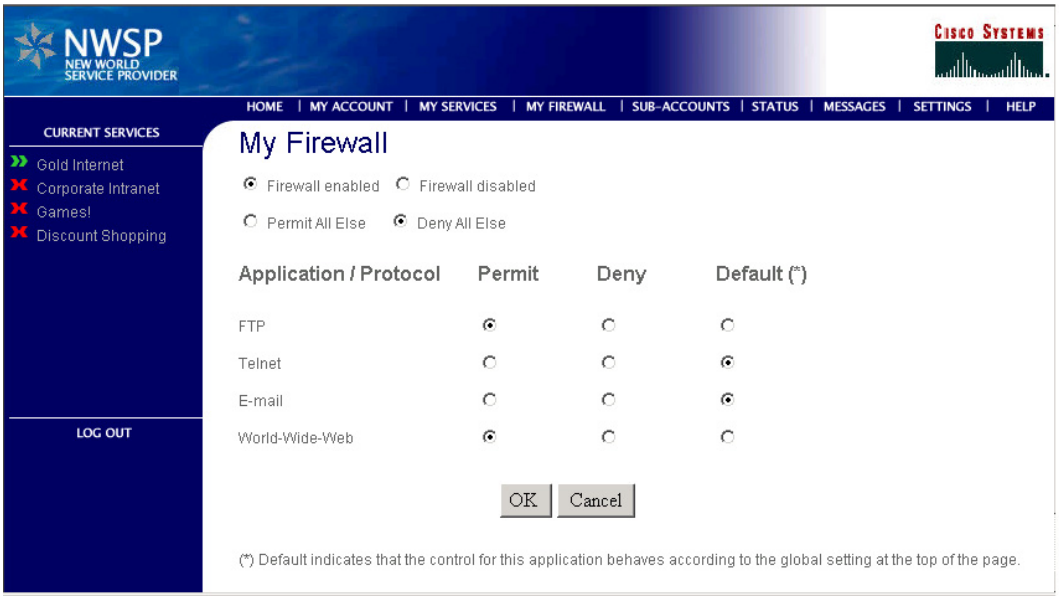
- When a subscriber configures firewall settings from the SESM portal, the portal creates the appropriate ACLs to support the subscriber's choices. The created ACLs are grouped by application, with one ACL per chosen protocol and control direction (upstream or downstream). The ACLs allow traffic to and from *any* source and destination IP address, for a given protocol and port number. (The subscriber does not have the means to enter specific IP addresses when configuring a personal firewall.)
- In the case of deployer imposed firewall settings, the administrators manually create the correctly formatted ACLs and enter them in CDAT. The ACLs entered in CDAT can use the full range of ACL options as described in the Cisco IOS documentation.

SESM and SSG implement the firewall as follows:

- The subscriber logs into the SESM portal.
- The logon request is accepted by SESM and passes through the SSG to RDP.
- During authentication processing, RDP obtains the subscriber profile from the directory and adds all of the profile information, including the ACLs, in the access-accept reply to the SSG.
- The SSG applies the ACLs against traffic to and from the subscriber's connection.

Figure 4-2 shows the My Firewall page in NWSP.

Figure 4-2 NWSP My Firewall Page



By clicking the Permit, Deny, and Default radio buttons on this page, subscribers can control the upstream and downstream traffic to their IP address.

For each application, the initial displayed state of the Permit, Deny, and Default radio buttons depends upon the ACLs that exist in the subscriber profile. The SESM portal analyzes the ACLs to determine the appropriate settings to display.

The Application/Protocol column is configurable by the deployer:

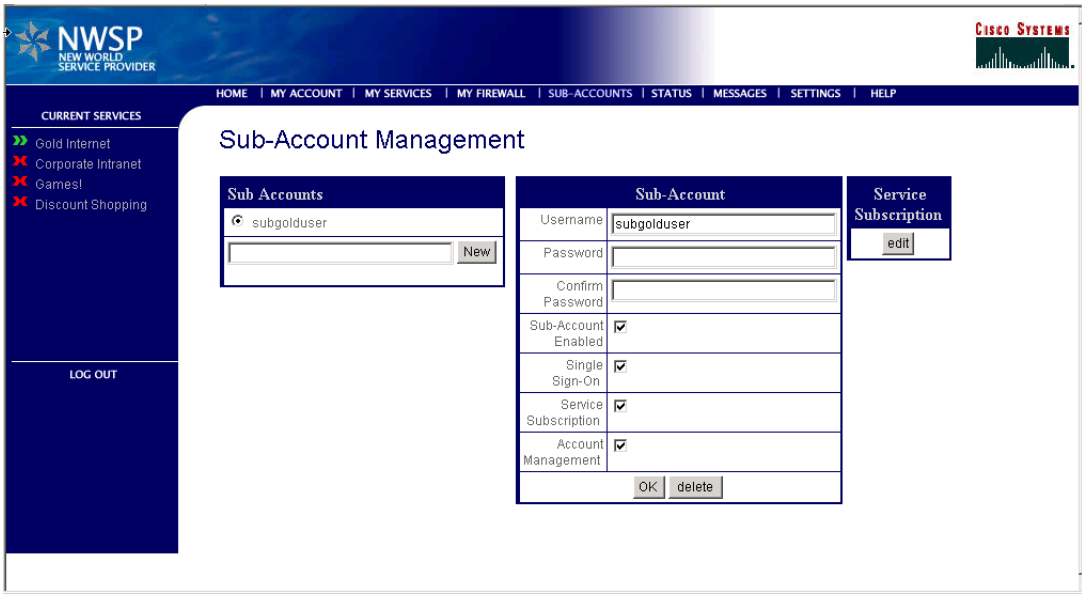
- The contents of the Applications/Protocols list is controlled by configuration attributes.
- The text strings in the Applications/Protocols list are resource bundles. The strings can be anything the deployer wants, and can be localized to match subscriber language preferences.

Subaccount Creation

Subscriber subaccount creation and management allows a subscriber with a main account to create subaccounts, with different services and access information in each subaccount. For example, a family might have subaccounts for each family member, with a different set of authorized services within each subaccount. The main account can create and delete subaccounts and subscribe to services for the subaccounts, and control whether the subaccounts can subscribe to services themselves.

Figure 4-3 shows the NWSP Subaccounts page.

Figure 4-3 NWSP Subaccounts Page



From this page, a subscriber can:

- Create new subaccounts
- Change passwords for subaccounts
- Change the permissions for subaccounts. For example, give or deny permission for the subaccount to:
  - Self-subscribe to services
  - Perform account self-maintenance
- Change the service subscription information for a subaccount, including:
  - Block services from this subaccount
  - Subscribe and unsubscribe services

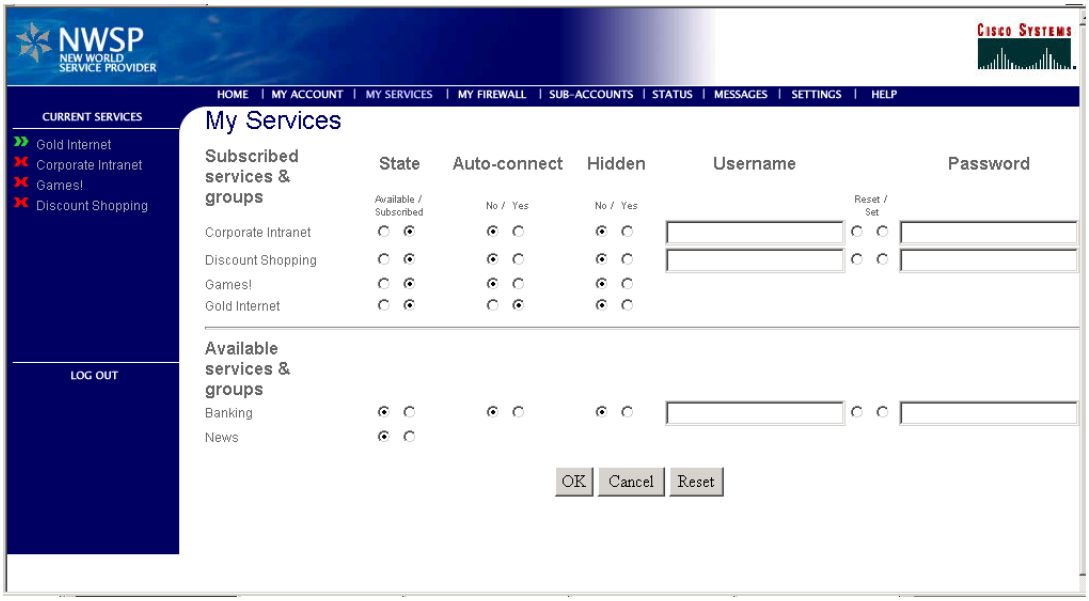
- Mark services as automatically connected and hidden.
- Provide user names and passwords for service authentication

Service Self-Subscription

Service self-subscription allows subscribers to sign up for new services and have immediate access to those services. This feature relieves the service provider from time-consuming service enrollment tasks. It also benefits the subscriber because there is no delay in receiving access to a new service. Subscribers can also unsubscribe from a service.

Figure 4-4 shows the My Services page from the NWSP application.

Figure 4-4 NWSP My Services Page



The page shows:

- Services available for subscription, as listed in the subscriber profile
- Whether or not this subscriber is subscribed to the service
- Whether or not the service is marked for automatic connection upon SESM logon
- Whether or not automatically connected services are hidden (not shown) on the service list
- User name and password for the service, if the service requires a logon

SESM Self-Care Demo

To demonstrate SESM self-care features using Demo mode, follow this procedure:

Step 1 Install NWSP (LDAP evaluation or licensed version) in Demo mode. See the "Quick Start for Installing and Running Portals in Demo Mode" section on page A-2 for instructions.

Step 2 Start NWSP. The start script path name is:

```
jetty
    bin
        startNWSP
```

See the "Starting a Demo" section on page A-5 for more information.

Step 3 Open a web browser and go to the NWSP page.

If the web browser is on the same system where NWSP is running, and you accepted the default port during installation, you can use the following URL:

```
http://localhost:8080
```

Otherwise, the URL is:

```
http://NWSPhostName:NWSPportNumber
```

Step 4 On the NWSP login page, log in using the following information:

User: golduser

Password: cisco

Note To understand the relationship between values in a subscriber profile and the initial contents of the NWSP pages, examine the golduser profile in the nwsp/config/demo.txt file.

Step 5 Close the new browser window that opens as a result of the home URL specified in the profile.

Step 6 On the NWSP main page, click the **MY SERVICES** tab.

The My Services page initially displays information as recorded in the profiles in the demo.txt file.

You can change the service information on the My Services page to demonstrate self-management features. In Demo mode, the changes you make are *not* propagated into the demo.txt file.

Step 7 To demonstrate self-subscription to a new service, click the **Subscribed** radio button for one of the services in the Available list. The available services and service groups are obtained from the subscriber profile.

Note To demonstrate subscription to a service group, subscribe to News.

After a confirmation prompt, the My Services page reappears, showing the new service in the Subscribed list. In Demo mode, the new service is *not* changed to subscribed in the subscriber profile.

Step 8 To demonstrate that the new service in immediately available for connection, click the newly subscribed service in the Current Services list.

The status of the new service changes to active.

Step 9 To demonstrate setting and changing service authentication values:

1. Check the service status to make sure the service is stopped. If not, click on it in the Current Services list to stop it.
2. Click the **Set** button for one of the services, and enter a user name and password of your choice. (The golduser profile in demo.txt does not configure any service authentication values for any of the services.)
3. Click **OK**.
4. Answer **OK** to the confirmation prompt.
5. When the My Services page reappears, click the service in the Current Services list to restart it.
6. To see the Authentication Failed message, enter an invalid user name or password on the authentication page.
7. To complete service authentication, enter the user name and password you just set on the My Services page.

Step 10 To demonstrate unsubscribing to a service, click the **Available** radio button next to the service.

After a confirmation prompt, the My Services page reappears, showing the service in the Available list. If the service was running at the time you unsubscribed, the service is now stopped.

Step 11 Although you can click on the **Auto-connect** and **Hidden** radio buttons in Demo mode, you cannot demonstrate the effects of these buttons because changes are not recorded in the subscriber profile when SESM is running in Demo mode.

Step 12 Click the **MY ACCOUNT** tab to display information recorded in the subscriber profile.

The page initially displays information as recorded in the profile in the demo.txt file. You can change the subscriber information on the My Account page to demonstrate self-management features. In Demo mode, the changes you make are *not* propagated into the demo.txt file.

Step 13 To demonstrate subaccount maintenance, click the **SUB-ACCOUNTS** tab.

The installed demo.txt file contains a profile for one subaccount user (subgolduser) under the main golduser account.

Step 14 To create a new subaccount under golduser:

1. Enter a new user ID in the New field.
2. Click **New**. The new subaccount appears in the subaccount list.
3. Enter a password in the Password field.
4. Click **OK**.
5. Click Service Subscription **Edit**.
6. Select services for the subaccount and decide if they should be automatically connected and hidden.
7. Click **OK**.

In Demo mode, the subaccount profile is not added to the demo.txt file. Therefore, you cannot log in using the new subaccount.

Demonstrating Personal Firewalls

You can use the My Firewall page in Demo mode to simulate firewall changes. To see the effects of the changes, you must use a fully configured system running in LDAP mode. In a fully configured system, the effects of changes made on the My Firewall page are visible in these ways:

- View the subscriber profile in CDAT or on the LDAP directory. The firewall ACLs are visible in the Local Generic Attribute field in CDAT.
- Wait about 20 minutes (the time it takes the RDP to refresh its cache) and then view the My Firewall page again. The initial display reflects the newly created ACLs.
- Try accessing an application or protocol that you have blocked with a Deny firewall. For example, Deny access to FTP and then try to perform an FTP transfer.