Chapter 26

Configuring Subscriber–Related Properties on the SAE with the C-Web Interface

This chapter describes how to use the C-Web interface to configure subscriber-related properties on the SAE.

- To use the SRC CLI, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 4, Configuring Subscriber–Related Properties on the SAE with the SRC CLI*.
- To use the C-Web interface to configure the SAE on a Solaris platform, see *SRC-PE Subscribers and Subscriptions Guide, Chapter 5, Configuring Subscriber–Related Properties on the SAE on a Solaris Platform*.

Topics in this chapter include:

Configuring the Length of Time That MAC Addresses Remain in SAE Cache with the C-Web Interface

When a DHCP subscriber transitions from an authenticated IP address to an unauthenticated IP address or vice-versa, the SAE:

1. Logs out the subscriber associated with the original IP address.

2. Caches the subscriber profile in the in-memory cache, indexed by the DHCP subscriber's MAC address.

3. Waits until the DHCP subscriber with the cached MAC address obtains its new IP address, and then logs in the subscriber and associates it with the new IP address.

The period during which the subscriber profile remains in the in-memory cache can last until the DHCP lease time for the original address. If something happens during this period—for example, the subscriber turns off the client computer—the subscriber profile remains in the SAE's in-memory cache forever. When a new IP address is assigned to the same DHCP client, problems can occur. To avoid such problems, entries in the in-memory cache are removed after a configurable amount of time.

Configure the amount of time that entries remain in cache to be greater than the time required for a DHCP subscriber to transition from an unauthenticated IP address to an authenticated IP address or vice versa. The time required for a DHCP subscriber to transition from one IP address to another depends on the lease times configured on the JUNOSe router and the instructions given to the subscriber on the Web portal, such as reboot your PC now.

To configure the amount of time that subscriber profiles remain in the SAE's in-memory cache:

1. Click **Configure**, expand **Shared > SAE**, and then click **Driver**.

   The Driver pane appears.

2. Click **Create**, specify the amount of time that subscriber profiles remain in the SAE's cache as described in the Help text in the Main pane, and then click **Apply**.

Identifying a Profile for Unauthenticated Subscribers with the C-Web Interface

The SAE uses an unauthenticated subscriber profile as a transitional profile for subscribers who are not logged in to the SAE. For example, if a subscriber logs out of the SAE using the API method Subscriber.logout(), an unauthenticated subscriber session is created. The unauthenticated subscriber profile must exist and can be subscribed to services available for unauthenticated subscribers. The portal implementation determines whether unauthenticated (anonymous) subscribers can access the portal.

To specify an unauthenticated subscriber profile:

1. Click **Configure**, expand **Shared > SAE**, and then click **Driver**.

   The Driver pane appears.

2. Click **Create**, specify a subscriber profile for unauthenticated access to the portal as described in the Help text, and then click **Apply**.

Configuring Interim Accounting for Services and Subscribers with the C-Web Interface

You can enable and disable interim accounting and set intervals between interim accounting messages for services and subscribers. These settings apply to all subscriber sessions and service sessions unless you override these settings for specific services by configuring an accounting interim interval in the value-added service configuration.

To set up interim accounting:

1. Click **Configure**, expand **Shared > SAE**, and then click **Interim Accounting**.

   The Interim Accounting pane appears.

2. Click **Create**.
3. (Optional) Enable service interim accounting as described in the Help text.
4. Specify the interval between service interim accounting messages as described in the Help text.
5. (Optional) Enable interim accounting for subscribers as described in the Help text.
6. Specify the interval between subscriber interim accounting messages as described in the Help text.
7. Click **Apply**.

Avoiding Overcharges for Sessions That Time Out with the C-Web Interface

When an idle timeout terminates a session, you can set up the SAE to reduce the session time reported in the accounting stop message by the idle time. This way the session time is accurately reported; the report avoids overcharges for the session.

To adjust the session time:

1. Click **Configure**, expand **Shared > SAE**, and then click **Idle Timeout**.

   The Idle Timeout pane appears.

2. Enable when an idle timeout terminates a session as described in the Help text.

   The session time reported in the accounting stop message is reduced by the idle time.

3. Click **Apply**.

Allowing Multiple Logins from the Same IP Address with the C-Web Interface

You can specify whether the SAE allows a login from the same IP address without requiring that the previous session log out first.

- If you enable this setting, the SAE logs in the new subscriber session and automatically logs out the previous session.
- If you disable this setting, the SAE denies login requests if a subscriber session for an IP address is active.

To specify whether the SAE allows a login from the same IP address without requiring that the previous session log out first:

1. Click **Configure**, expand **Shared > SAE**, and then click **Subscriber Sessions**.

   The Subscriber Sessions pane appears.

2. Enable or disable whether the SAE allows a login from the same IP address without requiring that the previous session log out first, as described in the Help text.

3. Click **Apply**.

Authenticating Registered Username/Password Pairs with the C-Web Interface

You can specify whether the application programming interface (API) method registerLoginCredentials authenticates the registered username/password or creates the registration without authentication. Enable this setting if your authentication server does not allow authentication while a session for the authenticated username is active.

To specify whether or not registered username/password pairs are authenticated:

1. Click **Configure**, expand **Shared > SAE**, and then click **Login Registration.**

   The Login Registration pane appears.

2. Enable or disable whether registered username/password pairs are authenticated, as described in the Help text.
3. Click **Apply**.

Configuring Timers for Session Reactivation with the C-Web Interface

If a service session fails unexpectedly, the SAE tries to start the session again in the background. You can change how many times the SAE tries to activate the session and the interval between these attempts. In most instances, you do not need to change the default values.

To configure session reactivation behavior:

1. Click **Configure**, expand **Shared > SAE**, and then click **Service Activation**.

   The Service Activation pane appears.

2. Configure the number of times the SAE tries to activate a service session if activation fails or to deactivate a service session if deactivation fails, as described in the Help text.
3. Configure the time between attempts to activate a service session if activation fails or to deactivate a service session if deactivation fails, as described in the Help text.
4. Click **Apply**.