Chapter 4

Configuring Subscriber–Related Properties on the SAE with the SRC CLI

This chapter describes how to use the SRC CLI to configure subscriber-related properties on the SAE.

- To use the SRC CLI to configure the SAE on a Solaris platform. See *Chapter 5, Configuring Subscriber–Related Properties on the SAE on a Solaris Platform*.
- To use the C-Web interface, see *SRC-PE C-Web Interface Configuration Guide, Chapter 26, Configuring Subscriber–Related Properties on the SAE with the C-Web Interface*.

Topics in this chapter include:

Configuring the Length of Time MAC Addresses Remain in SAE Cache

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.

Use the following configuration statement to configure the length of time that a subscriber profile remains in the SAE's in-memory cache:

```
shared sae configuration driver {
    mac-cache-expiration mac-cache-expiration;
}
```

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

1. From configuration mode, access the SAE driver configuration statement.

   ```
   user@host# edit shared sae configuration driver
   ```

2. Specify the amount of time that subscriber profiles remain in the SAE's cache.

   ```
   [edit shared sae configuration driver]
   user@host# set mac-cache-expiration mac-cache-expiration
   ```

3. (Optional) Verify your configuration.

   ```
   [edit shared sae configuration driver]
   user@host# show mac-cache-expiration
   mac-cache-expiration 1800;
   ```

Identifying a Profile for Unauthenticated Subscribers

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.

Use the following configuration statement to specify an unauthenticated subscriber profile.

```
shared sae configuration driver {
    unauthenticated-subscriber-dn unauthenticated-subscriber-dn
}
```

To specify an unauthenticated subscriber profile:

1. From configuration mode, access the SAE driver configuration statement.

   ```
   user@host# edit shared sae configuration driver
   ```

2. Specify a subscriber profile for unauthenticated access to the portal.

   ```
   [edit shared sae configuration driver]
   user@host# set unauthenticated-subscriber-dn unauthenticated-subscriber-dn
   ```

3. (Optional) Verify your configuration.

   ```
   [edit shared sae configuration driver]
   user@host# show unauthenticated-subscriber-dn
   unauthenticated-subscriber-dn
   uniqueID=unauthentication,ou=local,RetailerName=default,o=Users,<base>;
   ```

Configuring Interim Accounting for Services and Subscribers

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.

Use the following configuration statements to configure interim accounting.

```
shared sae configuration interim-accounting {
    service-interim-accounting;
    service-interim-interval service-interim-interval;
    subscriber-interim-accounting;
    subscriber-interim-interval subscriber-interim-interval;
}
```

To set up interim accounting:

1. From configuration mode, access the configuration statement for interim accounting.

   user@host# **edit shared sae configuration interim-accounting**

2. (Optional) Enable service interim accounting.

   [edit shared sae configuration interim-accounting]
   user@host# **set service-interim-accounting**

3. Specify the interval between service interim accounting messages.

   [edit shared sae configuration interim-accounting]
   user@host# **set service-interim-interval** *service-interim-interval*

4. (Optional) Enable interim accounting for subscribers.

   [edit shared sae configuration interim-accounting]
   user@host# **set subscriber-interim-accounting**

5. Specify the interval between subscriber interim accounting messages.

   [edit shared sae configuration interim-accounting]
   user@host# **set subscriber-interim-interval** *subscriber-interim-interval*

6. Verify your configuration.

   ```
   [edit shared sae configuration interim-accounting]
   user@host# show
   service-interim-accounting;
   service-interim-interval 900;
   subscriber-interim-accounting;
   subscriber-interim-interval 900;
   ```

Avoiding Overcharges for Sessions That Time Out

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 to avoid overcharges for the session.

Use the following configuration statement to configure the length of time that a subscriber profile remains in the SAE's in-memory cache:

```
shared sae configuration idle-timeout {
    adjust-session-time;
}
```

To adjust the session time:

1. From configuration mode, access the SAE idle timeout configuration statement.

   ```
   user@host# edit shared sae configuration idle-timeout
   ```

2. Enable when an idle timeout terminates a session, the session time reported in the accounting stop message is reduced by the idle time.

   ```
   [edit shared sae configuration idle-timeout]
   user@host# set adjust-session-time
   ```

3. (Optional) Verify your configuration.

   ```
   [edit shared sae configuration idle-timeout]
   user@host# show
   adjust-session-time;
   ```

Allowing Multiple Logins from the Same IP Address

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

Use the following configuration statement to specify whether or not the SAE allows multiple logins from the same IP address:

```
shared sae configuration subscriber-sessions {
    allow-same-ip-login;
}
```

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

1. From configuration mode, access the subscriber sessions statement.

   ```
   user@host# edit shared sae configuration subscriber-sessions
   ```

2. Enable or disable whether the SAE allows a login from the same IP address without requiring that the previous session logs out first.

   ```
   [edit shared sae configuration subscriber-sessions]
   user@host# set allow-same-ip-login
   ```

3. (Optional) Verify your configuration.

   ```
   [edit shared sae configuration subscriber-sessions]
   user@host# show
   adjust-session-time;
   ```

Authenticating Registered Username/Password Pairs

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

Use the following configuration statement to specify whether or not registered username/password pairs are authenticated:

```
shared sae configuration login-registration {
    registration-authentication;
}
```

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

1. From configuration mode, access the subscriber sessions statement.

   ```
   user@host# edit shared sae configuration login-registration
   ```

2. Enable or disable whether registered username/password pairs are authenticated.

   ```
   [edit shared sae configuration login-registration]
   user@host# set registration-authentication
   ```

3. (Optional) Verify your configuration.

   ```
   [edit shared sae configuration login-registration]
   user@host# show
   registration-authentication;
   ```

Configuring Timers for Session Reactivation

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.

Use the following configuration statements to configure background session reactivation behavior

```
shared sae configuration service-activation {
    retry-time retry-time;
    retry-limit retry-limit;
}
```

To configure session reactivation behavior:

1. From configuration mode, access the service activation statements.

   user@host# **edit shared sae configuration service-activation**

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.

   [edit shared sae configuration service-activation]
   user@host# **set retry-limit** *retry-limit*

3. Configure the time between attempts to activate a service session if activation fails or to deactivate a service session if deactivation fails.

   [edit shared sae configuration service-activation]
   user@host# **set retry-time** *retry-time*

4. (Optional) Verify your configuration.

   ```
   [edit shared sae configuration service-activation]
   user@host# show
   retry-time 60;
   retry-limit -1;
   ```