Advanced Services Configuration and Operation Using the NetOp EMS Software

USER GUIDE

Copyright

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

SmartEdge	is a registered trademark of Telefonaktiebolaget LM Ericsson.
NetOp	is a trademark of Telefonaktiebolaget LM Ericsson.

Contents

1 Configuring Log Server Settings for the Security Service

You must configure a SmartEdge® router to communicate with the Security Services log server of the NetOp™ Element Management System (EMS) so that it can use an Advanced Services Engine (ASE) card to provide Security Services. An ASE card does not have to be installed on a SmartEdge router before the router is configured to support Security Services. If you do not configure the router to communicate with the log server, the download of the Advanced Services Processor (ASP) configuration to the ASE card cannot take place and no logging records of IP Security (IPsec) Virtual Private Network (VPN) events are received by the NetOp EMS software.

Before you configure the Security service on a SmartEdge router, you must already be using the NetOp EMS software to manage the SmartEdge router and have the IP address of the NetOp EMS host.

To configure log server settings on a SmartEdge router, do the following:

1. Find the node and open its provision view.

2. In the **Security Settings** area of the **General** tab, complete the steps in Table 1.

Table 1   Steps to Configure Log Server Settings for Security Services

Step	Task	Additional Instructions
❶	In the **Log Server IP** field, type the IP address of the Security Services log server.	Enter the IP address of the Security Services log server, which is the same IP address as that for the host of the NetOp EMS server.
❷	In the **Port** field, identify the port on the Security Services log server to which Security Services log messages are sent.	Accept the default value, or enter a new value for the port. The default value was defined when the Security Services log server was installed. [1]
❸	In the **Log Source IP** field, enter the IP address of the Network Address Translation (NAT) server.	(Optional; required only if NAT is used between the SmartEdge router and the NetOp EMS server.) Enter the IP address of the NAT server.

(1) If a firewall is configured between the NetOp EMS server and the SmartEdge router, this port and the next port in sequence must be opened.

3.   Click **Apply**.

2 Adding and Enabling an ASE Card

Add and enable an ASE card by provisioning a slot in the SmartEdge router and installing the card in that slot. These steps can be completed in any order.

Use the procedure in this section to use the NetOp EMS client to provision the SmartEdge router with an ASE card. You can also use the `card ase slot` CLI command in the SmartEdge OS. The card does not have to be installed to be added to the configuration of the SmartEdge router. Repeat this procedure for each card you install.
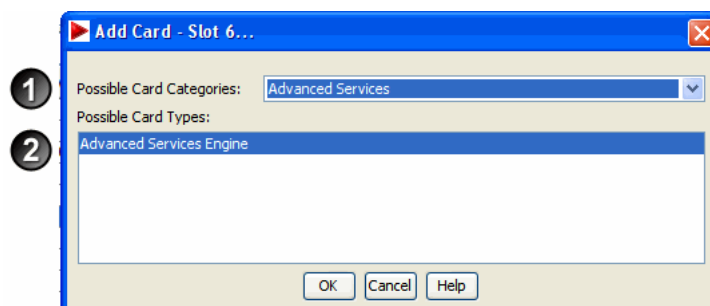

Caution!

Risk of loss of performance. If an ASE card that is not physically in the SmartEdge router is provisioned and its ASPs are members of ASP pools, there is a performance impact as Security Services tries to copy the IPsec VPN tunnel configuration to an ASP that is not physically present in the chassis. To avoid this risk, only provision ASE cards that are physically in the SmartEdge router.

After the card has been added to the configuration of the SmartEdge router, the ASE card is detected when it is physically installed and provides Security Service as soon as the ASP configuration is processed. Thereafter, the Security Services configurations of the Advanced Services Processors (ASPs) on the ASE card are automatically synchronized with the NetOp EMS database.

To add an ASE card to a SmartEdge router, do the following:

1. Find the node and open its provision view.

2. Expand the node and open the Card object to display the slots in the node. Find a slot with an empty Provision field and click **Add**.

3. Complete the steps in Table 2.

Table 2   Steps to Add an ASE Card to a SmartEdge Router

Step	Task	Additional Instructions
①	Identify the type of card in the **Possible Card Categories** field.	From the drop-down list, select **Advanced Services**.
②	Identify the card to add in the **Possible Card Types** field.	**Advanced Services Engine** is the only option and is already selected.

4. Click **OK**.

If the card is installed in the SmartEdge router, "ASE" appears in both the Physical and Provision columns. If it is not installed, "ASE" appears in the Provision column only, a fault is raised by the SmartEdge router for that slot, and a card alarm indicator appears on the card in the object navigator.

In the card fault view of the node, a "Circuit Pack Missing" fault appears. You can safely ignore this fault; it is automatically cleared when the ASE card is inserted in the slot.

3 Managing the Inventory of ASE Cards

The following sections describe what appears in the object navigator of the NetOp client when you add an ASE card to a SmartEdge router configuration file, physically install an ASE card in a SmartEdge chassis, delete an ASE card from a SmartEdge router configuration file, and physically remove an ASE card in a SmartEdge chassis.

3.1 Adding an ASE Card to the SmartEdge Router Configuration

You add an ASE card to the configuration of a SmartEdge router by using the Card provision view of the NetOp client; see Section 2 on page 3. For more information on the Card Provisioning view, see the "Manage Card Provisioning" section in the "Cards" section in Reference [1].

You see the following responses in the NetOp client when you add a card to the SmartEdge router configuration before the card is physically installed:

- In an empty unconfigured slot:

    - In the object navigator of the Card Provision view, a card icon labeled "ASE" appears in the Provision column.

    - In the Card Fault view, no new faults appear.

- In a slot preprovisioned for another type of card:

    - In the object navigator of the Card Provision view, in the slot that the ASE card is installed, card icons appear in the Physical and Provision columns. The icon in the Physical column is labeled "ASE," and the icon in the Provision column is labeled with the preprovisioned card type. An alarm indicator appears on the card icon in the Provision column.

    - In the Card Fault view, the "Circuit Pack Mismatch" fault appears.

For more information on the Card Fault view, see the "View Card-Level Faults" section in the "Alarms and Traps" section of Reference [1].

3.2 Installing an ASE Card in the SmartEdge Router

You install an ASE card in a SmartEdge router by following the instructions in Reference [2] provided with the card.

You see the following responses in the NetOp client when you install a card:

- In a slot preprovisioned for an ASE card:

    — In the object navigator of the Card Provision view, in the slot for the ASE card, a card icon appears in the Physical column, and the alarm indicator on the card icon in the Provision column disappears. Both icons are labeled "ASE".

    — In the Card Fault view, the "Circuit Pack Missing" fault is cleared.

    Note: We do not recommend preprovisioning an ASE card in a SmartEdge router.

- In an empty unconfigured slot:

    — In the object navigator of the Card Provision view, in the slot that the ASE card is installed, a card icon appears in the Physical and Provision columns. Both icons are labeled "ASE".

    — In the Card Fault view, no new faults appear.

- In a slot preprovisioned for another type of card:

    — In the object navigator of the Card Provision view, in the slot that the ASE card is installed, a card icon appears in the Physical and Provision columns. The icon in the Physical column is labeled "ASE," and the icon in the Provision column is labeled with the preprovisioned card type. The alarm indicator on the card icon in the Provision column remains.

    — In the Card Fault view, the "Circuit Pack Mismatch" fault appears.

3.3 Deleting an ASE Card from the SmartEdge Router Configuration

You see the following responses in the NetOp client when you delete an ASE card from the Card Provision view without removing it from the SmartEdge router

- In the object navigator, in the slot that the ASE card is installed, the card icon in the Provision column disappears. An alarm indicator appears on the icon for the ASE card in the Physical column.

- In the Card Fault view, the "Circuit Pack Mismatch" fault appears.

3.4 Removing an ASE Card from the SmartEdge Router

Caution!

Risk of loss of performance. If the ASPs on the ASE card have not been removed from ASP pools there will be a performance impact as Security Services tries to copy the IPsec VPN tunnel configuration to an ASP that is not physically present in the chassis. To avoid this risk, remove the ASPs on the card from ASP pools before removing the ASE card from the SmartEdge router.

You see the following responses in the NetOp client when you remove an ASE card from a SmartEdge router:

- In the object navigator, in the slot that the ASE card is installed, the card icon in the Physical column disappears. An alarm indicator appears on the icon for the ASE card in the Provision column.

- In the Card Fault view, the "Circuit Pack Missing" fault appears.

4   Starting Up and Discovering an ASE Card

The NetOp EMS software detects when an ASE card in the card inventory is physically installed, or shut down and restarted, in a managed SmartEdge router.

Several processing scenarios are possible, each depending on the state of the following items:

- The required software processes.

- The provisioned state of the following items:

  - Log server settings (**General** tab of the node provision view)

  - ASP pools

  - ASP groups

  - Required shared objects needed to configure an IPsec VPN

  - Required contexts and interfaces bound to physical ports on the SmartEdge router

The card appears in the Provision column and operates when all processes are running and all provisioning is completed. Any existing IPsec VPN configurations are sent to the ASPs in the associated ASP group. New IPsec VPN configurations are sent as they are provisioned. IPsec VPN configurations succeed when connectivity exists between both endpoints.

If any of the following conditions occur, the card appears in the Provision column, with the ASPs held in a waiting state, and any existing VPN configurations are not sent to the ASPs in the associated ASP group

- The log server settings are not provisioned.

- The log server process is not running.

- The device manager process is not running.

- The ASP group to which the ASPs belong is not associated with the context used by the IPsec VPN.

5 Verifying the Status of ASPs

Use the card active view to verify the status of the ASP devices on an ASE card. This view provides the following information for each ASP on the card:

- Operating State (Up or Down)

- Role (Active or Backup)

- Assigned ASP pool

- Allocated ASP group

- Assigned service (only Security is available in the current release)

To verify the status of an ASP:

1. In the object navigator, find the node and navigate to the ASE card.

2. Click **Active** in the management view launch bar.

   The Active view for the ASE card appears. Read-only information for each ASP on the card is displayed.

Note: The information that appears in the Active view for the ASE card is the same as the output from the **show asp detail** command using the Command Line Interface (CLI) of the SmartEdge OS.

6 Adding, Changing, or Removing ASP Pools

You can define an ASP pool at any time; however, you cannot add ASPs to an ASP pool until an ASE card is installed in the SmartEdge router. If you are using the ASE Licensing view to manage the ASE licenses, do not add ASPs to an ASP pool using the ASP pool provisioning view.
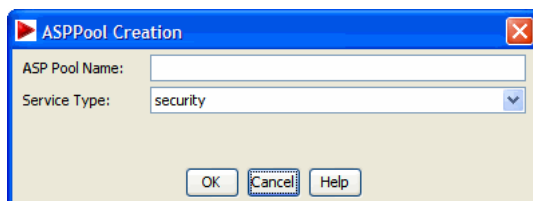
An ASP pool definition contains the following information:

- A list of the ASPs on the ASE cards installed in a SmartEdge router assigned to this pool.

- The specific service provided by the ASPs in the pool.

  Currently, only the Security service type is defined.

To add, edit, or delete an ASP pool:

1. Find the node and open its ASP pool provision view.

2. Choose one of the following tasks:

   - Add an ASP pool—Click ✚ in the management view launch bar. The ASP Pool Creation dialog box appears as shown in the figure below. Go to step 3.

   - Edit an ASP pool—Click the ASP pool in the object navigator. The ASP pool provision view is updated. Go to step 4.

   - Delete an ASP pool—Click **Delete** on the management view launch bar, and then click **OK** in the dialog box that appears. An ASP pool cannot be deleted while an ASP group belongs to the pool.

3. Type the name of the new ASP pool, and then click **OK**. The new ASP pool appears in the ASP pool provision view.

4. For a new ASP pool, the list of ASP devices is empty; otherwise, previously added ASPs are listed. ASPs can only be added after an ASE card is installed in the SmartEdge router.

    Choose one of the following tasks:

    - Add an ASP device to the pool—Click **Add** to open the Add a New Device dialog box. Go to step 5.

    - Remove a device from the pool—Click **Remove**, and then click **OK** in the dialog box that appears.

5. In the **Add a New Device** dialog box, complete the steps in Table 3.

Table 3   Steps to Add a New Device to an ASP Pool

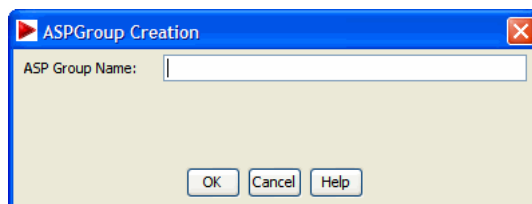| Step	Task	Instructions
1	Identify the card type	Click **Search** and select the slot containing the ASE card in the **Select Card** dialog box.
2	Specify the slot number	The slot number appears in the **Slot Number** field.
3	Specify the device ID	Type the device ID in the **Device ID** field. There are two ASPs on an ASE card, **1** and **2**.

7 Adding, Changing, or Removing ASP Groups

An ASP group contains the following information:

- The ASP pool that provides the ASPs for the group

- The number of ASPs requested from the ASP pool

- The priority of the ASP group

  Priority determines the distribution of ASPs to groups when the number of available ASPs is fewer than the total requested as well as which ASP group is allocated a newly operational ASP.

To add, edit, or delete an ASP group, do the following:

1. Find the node and open its ASP group provision view.

2. Choose one of the following tasks:

   - Add an ASP group—Click ✚ in the management view launch bar. The **ASP Group Creation** dialog box appears as shown in the figure below. Go to step 3.

   - Edit an ASP group—Click the ASP group in the object navigator. The ASP group provision view is updated. Go to step 4.

   - Delete an ASP group—Click **Delete** on the management view launch bar, and then click **OK** in the dialog box that appears. Any context associations with the ASP group are removed.

3. Type the name of the new ASP group, and then click **OK**. The new ASP group appears in the ASP group provision view.

4. In the ASP Group area of the ASP group provision view, complete the steps in the following table.

Table 4   Steps to Complete the ASP Group Fields

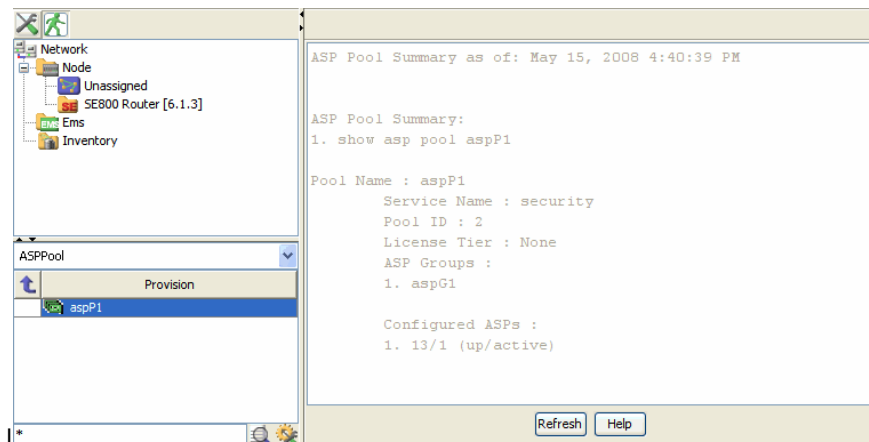| Step	Task	Additional Instructions
1	Identify the ASP pool.	Click **Search** to select an existing ASP pool, or type the name of the ASP pool in the **Pool Name** field.
2	Specify the ASP count.	Specify a value in the **ASP Count** field from the following ranges • SmartEdge 400: 1–6 • SmartEdge 600, 800, 1200, and 1200H:1–22
3	Specify the priority of the ASP group.	Specify a value in the **Priority** field from the range 1–1024, where 1 is highest possible priority and 1024 is the lowest. Accept the default value to set the priority to the highest possible value.

8   Verifying the Status of ASP Pools

Use the ASP pool active view to verify the status of the ASP pools on a SmartEdge router. This view provides the following information for each ASP pool:

- The service assigned to the pool.

- Licensing information.

- ASP groups associated with the pool.

- Location and state of each ASP enrolled in the pool and assigned to ASP groups to provide the assigned service.

To verify the status of an ASP pool:

1. In the object navigator, find the node and navigate to the ASP pool.

2. Click **Active** in the management view launch bar.

   The Active view for the ASP pool appears. The view contains read-only information.

Note: The information that appears in the Active view for the ASP pool is the same as the output from the `show asp pool detail` command using the CLI of the SmartEdge OS.
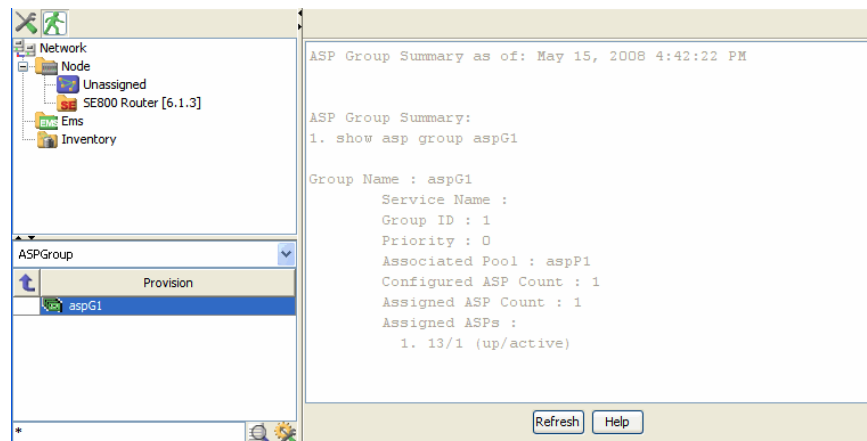
9 Verifying the Status of ASP Groups

Use the ASP group active view to verify the status of the ASP group on a SmartEdge router. This view provides the following information for each ASP group:

- The ASP pool the group is enrolled in.

- The number of ASPs allocated to the group.

- The location and state of each assigned ASP.

To verify the status of an ASP group, do the following:

1. In the object navigator, find the node and navigate to the ASP group.

2. Click **Active** in the management view launch bar.

   The Active view for the ASP group appears. Read-only information is displayed.

Note: The information that appears in the Active view for the ASP pool is the same as the output from the **show asp group detail** command using the CLI of the SmartEdge OS.

10   Associating Contexts With ASP Groups

You enable a context to provide ASE-based security on traffic that flows through the context by associating it to an ASP group. This association directs traffic carried on the context to the ASPs in the associated group for processing. You can associate all or some of the contexts with the same ASP group, or associate each context to a different ASP group. The association is made one context at a time, up to a maximum of 16 contexts. Before you can make this association, the ASP group must be defined; for more information, see Section 7 on page 15.

Caution!

Risk of inability to associate a context with Security Services. Contexts with names containing the following characters cannot be associated with Security Services: > < &

To avoid this risk, do not associate a context that has any of these characters in its name to an ASP group.

To specify the Security Services attributes of a context, do the following:

1. Find the node, open the Context object, select the context, and open the context provision view.

2. Identify the ASP group that you want to use to process all traffic for this context in the **Security ASP Group** field. Select the **Security ASP Group** check box and click **Search** to select an existing ASP Group, or type the name of the ASP group.

3. Click **Apply**.

Glossary

ASE
Advanced Services Engine

ASP
Advanced Services Processor

ASPs
Advanced Services Processors

CLI
Command Line Interface

EMS
Element Management System

IPsec
IP Security

NAT
Network Address Translation

VPN
Virtual Private Network

Reference List

[1]   *SmartEdge and SM Node Configuration*, 1543-CRA 119 1171/1

[2]   *Quick Installation Guide for the SmartEdge Advanced Services Engine Card*, 9/153 30-CRA 119 1170/1-V1