Administering SAL on Avaya Aura ™ System Platform

November 2009

Issue Number: 1

Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document may be incorporated in future releases.

Documentation disclaimer
Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees
against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer
Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all of the time and we have no control over the availability of the linked pages.

Warranty
Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the following Web site: http://www.avaya.com/support

Copyright
Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Open Source Attribution
The Product utilizes open source software. For copyright notifications and license text of third-party open source components, please see the file named Avaya/Gateway/LegalNotices.txt in the directory in which you have installed the software.

Avaya support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

The *SAL (Secure Access Link) Gateway Implementation Guide* (http://compasweb.dr.avaya.com/cgi-bin/wwwcompas?prodid=140284&dformat=pdf) provides an overview of the SAL 1.5 and explains how to install the gateway and configure the gateway for the remote service of managed devices for the use of support Avaya Customers, Business Partner and Avaya personnel. You can read the Gateway Implementation Guide to understand how SAL 1.5 works and gain some background on how to install and configure SAL gateway in general.

This document focuses on how to make the SAL gateway configurations especially for System Platform (SP) and how to test remote access and alarming for SP and the products (in the MBT/SP template) running on the virtual machines of SP.

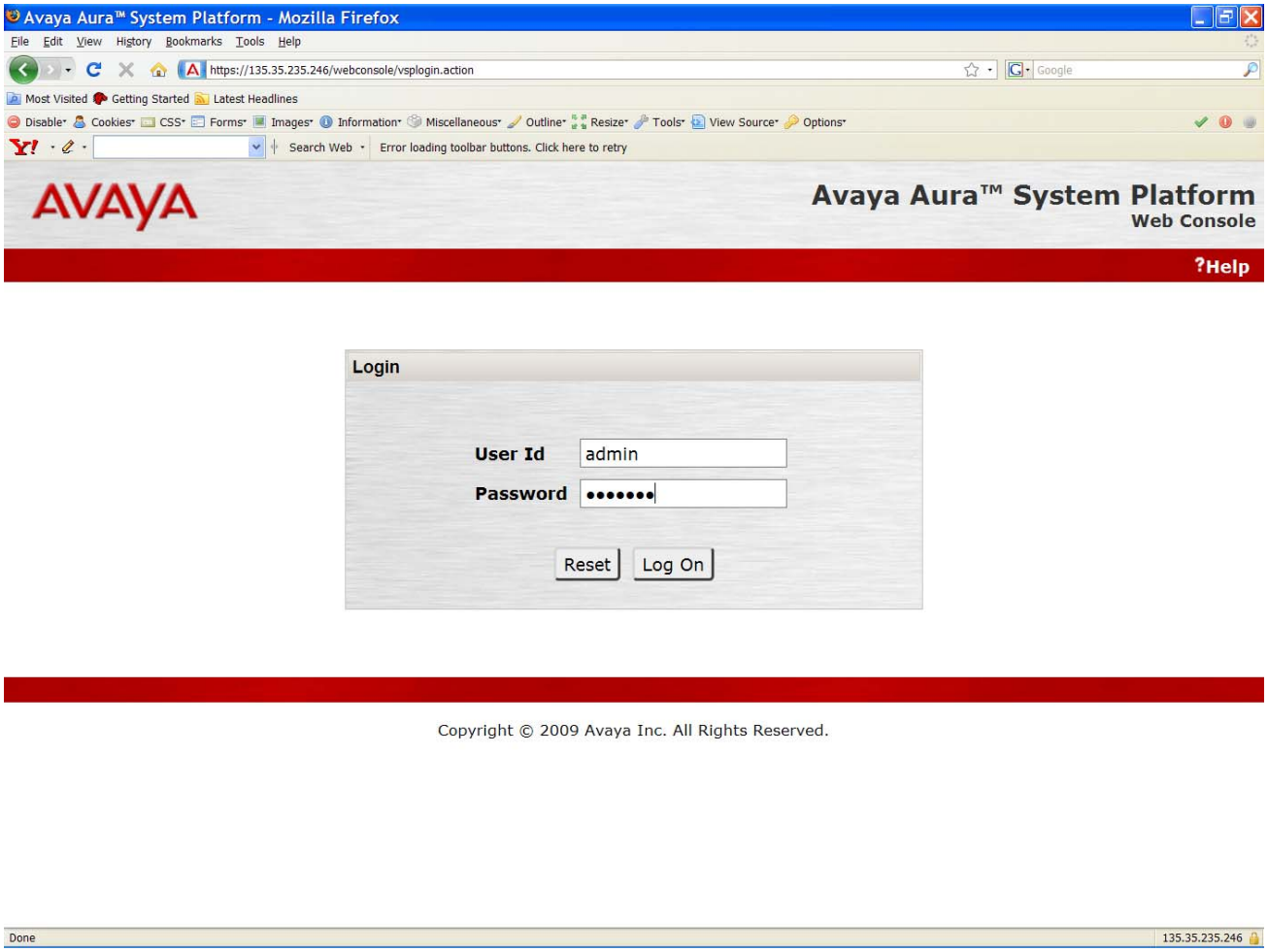
SAL Gateway configurations

The SAL (Secure Access Link) Gateway includes a Web-based Gateway UI that provides status information, configuration interfaces, and logging. This section describes how to configure the gateway and the managed devices for alarming and remote access. The devices include SP's domain0 (dom0), console domain (cdom), and other product virtual machines (CM, CMM, AES, SES, Utility Server and Media Services) in SP.

The configuration steps are described as follows:

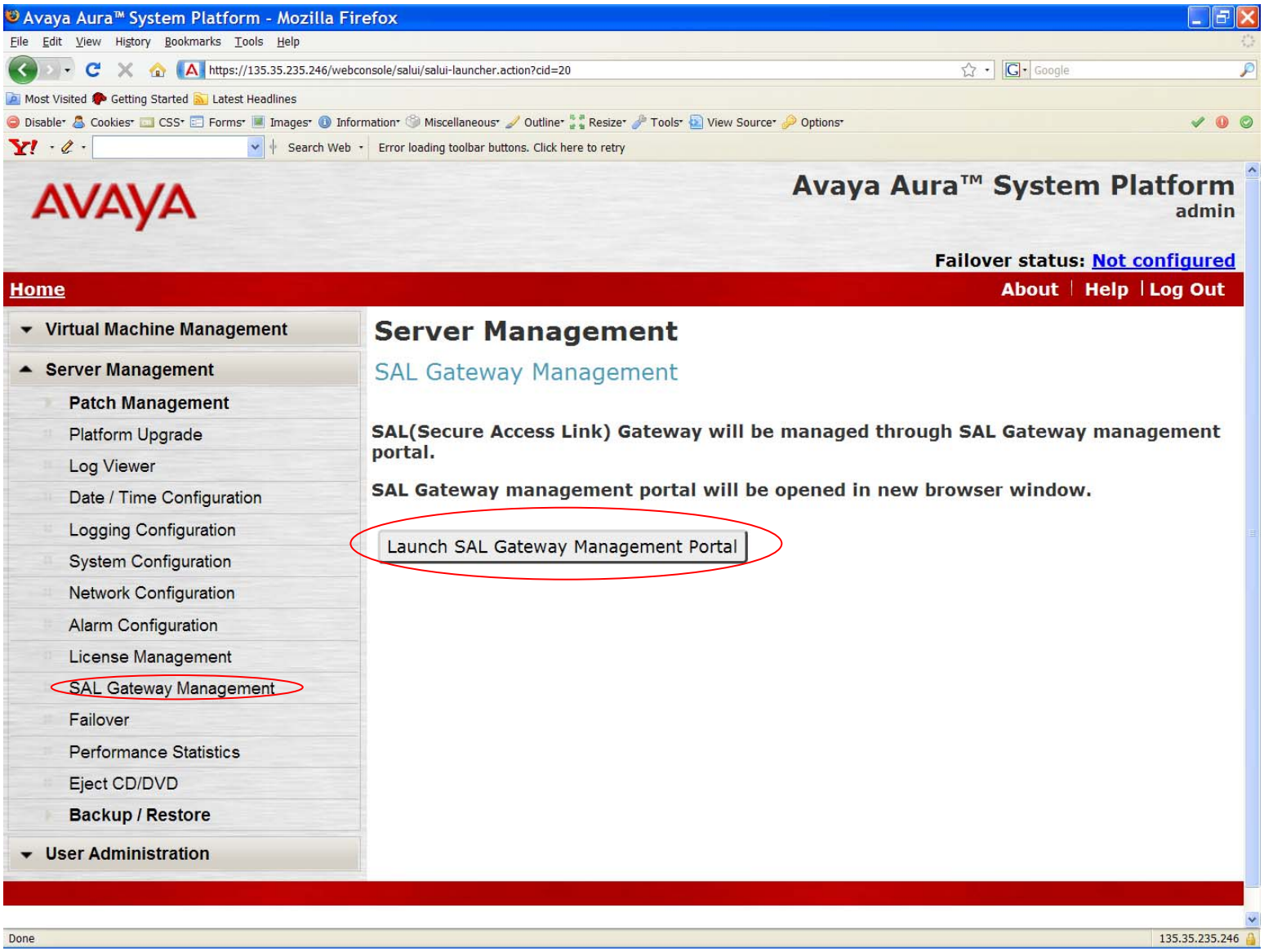
1: To log into the SP Web console:

Go to Avaya Aura System Platform's Web console https://*<SP cdom name or ip addr>*/webconsole and log in.



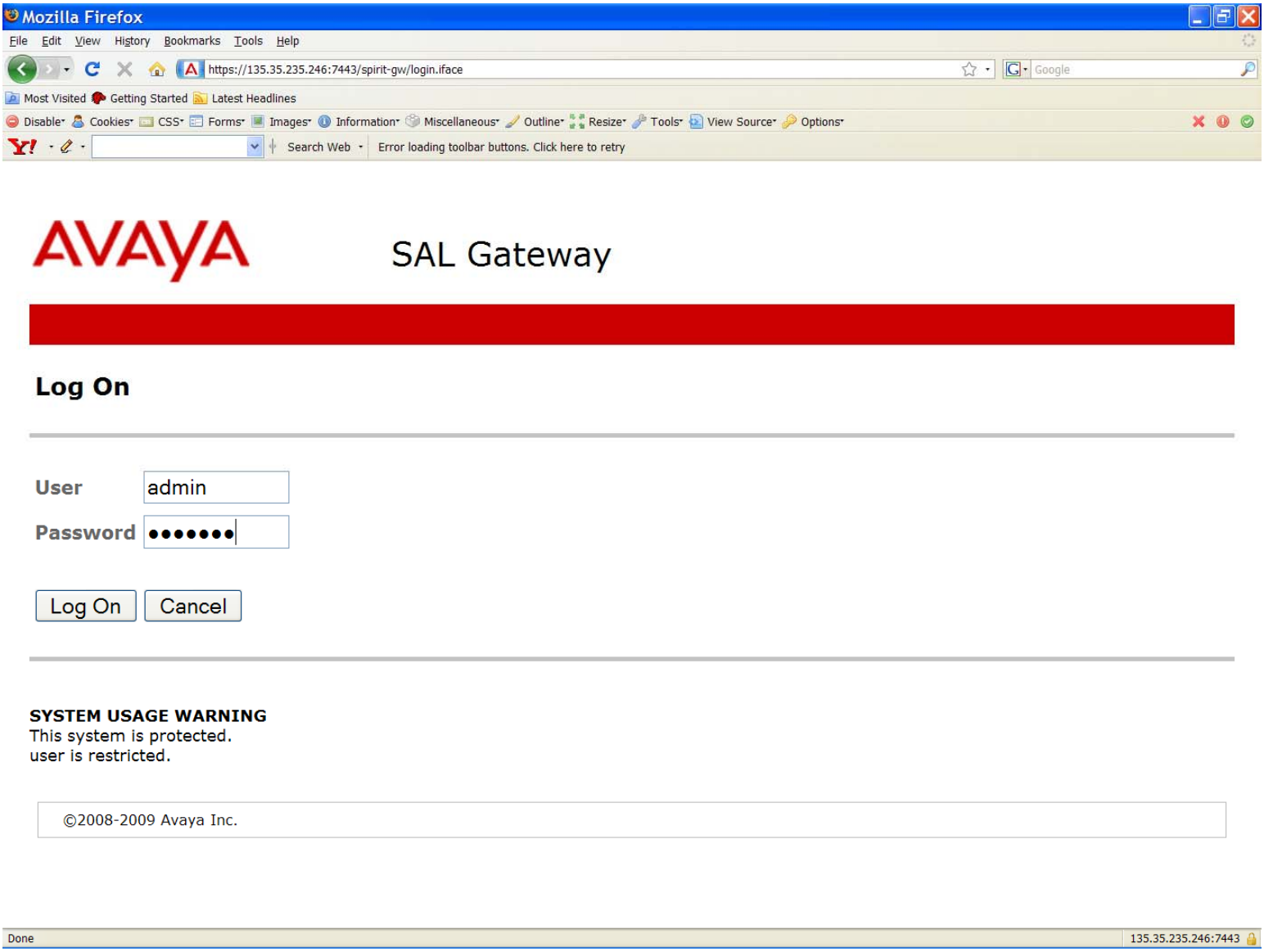
2. To launch the SAL gateway UI:

After logging in, select Server Management from the left side menu and then select **SAL Gateway Management** under **Server Management**. After the SAL Gateway Management page is loaded on the right panel, click **Launch SAL Gateway Management Portal** to launch the SAL Gateway UI.



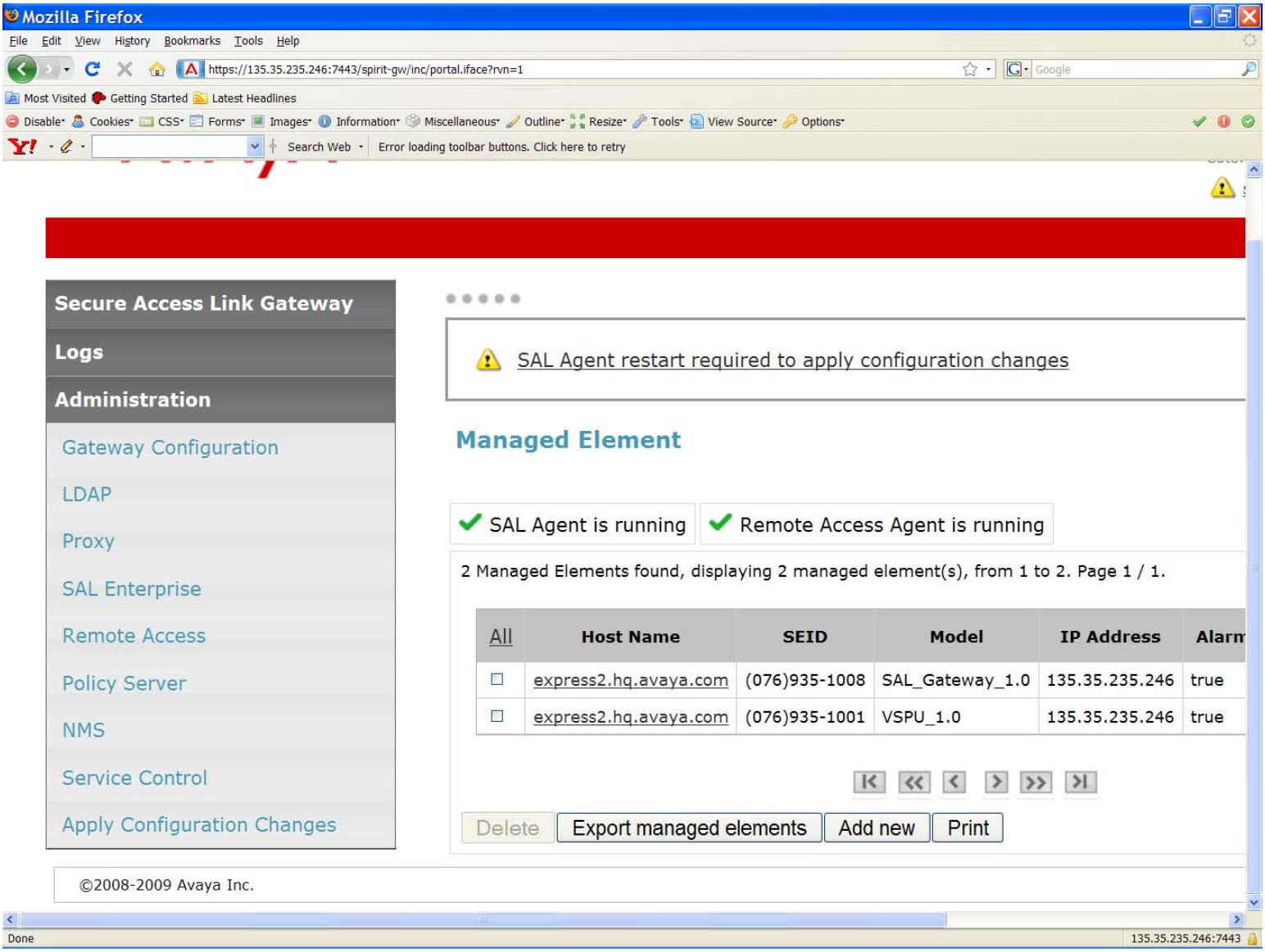
3. To log in to the SAL Gateway UI:

After the SAL Gateway UI is launched, use the same login credentials that you used for the SP Web console to log into SAL Gateway UI.



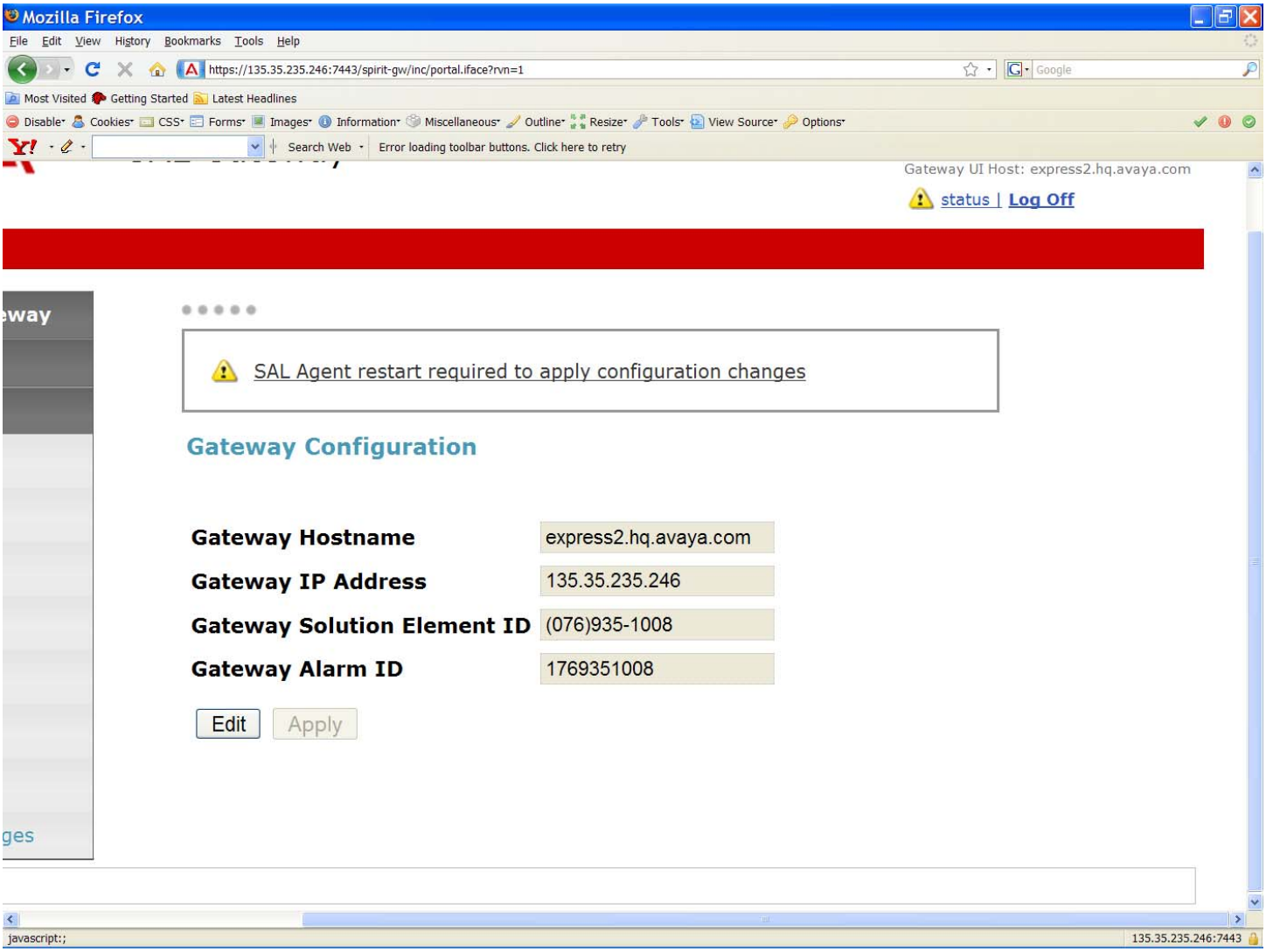
4. On the Gateway home page navigation directory, click **Administration**. The system displays the following items under **Administration**.

- Gateway Configuration
- LDAP
- Proxy
- SAL Enterprise
- Remote Access
- Policy Server
- NMS
- Service Control
- Apply Configuration Changes



5. To configure a SAL Gateway:
    1. Click **Gateway Configuration** in the **Administration** section of the SAL Gateway menu.
       The system displays the Gateway Configuration in the body of the web page.
    2. To change the configuration, click **Edit**.
       The system displays the Gateway Configuration (edit) panel.
    3. In the **Gateway Hostname** field, enter a distinguishing host name for the SAL Gateway.
    4. In the **Gateway IP Address** field, enter the IP address of the SAL Gateway.
    5. In the **Solution Element ID** field, enter the Solution Element ID that uniquely identifies this SAL Gateway. The SAL Gateway Solution Element ID is used to register this SAL Gateway with the Secure Access Concentrator Remote Server.
    6. In the **Gateway Alarm ID** field, enter the Alarm ID of this gateway.
       The value in the **Gateway Alarm ID** field is used to uniquely identify the source of Gateway alarms to the Secure Access Concentrator Core Server.
    7. To make the required changes. Click **Apply**.
       Notes
       The configuration changes take effect immediately. When you click **Apply**, the system changes the configuration.
    8. To undo the changes you made, click **Undo Edit**.
       The system returns to the configuration before the **Edit** button was pressed.

For more information, see the *Secure Access Link 1.5 Gateway Implementation Guide*.



6. To configure SAL Enterprise:

1. Click **SAL Enterprise** under **Administration** on the navigation directory.
   The system displays the SAL Enterprise page in the right pane.
2. In the **Primary Enterprise** field, enter the IP Address or host name of the primary SAL Enterprise.
3. In the **Port** field, enter the Port number of the primary SAL Enterprise.
4. In the **Secondary Enterprise** field, enter the IP Address or host name of the secondary SAL Enterprise.
5. In the **Port** field, enter the Port number of the secondary SAL enterprise.
6. Click **Apply**.

The page provides three buttons:

- **Edit**: to change the configuration
- **Apply**: to apply the changes made to the configuration
- **Test**: to run the diagnostic tests for connectivity

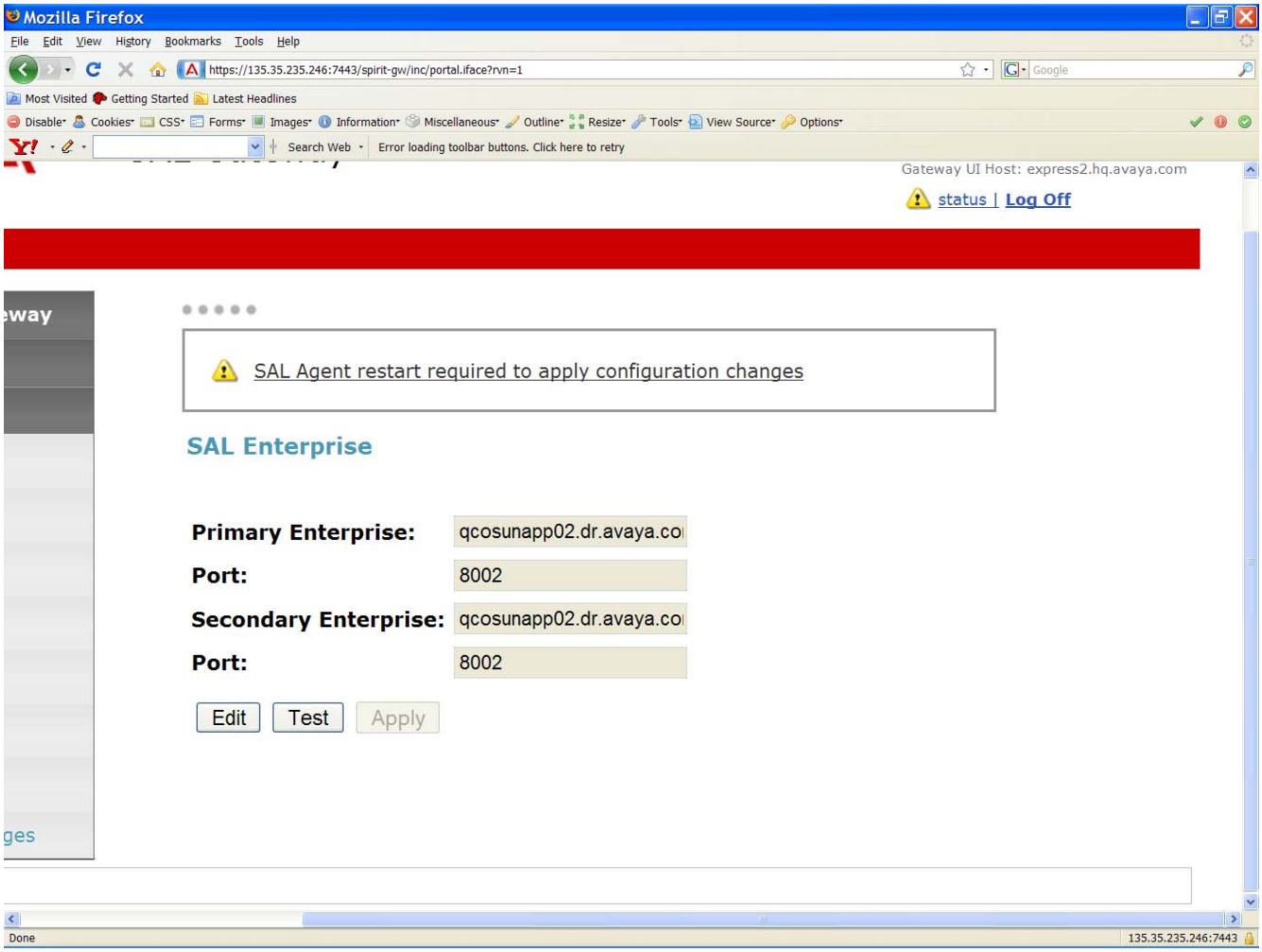
Notes

- You must restart the SAL Gateway for the configuration to take effect. Until you restart the SAL Gateway, it will not connect to the new SAL Enterprise.
- Restarting the SAL Gateway may result in SNMP traps being missed.

If you want to use the **Avaya production enterprise server**, you need to do the following:

1. Enter **alarming.esp.avaya.com** for Primary Enterprise and **8002** for port number.
2. Use the Avaya proxy when connecting from Avaya internal network.

For more information, see the *Secure Access Link 1.5 Gateway Implementation Guide*.



7. To configure Remote Access Server:
    1. Click **Remote Access** under **Administration** on the navigation directory.
       The system displays the Remote Access page in the right pane.
    2. In the **Primary Enterprise** field, enter the IP Address or host name of the primary Remote Access Server.
    3. In the **Port** field, enter the port number of the primary Remote Access Server.
    4. (*Optional*) In the **Secondary Enterprise** field, enter the IP Address or Host name of the secondary Remote Access Server
    5. (*Optional*) In the **Port** field, enter the port number of the secondary Remote Access Server
    6. Click **Apply**.

    The page displays three buttons:
    - **Edit**: to change the configuration
    - **Test**: to send a test SAL Gateway alarm to the Secure Access Concentrator Core Server
    - **Apply**: to apply a configuration or apply the changes made to the configuration

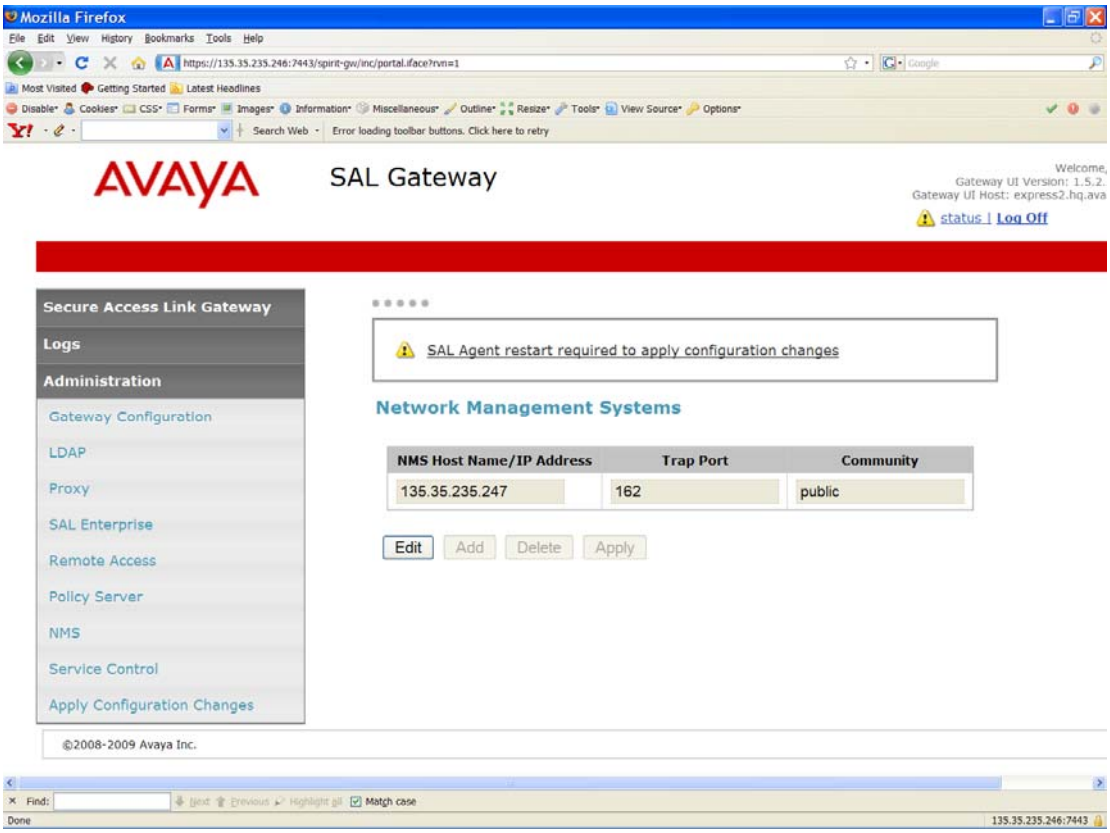
    Note
    - You must restart the SAL Gateway for the configuration to take effect. Unless you restart the SAL Gateway, it will not connect to the new Secure Access Concentrator Remote Servers.
    - Restarting the SAL Gateway terminates all connections.

For more information, see the *Secure Access Link 1.5 Gateway Implementation Guide*.

8. To configure NMS:
    1. Click **NMS** under **Administration** on the navigation directory.
       The system displays the **Network Management Systems** page.
    2. In the **NMS Host Name/ IP Address** column, enter the IP Address or host name of the NMS server.
    3. In the **Trap port** column, enter the port of the NMS server.
    4. In the **Community** column, enter the community string of the NMS server.
    5. Click **Apply**.
    6. You add multiple NMS(s) using **Add** button.

For more information, see the *Secure Access Link 1.5 Gateway Implementation Guide*.

Note: Enter **public** as the Community because currently **public** is the only community supported by SAL agent.



9. To manage Service Control:

You can view the status of a service, stop a service, or test a service that the SAL Gateway manages. Click **Service Control** under **Administration** on the navigation directory.

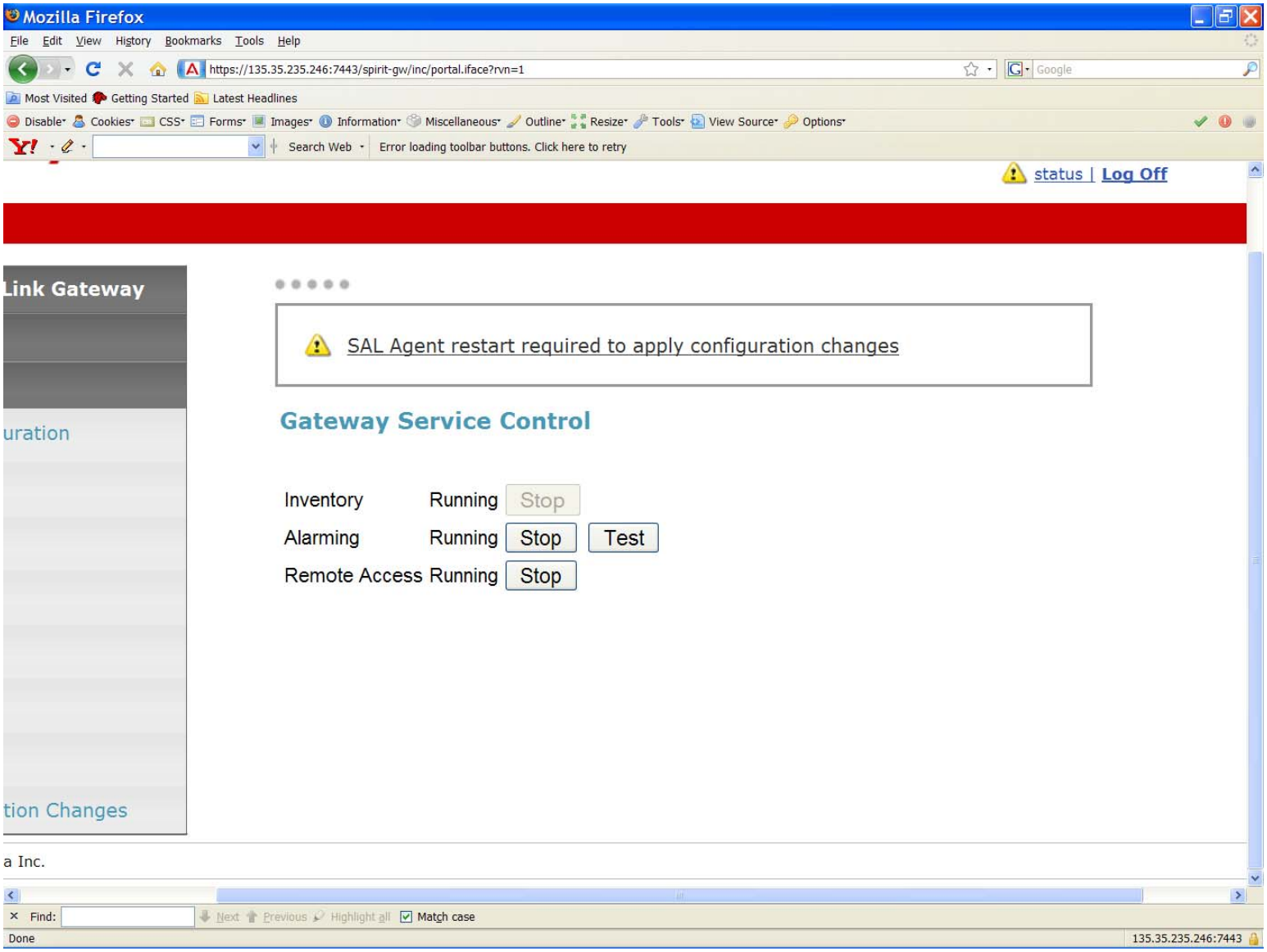
The system displays the Gateway Service Control page. The page lists the following services:

- Inventory (disabled in the current release)
- Alarming
- Remote Access

The Gateway Service Control page also displays the status of each service as:

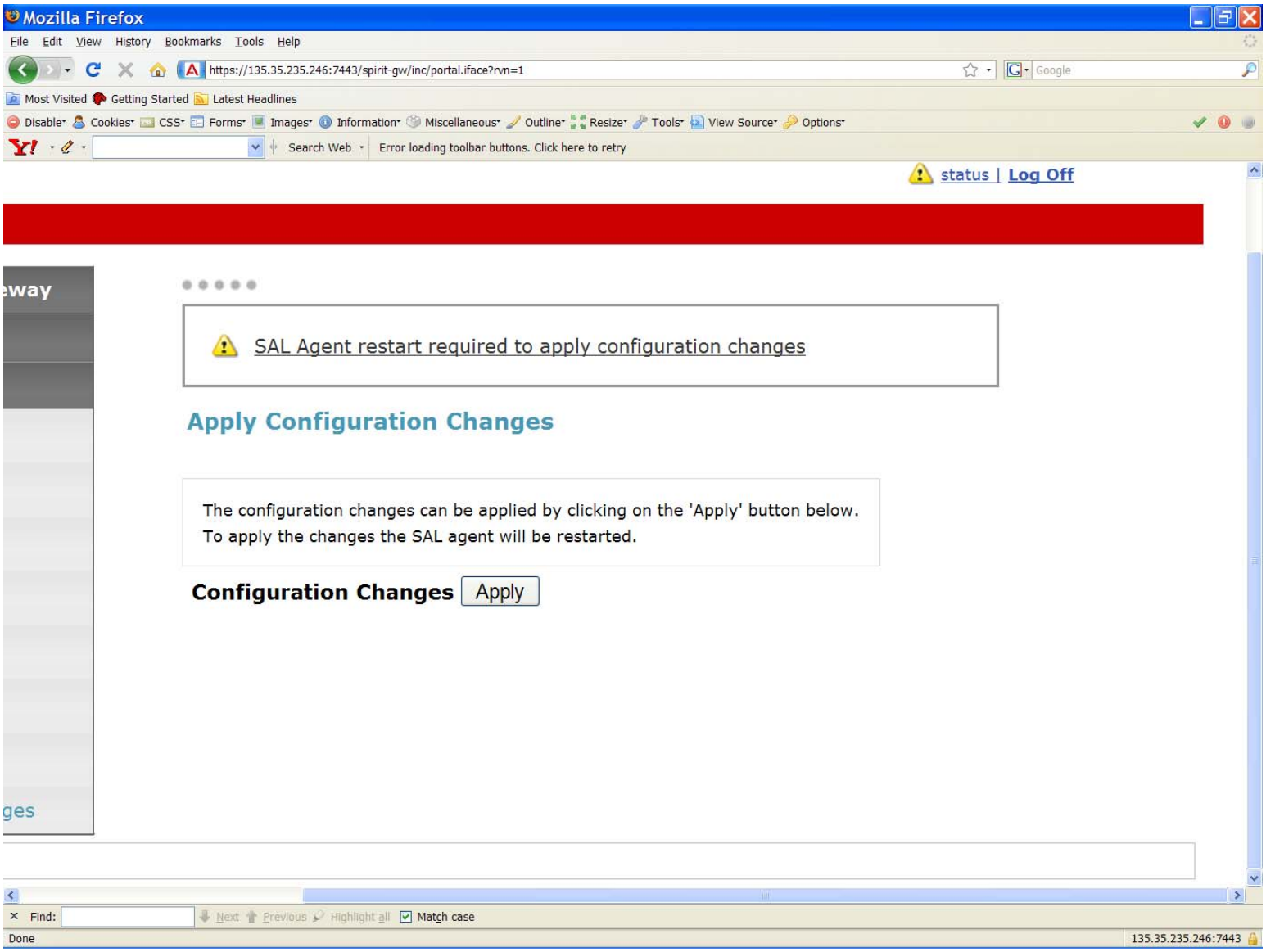
- Stopped
- Running

For more information, see the *Secure Access Link 1.5 Gateway Implementation Guide*.



10. To apply configuration changes:
    1. Click **Apply Configuration** Changes.
       The system displays the Apply Configuration Changes page.
    2. Click the **Apply** button beside Configuration Changes.
       When you click **Apply**, the SAL Gateway is restarted and updated with the new values you configured. All configuration changes that you made, take effect.

For more information, see the *Secure Access Link 1.5 Gateway Implementation Guide*.



11. To configure a managed element:
    1. Click **Managed Element** on the navigation directory.
       The system displays the Managed Element page.
    2. Click **Add new**.
    3. In the **Host Name** field, enter a host name for the managed device.
    4. In the **IP Address** field, enter the IP address of the managed device.
    5. Select the **NIU** check box if you want to use a Network Interface Unit port for remote access and select a value from the list box.

    Note: The range of values allowed is 1 through 9. Some older managed devices can only be reached on a network though an NIU interface. The NIU emulates a modem to convert a managed device from modem support to network accessibility. To make a remote connection to NIU-supported devices, it is necessary to know which NIU port number to connect to.

    6. In the **Solution Element ID** field, enter the Solution Element ID of the device.
    7. In the **Product ID** field, enter the Product ID or Alarm ID.
    8. In the **Model** field, enter the model that is applicable to this managed device.
    9. Select the **Provide Remote Access to this device** check box, if you want to allow the ability to remotely connect to the managed device.
    10. Select the **Transport alarms from this device** check box, if you want alarms from this device to be sent to the Secure Access Concentrator Core Server.
    11. Select the **Collect Inventory for this device** check box, if you want an inventory schedule at the managed device level. This selection manages Inventory Collection and sends the inventory to Avaya. The selection also decides the Inventory Collection Schedule interval. *This feature is not available yet*.
    12. Click **Add**.

    To change the configuration, to apply the changes, and to delete the configurations, click the **Edit**, **Apply**, and **Delete** buttons respectively.

    Note
    After you select **Apply** or **Delete**, you must restart the SAL Gateway services for the configuration to take effect.

Special Notes on the relationship between the product device managed by the SAL gateway and the models the managed device should use.

Products	***Models***
SP Dom0	*VSP_1.0*
SP CDom	*VSPU_1.0*
SAL Gateway	*SAL_Gateway_1.0*
CM	*CM_Media_server_1.0*
CMM	*CM_Media_server_1.0 (temporary solution)*
AES	*AES_1.0*
SES	*SIP_Server_1.0*
Utility Server	*VUS_1.0*
Media Services	*Cobar_1.0*

You can create a cheat sheet as follows:

SP domain	IP Addr	SEID	Product ID	Models	Notes
Dom0	10.0.0.66	(076)934-2000	7000135491	VSP_1.0	
Cdom	10.0.0.67	(076)934-2001	5023427441	VSPU_1.0	
Dom1-CM	10.0.0.71	(076)934-2002	1000237197	CM_Media_server_1.0	
Dom1-CMM	10.0.0.72	(076)934-2003	2000041897	CM_Media_server_1.0	Use CM model as a temporary solution
Dom2-SES	10.0.0.73	(076)934-2004	1000237198	AES_1.0	
Dom3-AES	10.0.0.74	(076)934-2005	4000006620	SIP_Server_1.0	
Dom4-Utility	10.0.0.75	(076)934-2006		VUS_1.0	
Dom5-Media_Services	10.0.0.76	(076)934-2007		Cobar_1.0	

Note:

- There is no alarm mechanism in Utility Server and Media Service; you need not enable alarming for the managed elements used by Utility Server and Media Services.
- Dom0 (VSP) does not have alarming enabled, but CDOM (VSPU) has alarming enabled. Dom0 sends all syslog to CDOM, CDOM will trigger alarms on behalf of DOM0. But Dom0 has its own AlarmID (ProductID).
- In SP HA (High Availability) mode, you need two different solution element IDs (SEID) for dom0: One is for active dom0 and the other is for standby dom0. Both SEIDs need to be administered through the SAL Gateway UI.