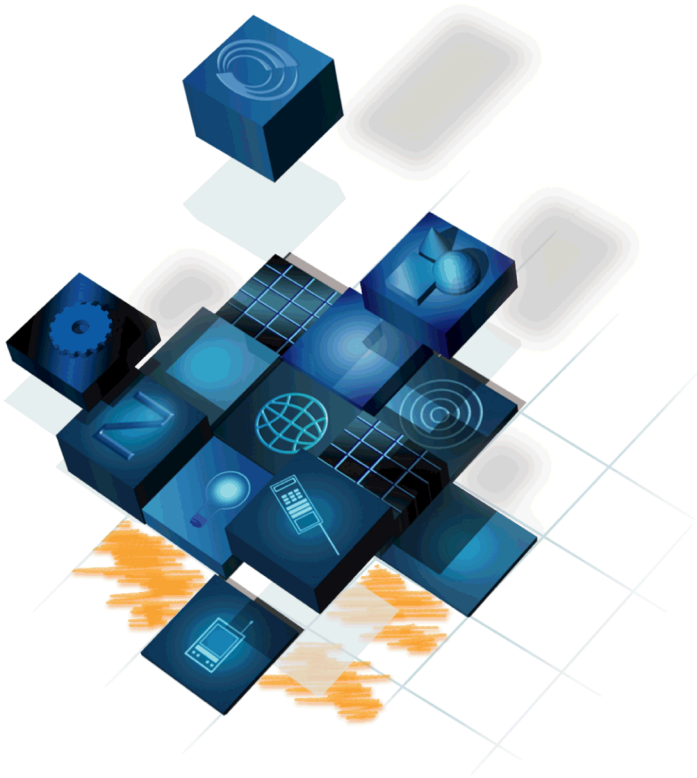
novarra

Engines for Wireless Data



Installation and Administration Guide

Novarra WirelessWeb Enterprise Suite 3.10 Installation and Administration Guide

Abstract

This User's Guide contains server installation procedures, and administration and troubleshooting procedures.

Manning Publications Company; ISBN 188477749X, http://nitric.com/jnp/.

Note:

While every effort has been made to ensure technical accuracy, information in this document is subject to change without notice and does not represent a commitment on the part of Novarra, Inc.

Novarra, Inc.
3232 N. Kennicott
Arlington Heights, IL 60004
Tel: (847) 368-7800
Fax: (847) 590-8144
E-mail: info@novarra.com
Web site: www.novarra.com

Table of Contents

1 Introduction

Thank you for choosing Novarra WirelessWeb Enterprise Suite, the sophisticated wireless software suite that empowers your mobile workforce with seamless access to the Internet, your Intranet, and corporate applications from their wireless devices.

1.1 Product Overview

Novarra WirelessWeb Enterprise Suite transforms and adapts Internet content so that it can be efficiently delivered to mobile devices without customizations to existing content. Our InstantWireless solution allows you to implement your wireless strategies in the fastest time possible and without the time and cost setbacks required for developing custom applications or re-authoring Web content in another markup language.

Novarra WirelessWeb Server has two main components: the Adaptive Content Accelerator and Wireless Connectivity Manager. The Adaptive Content Accelerator performs real-time adaptation of Web content including WAP-compliant phones. The Wireless Connectivity Manager controls wireless sessions, protocols, and content transmission for efficient and secure communication with wireless devices.

WirelessWeb Server supports HTML 4.01, JavaScript 1.3, and WML 1.2 languages. Key objects, such as tables, frames, hypertext links, and forms, are utilized to fully leverage Web-based eBusiness applications on handheld devices. End-to-end security is achieved using HTTP 1.1 Basic Authentication, device authorization, behind-the-firewall deployment, as well as SSL encryption over the Internet and Certicom-based ECC encryption over-the-air.

WirelessWeb microBrowser is a thin-client browser that can be installed on wireless devices to serve as an effective user interface to easily navigate across Internet content or applications. When implemented together, WirelessWeb Server and microBrowser offer an end-to-end information delivery solution that provides efficient communication between the wireless device and Internet/Intranet content.

1.2 About Novarra Documentation

This WirelessWeb Enterprise Suite 3.10 Installation and Administration Guide shows you how to set up, administer, and troubleshoot problems you might encounter with WirelessWeb Server.

The WirelessWeb Enterprise Suite 3.10 Developer's Guide explains the basics of the WirelessWeb Server's normalization process and how you can take advantage of autonormalization, Novarra markup language, and templates to control the presentation of your existing Web content on wireless devices. This document is intended for Web developers.

We're very interested in knowing how we can improve WirelessWeb Enterprise Suite to better meet your needs. Feel free to send any comments or suggestions about the software or documentation to info@novarra.com.

1.3 Contacting Technical Support

Novarra provides technical and installation support for all administrators of this product. Novarra Technical Support is available between the hours of 8:00 a.m. to 5:00 p.m. PST, Monday through Friday. You may reach us at:

E-mail:	support@novarra.com
Telephone:	847-368-7895
Fax:	847-463-0539
Mail:	Novarra Technical Support 3232 N. Kennicott Arlington Heights, IL 60004

When contacting technical support, please be prepared to provide the following information:

- General contact information, including name, company, e-mail, and phone number
- Type of mobile device in use
- Type and version of the operating system
- A brief description of the problem and the steps necessary to recreate it
- Specific error messages

Installing Novarra WirelessWeb Enterprise Suite 2

The Novarra WirelessWeb Enterprise Suite setup provides an easy to use interface for installing the software.

2.1 Pre-installation

If Tomcat JSP Engine has already been installed, check that the **TOMCAT_HOME** environment variable is set to the directory where it is installed.

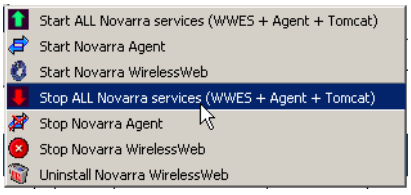
Novarra WirelessWeb Enterprise Suite supports other JSP engine servers. Please contact Novarra Technical Support for more details. For Technical Support contact information see section 1.3, “Contacting Technical Support” on page 1-2.

2.2 Installing Novarra WirelessWeb Enterprise Suite

Warning:

Novarra WirelessWeb, Novarra Agent and Tomcat JSP Engine must be stopped before reinstalling or upgrading:

Start→Programs→Novarra WirelessWeb→Stop ALL Novarra services (WWES + Agent + Tomcat)



2.2.1 Installing WirelessWeb Server

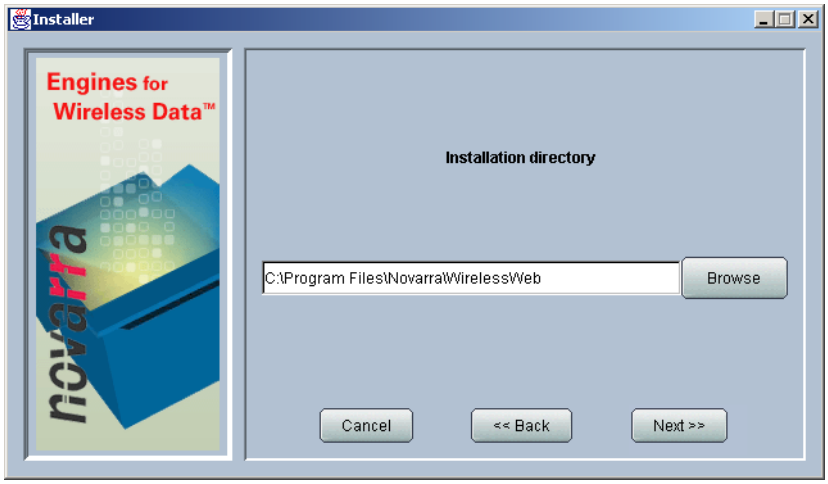
Note:

Make sure you are installing WirelessWeb onto a system that meets the minimum requirements.

The setup performs each of the following procedures:

- Installs the Java Run-Time Environment (JRE)
- Transfers the WirelessWeb software to the hard drive
- Backs up existing configuration files if necessary
- Automatically installs HotSpot™ Server if you do not have the latest version installed

1. Insert the WirelessWeb CD into the CD-ROM drive.
2. From the Windows Start menu, select Run and type:
   `x:\server\setup`
   substituting "x" with the letter designating your CD-ROM drive.
3. Click the OK button.
4. After some initial loading and status text, the Novarra copyright information is displayed. Click Next to continue.
5. The Welcome panel opens to introduce you to the Novarra WirelessWeb installation. Click Next to proceed.
6. Read the license agreement and click the I Agree button to accept its terms.
7. When prompted to select an installation folder (on a clean installation only), either accept the default location (C:\Program Files folder\Novarra\WirelessWeb) or enter a different path. Then, click the Next button to continue.

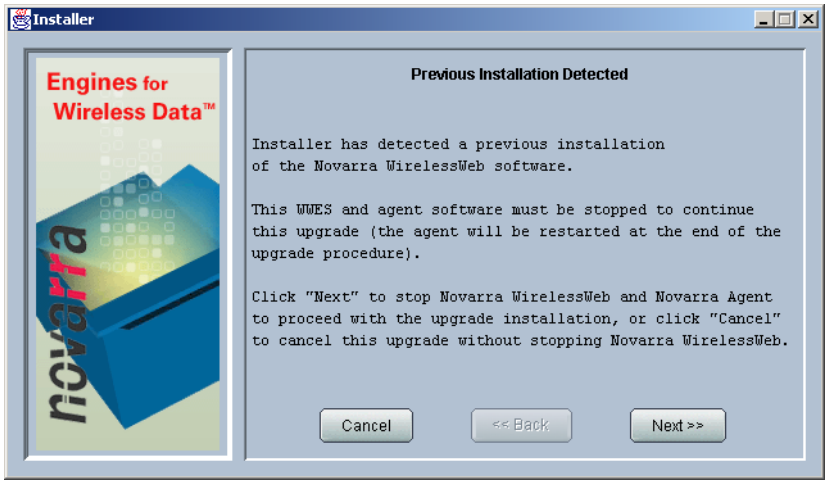


Note:

Since the installation folder varies depending on your system settings or the value you enter in this panel, it is referred to as <WirelessWeb location> throughout the Novarra WirelessWeb Enterprise Suite documentation.

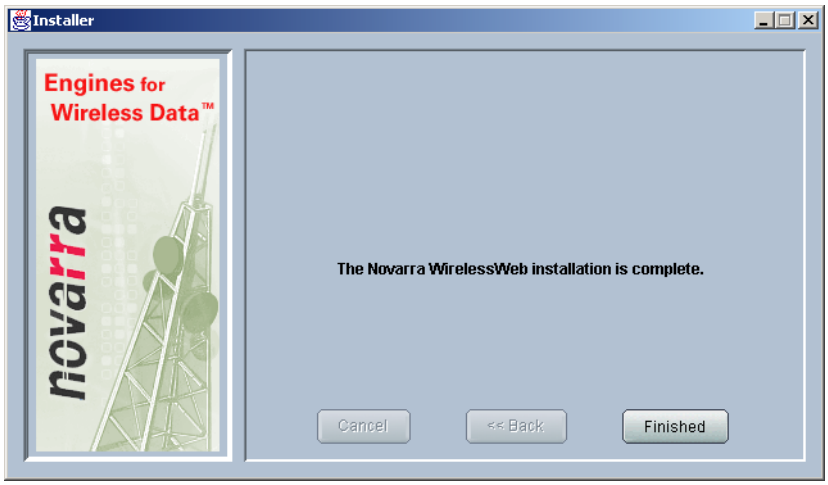
8. If you are reinstalling or upgrading WirelessWeb Server, then the Previous Installation Detected panel is displayed in the setup.

   This panel informs you that the WirelessWeb software must be stopped before proceeding. If you are not ready to stop WirlessWeb, you can cancel the upgrade and come back later.



9. The main file transfer proceeds. Several panels and command prompt screens will appear and disappear. The setup completes its changes to your system such as adding shortcuts and updating the WirelessWeb configuration files. A status bar informs you of the progress.
10. The Novarra Thank you panel appears. Click Next to continue

11. The installation complete panel appears. Click on Finished.



2.2.2 Installing Novarra Management Console

Note:

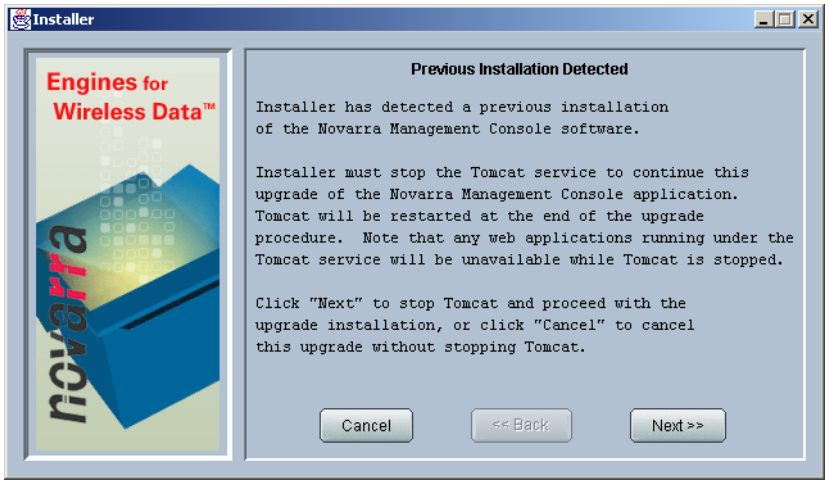
The WirelessWeb Server must be installed before the Novarra Management Console.

1. Insert the WirelessWeb CD into the CD-ROM drive.
2. From the Windows Start menu, select Run and type:

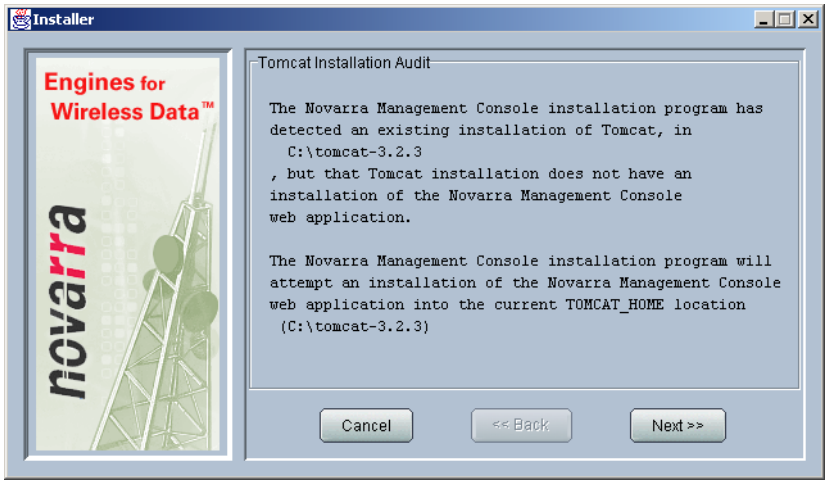
   `x:\server\oamp_setup`

   substituting "x" with the letter designating your CD-ROM drive.
3. Click the OK button.
4. After some initial loading and status text, the Novarra Management Console copyright information is displayed. Click Next to continue.
5. The Welcome panel opens to introduce you to the Novarra Management Console installation. Click Next to proceed.
6. Read the license agreement and click the I Agree button to accept its terms.
7. If this is a new installation (or an uninstall has been performed prior to this installation), go to step 11.
8. If you are reinstalling or upgrading Management Console, then the Previous Installation Detected panel is displayed in the setup.

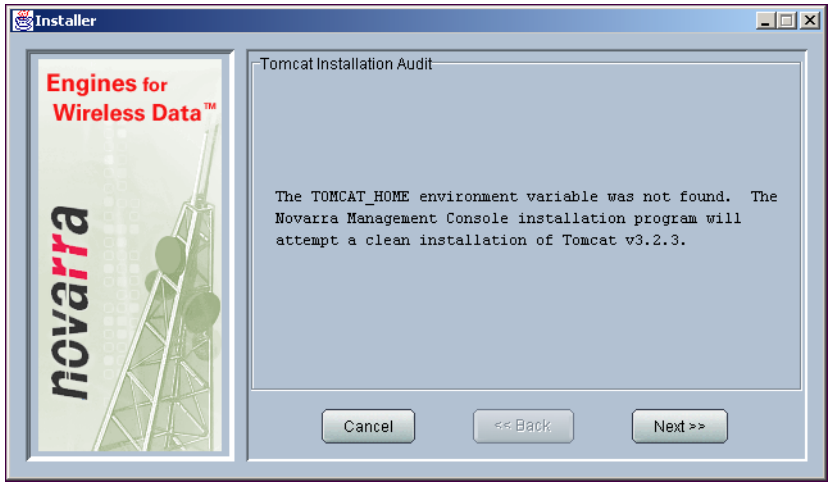
This panel informs you that the Tomcat software must be stopped before proceeding. If you are not ready to stop Tomcat, you can cancel the upgrade and come back later.



9. The main file transfer proceeds. Several panels and command prompt screens will appear and disappear. The setup completes its changes to your system such as adding shortcuts and updating the Management Console configuration files. A status bar informs you of the progress.
10. If you are reinstalling or upgrading Management Console (without having performed an uninstall), then the Tomcat Installation Audit panel appears stating Tomcat was found. Click the Next button to continue. Go to step 16.

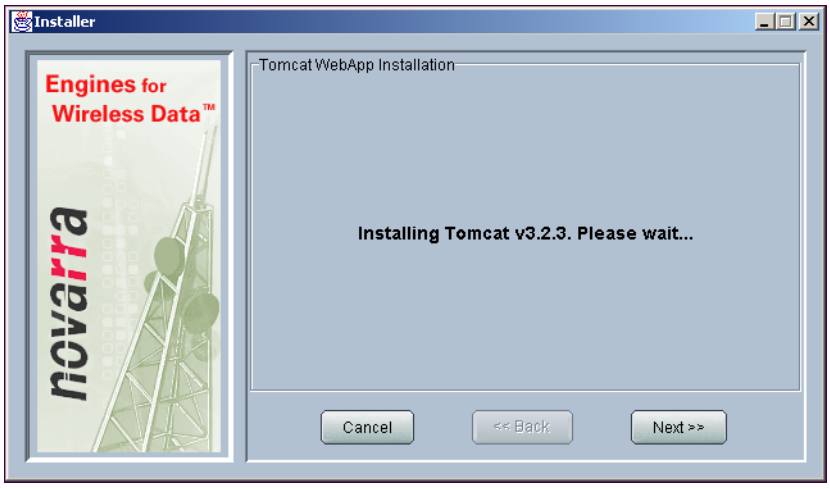


11. If this is a new installation (or an uninstall has been performed prior to this installation), an alert appears asking you to install Tomcat. Click the Next button to continue the installation.

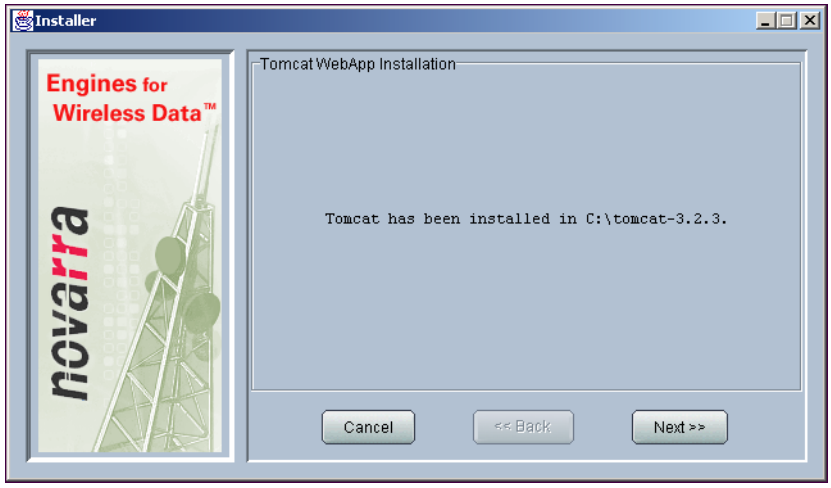


12. Click the Yes button to install Tomcat.

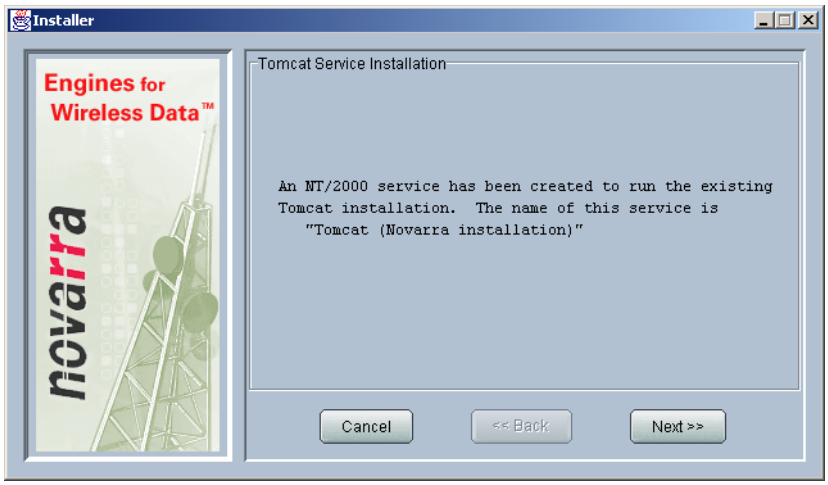
13. The Tomcat Installation panel appears asking you to wait while it installs Tomcat 3.2.3.



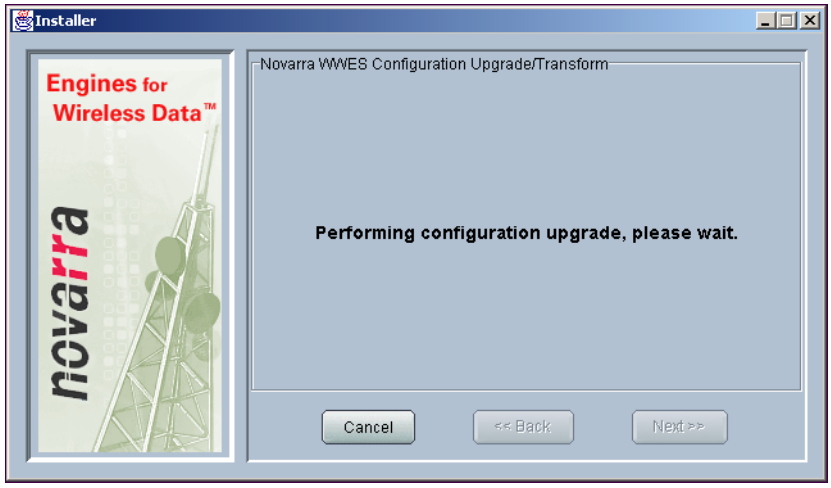
14. The Tomcat Install Complete panel appears. Click the Next button to continue.



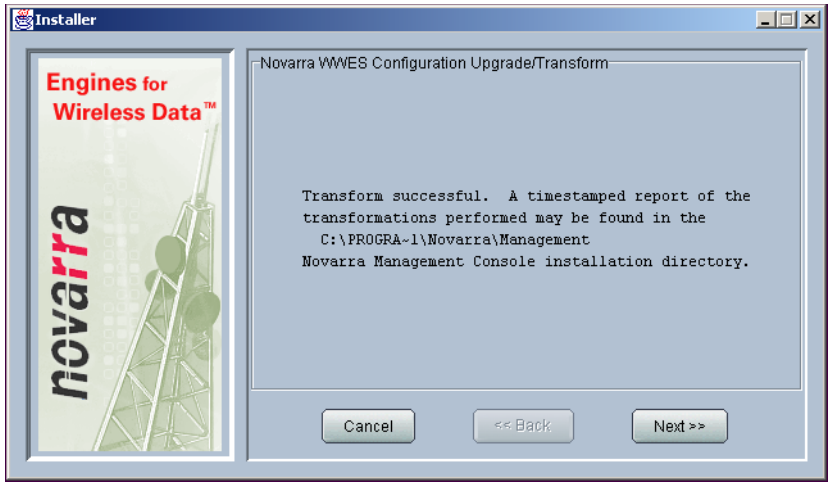
15. The Tomcat Service Installation panel appears. Click the Next button to continue. Go to step 17.



16. If you are upgrading WirelessWeb (without uninstalling first), the Novarra WWES Configuration Upgrade/Transform panel appears.



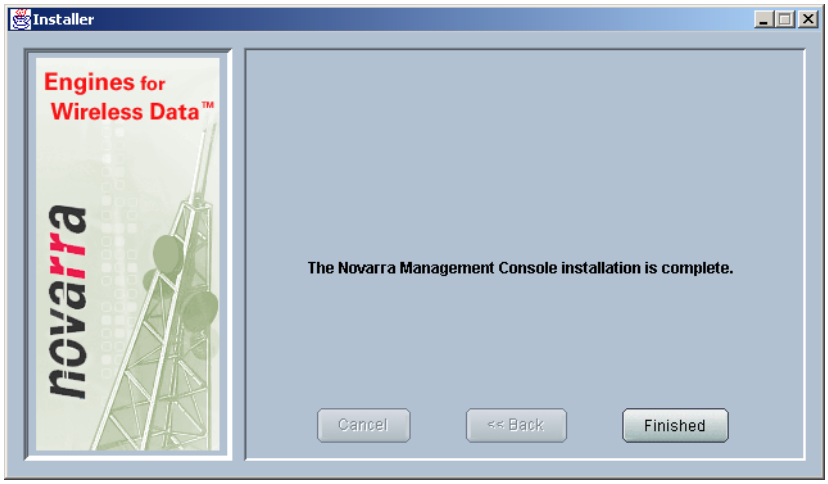
The installer now restores all saved configuration files (for any services and constituent components you may have added, their application configurations, and for any subscriber authorization files you may have added). It also performs an upgrade transformation for any new configuration parameters or groups that may be part of the new release. Any existing configuration that you may have had is preserved.



A panel stating the success appears. The panel also directs you to the logfile which was created as part of the upgrade/transform, so that you may review any updates that were made to your configuration.

17. The Novarra Thank you panel appears. Click Next to continue.

18. The installation complete panel appears. Click on Finished.



2.3 Setting Up WirelessWeb Server

The Management Console provides an easy to use interface for setting up and configuring the server software. Before you can setup WirelessWeb, you may need to prepare some information or reconfigure your firewall in order to allow WirelessWeb to communicate with your wireless network connection.

2.3.1 Preparing to Setup WirelessWeb

You must perform the following prior to beginning the setup.

- Determine the static IP address of WirelessWeb Server.
- Configure your firewall.

2.3.1.1 Determine the Static IP Address of WirelessWeb Server

The IP address of the machine on which you're installing WirelessWeb Server is required so that wireless devices and networks can determine where to route traffic bound for the WirelessWeb Server. Record this information, which you must supply to your network vendor or for use with a wireless device simulator.

Note:

The IP address of WirelessWeb Server must be static because the various networks and wireless devices must always point to the same IP address.

2.3.1.2 Configure Firewall

One of the advantages of WirelessWeb Server is that it can run behind a corporate firewall, adding another layer of security to your company's Internet or Intranet applications.

The following table details how you must configure the firewall to allow traffic from each network to reach WirelessWeb Server. For example, read the first row of data as, "On HTTP networks, forward incoming TCP traffic arriving on port 8827 to the New Server."

Table 2-1: Open ports through firewall

Novarra Connectivity Service	Traffic Type	Default Port	Forward To
HTTP	Incoming TCP	8827	WWES Server
HTTPS	Incoming TCP	8775	WWES Server

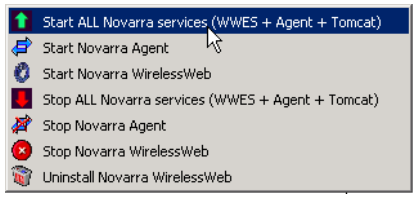
2.3.2 Setup WirelessWeb

2.3.2.1 Start WirelessWeb and Management Console

After installing Novarra WirelessWeb and Novarra Management Console (see Chapter 2, "Installing Novarra WirelessWeb Enterprise Suite"), the programs must be started.

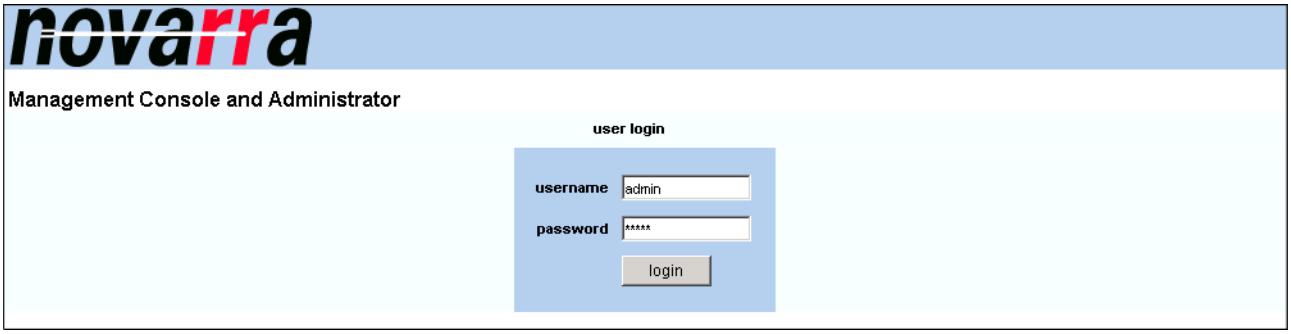
Navigate to and click the "Start ALL Novarra services (WWES + Agent + Tomcat)" shortcut:

Start→Programs→Novarra WirelessWeb→Start ALL Novarra services (WWES + Agent + Tomcat)



2.3.2.2 Login Management Console

1. Navigate to and click the "Management Console Login" shortcut:
   Start→Programs→Novarra Management Console→Management Console Login



2. Enter the username and password and click the login button:

Note:

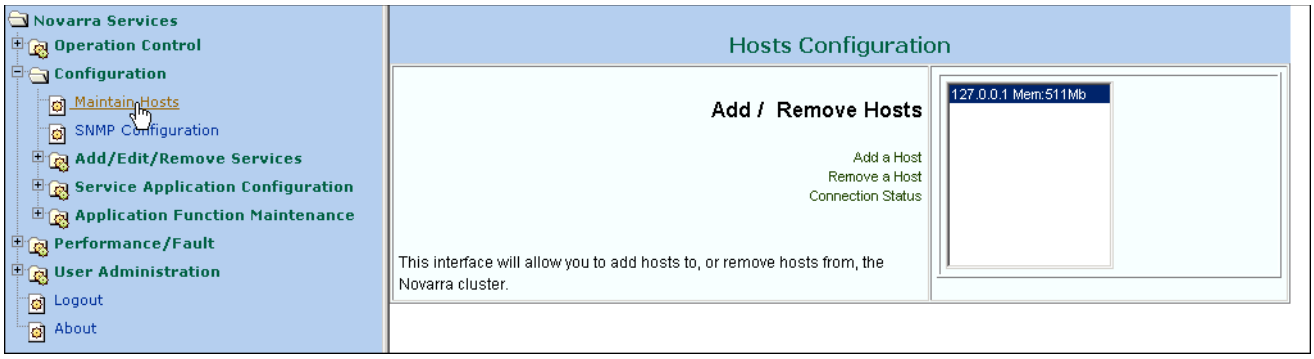
These are defaults and can be changed at a later time.

username: **admin**

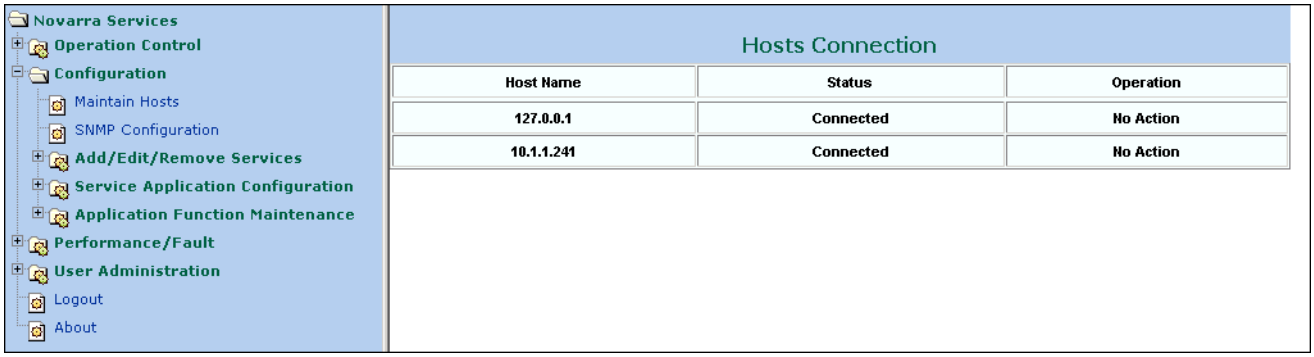
password: **admin**

2.3.2.3 Check Host Connection

1. From the navigation frame on the left hand side of the welcome page, click the + next to **Configuration** to expand the folder. Click the **Maintain Hosts** link. The **Hosts Configuration** frame appears.



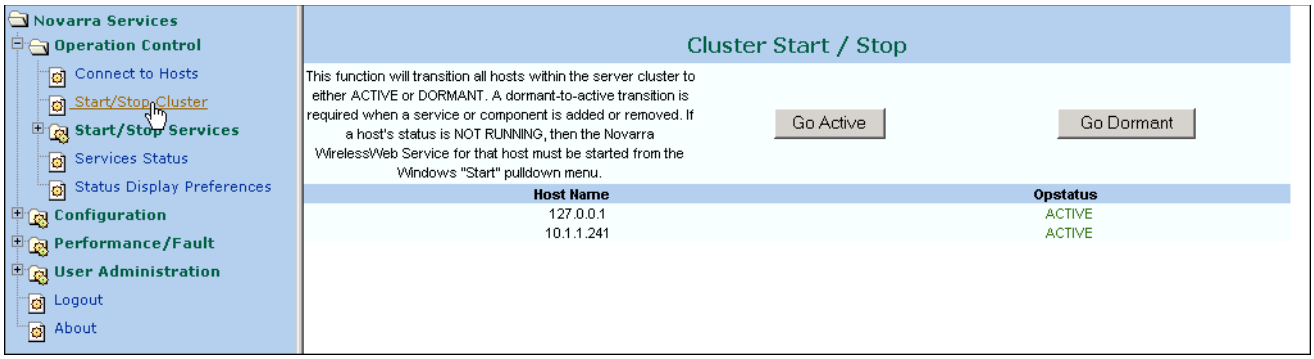
2. In the **Hosts Configuration** frame, click the **Connection Status** link. The **Hosts Connection** frame appears.



3. Make sure the Status for the host is Connected before proceeding.

2.3.2.4 Start Services

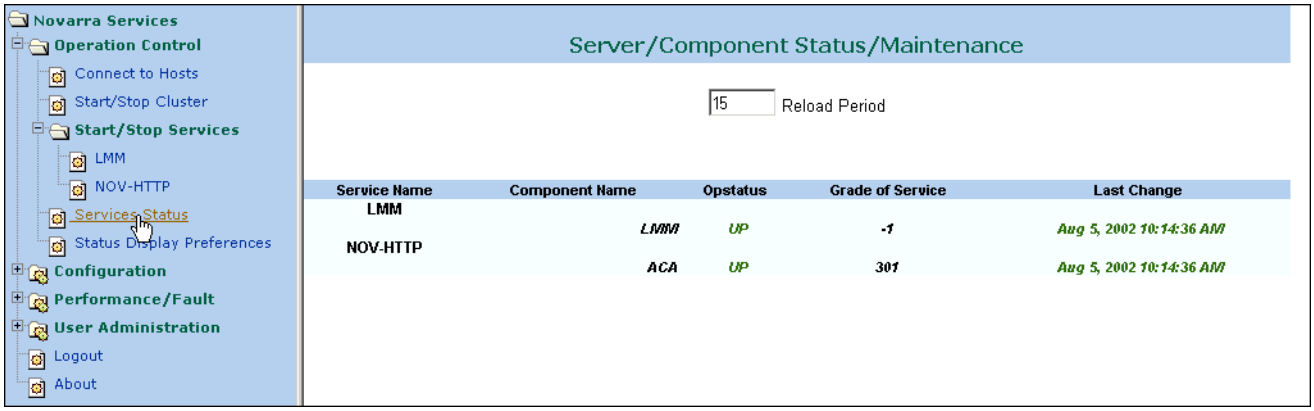
1. From the navigation frame on the left hand side of the page, click the + next to **Operation Control** to expand the folder. Click the **Start/Stop Cluster** link. The **Cluster Start/Stop** frame appears.



2. If the **Opstatus** is **Dormant**, click the Go Active button. The **Opstatus** changes to **ACTIVE**.

2.3.2.5 Check Services Status

1. From the navigation frame on the left hand side of the page, click the + next to **Operation Control** to expand the folder. Click the **Services Status** link. The **Server/Component Status/Maintenance** frame appears.



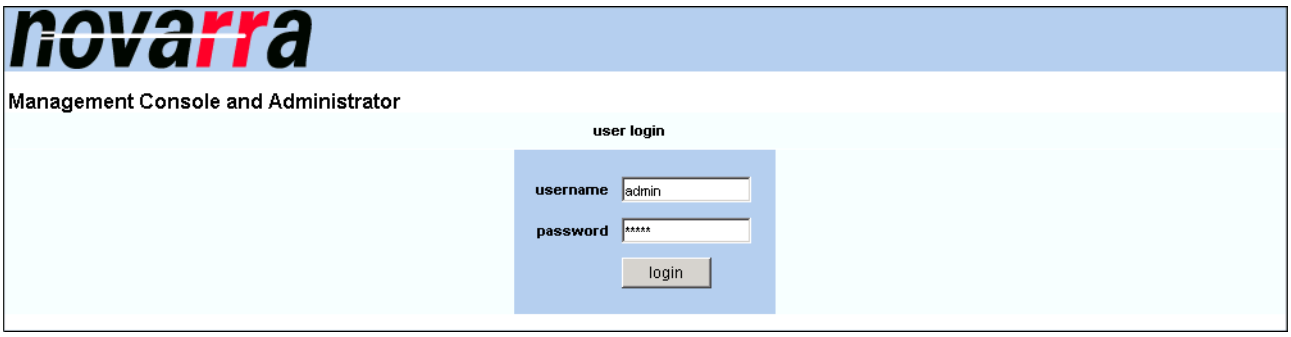
2. Check to see that the **Opstatus** of all the Services/Components are **UP**.

Novarra Management Console 3

The Novarra Management Console serves as an HTML tool that enables you to configure various aspects of Novarra WirelessWeb Enterprise suite.

3.1 Login

1. Navigate to and click the “Management Console Login” shortcut: Start→Programs→Novarra Management Console→Management Console Login



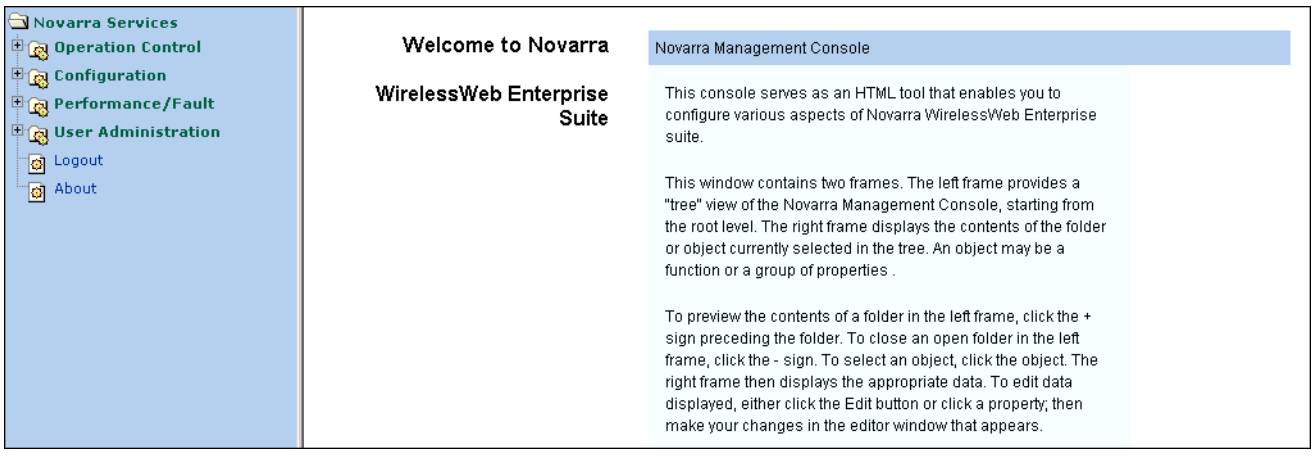
2. Enter the username and password and click the login button:

Note:

These are defaults when first installed and can be changed. See “Add/ Remove Users” on page 3-46.

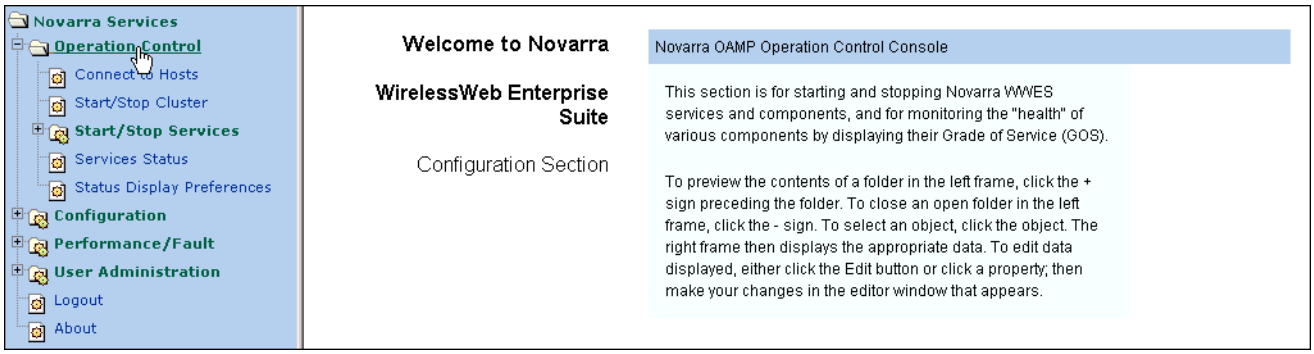
username: **admin**
password: **admin**

3. The WirelessWeb Enterprise Suite welcome page appears.



3.2 Operation Control

This section is for starting and stopping Novarra WWES services and components, and for monitoring the "health" of various components by displaying their Grade of Service (GoS). To access, click the **Operation Control** link in the navigation frame. The **Operation Control Section** welcome frame appears.

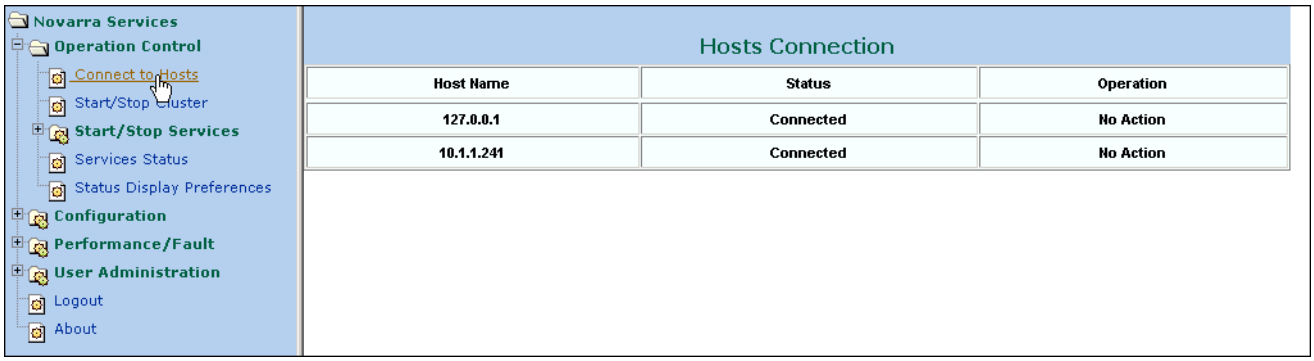


The following items are available in the **Operation Control** folder:

- "Connect to Hosts"
- "Start/Stop Cluster"
- "Start/Stop Services"
- "Services Status"
- "Status Display Preferences"

3.2.1 Connect to Hosts

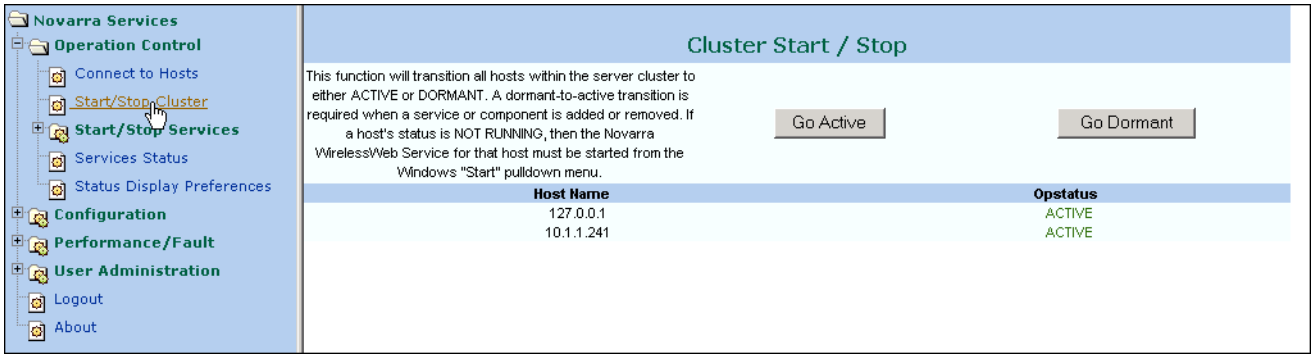
The **Hosts Connection** frame displays the host's status. If a host is not connected, a button is present to start that host.



3.2.2 Start/Stop Cluster

This function will start/stop all the services and the components in the whole cluster. This is required when a service or service/component is added/ removed.

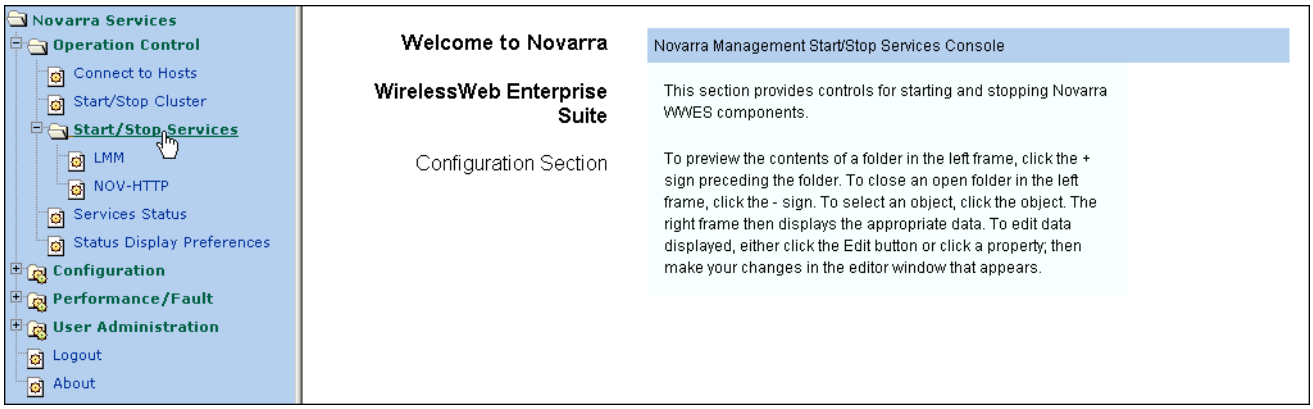
1. Click the **Start/Stop Cluster** link. The **Cluster Start/Stop** frame appears.



2. To stop the cluster, click the Go Dormant button. The **Opstatus** changes to **DORMANT**.
3. To start the cluster, click the Go Active button. The **Opstatus** changes to **ACTIVE**.

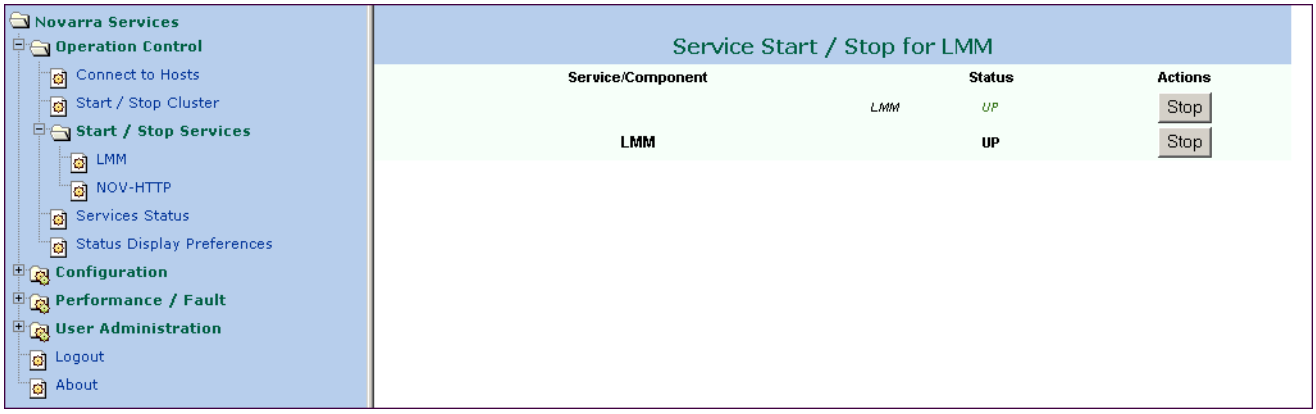
3.2.3 Start/Stop Services

This section provides controls for starting and stopping Novarra WirelessWeb Enterprise Suite components. To access, click the **Start/Stop Services** link in the navigation frame. The **Start/Stop Services Console** welcome frame appears.



3.2.3.1 Start/Stop LMM

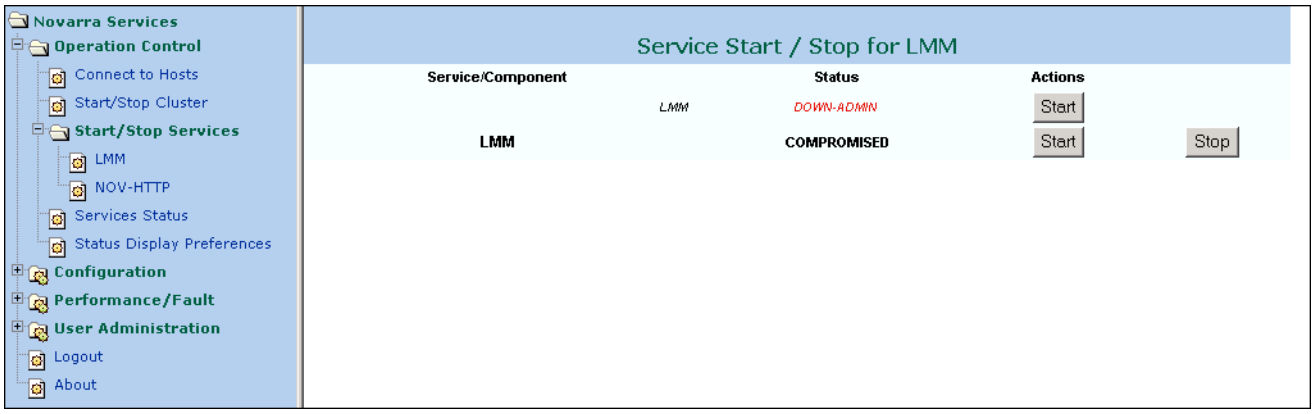
1. Click the **LMM** link. The **Service Start/Stop for LMM** frame appears.



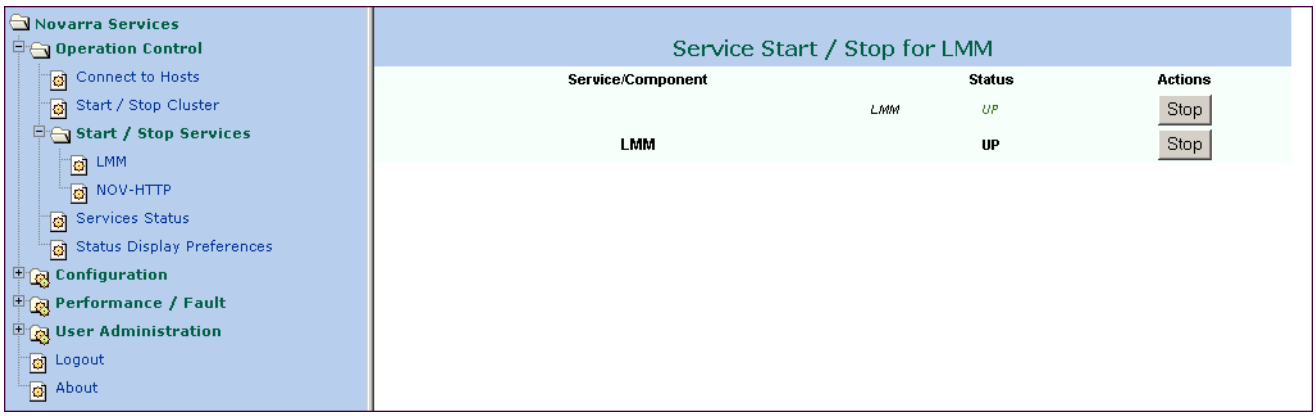
The two buttons that appear on this page are:

- Stop
- Start

2. To stop the LMM, click the Stop button. The Status for the component changes to **DOWN-ADMIN** and the Status for the service changes to **COMPROMISED**.



3. To start the LMM, click the Start button. The Status for the component changes to **UP** and the Status for the service changes to **UP**.



3.2.3.2 Start/Stop NOV-HTTP

1. Click the **NOV-HTTP** link. The **Service Start/Stop for NOV-HTTP** frame appears.

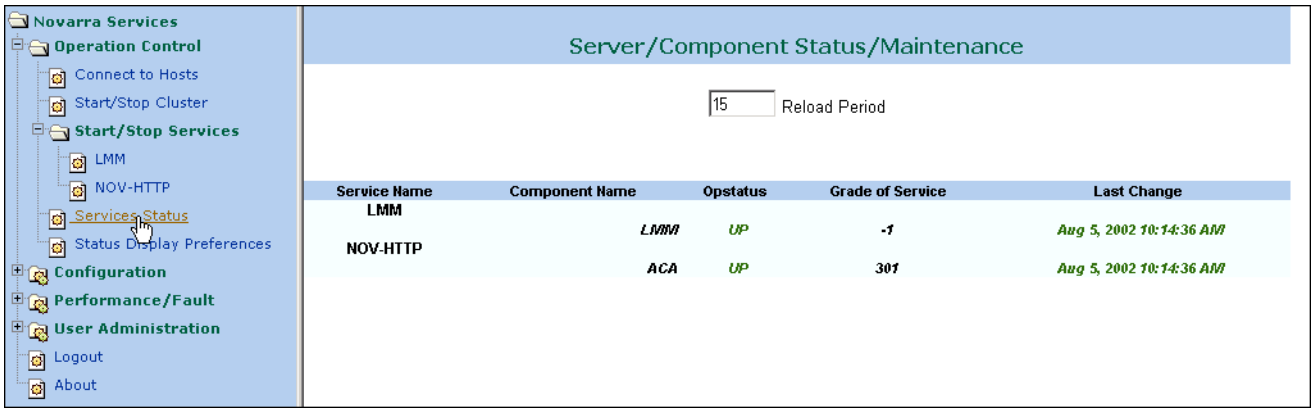
The two buttons that appear on this page are:

- Stop
- Start

2. To stop the NOV-HTTP, click the Stop button. The Status for the component changes to **DOWN-ADMIN** and the Status for the service changes to **COMPROMISED**.
3. To start the NOV-HTTP, click the Start button. The Status for the component changes to **UP** and the Status for the service changes to **UP**.

3.2.4 Services Status

1. Click the **Services Status** link. The **Server/Component Status/ Maintenance** frame appears.



2. The Reload Period can be changed by entering a new number of seconds (15 seconds is the minimum).

3. The Opstatus and Grade of Service of each Service/Component is shown.

   - **Opstatus** — The operational status. An Opstatus of **UP** indicates the Service/Component is running. An Opstatus of **DOWN-ADMIN** indicates the Service/Component was stopped by an administrator. An Opstatus of **DOWN-OP** indicates that there is a problem with that component.
   - **Grade of Service** — A numerical value of an attribute. When a mouseover is done on the number, a Tool Tip indicating what the attribute represents is displayed. The attribute's value is selectable (see section 3.2.5, "Status Display Preferences" on page 3-10.) It may be necessary to increase the Reload Period in order to view the Tool Tip.

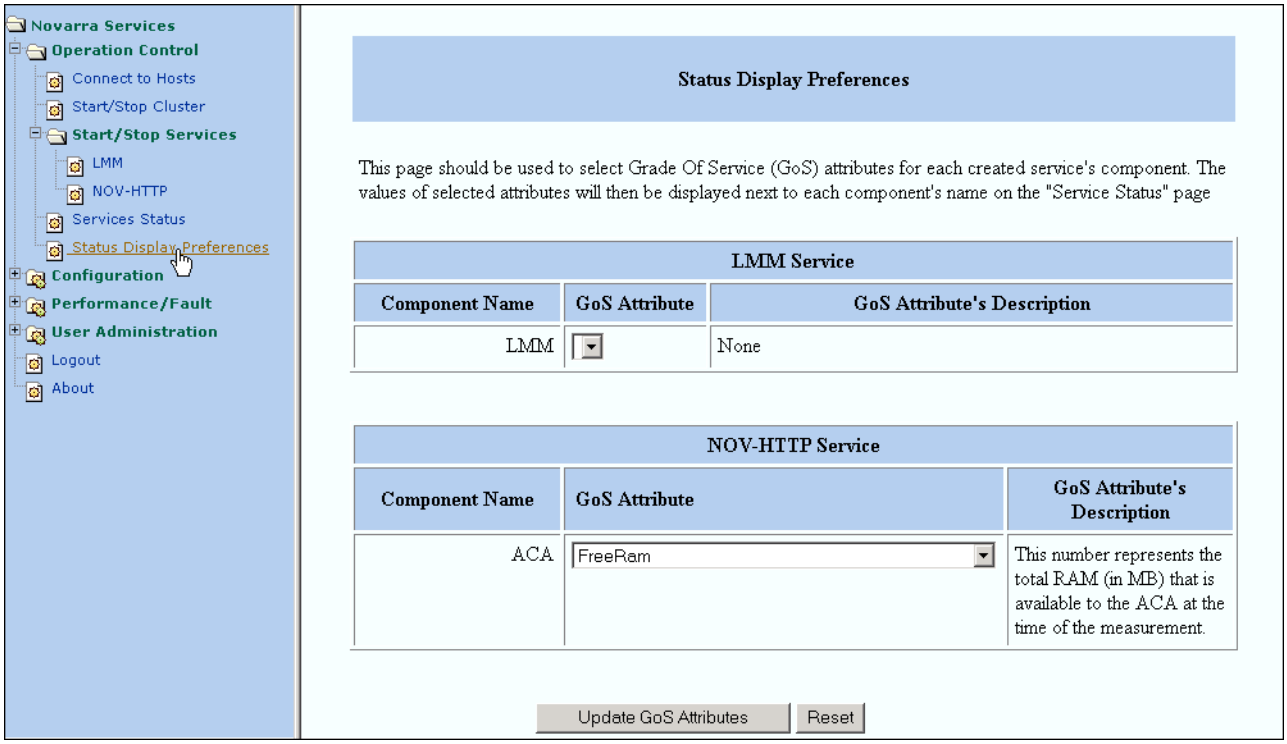
Note:

A "-1" in the Grade of Service column indicates that Grade of Service is not available for that Service/Component.

3.2.5 Status Display Preferences

This page is used to select Grade of Service (GoS) attributes for each created service's component. The values of selected attributes will then be displayed under the Grade of Service column in line with each component's name on the Services Status page (see section 3.2.4, "Services Status" on page 3-9.)

1. Click the **Status Display Pref** link. The **Status Display Preferences** frame appears.



2. Select a Grade of Service (GoS) attribute for each service/component on the dropdown menus. Once selected, a description of the attribute appears to the right. The default attribute for GoS is FreeRam.

Note:

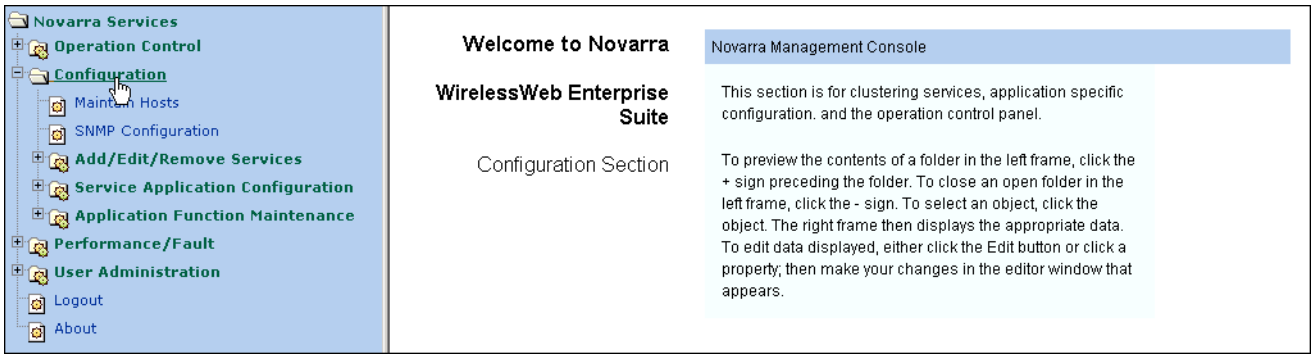
If no menu item appears in the dropdown, Grade of Service is not available for that service/component.

3. Click the Upgrade GoS Attributes button.

3.3 Configuration Folder

This section is for clustering services, application specific configuration and the operation control panel.

1. Click the **Configuration** folder link. The **Configuration Section** welcome screen appears in the right frame.



2. The following items are available in the **Configuration** folder:

   - "Maintain Hosts"
   - "SNMP Configuration"
   - "Add/Edit/Remove Services"
   - "Service Application Configuration"
   - "Application Function Maintenance"

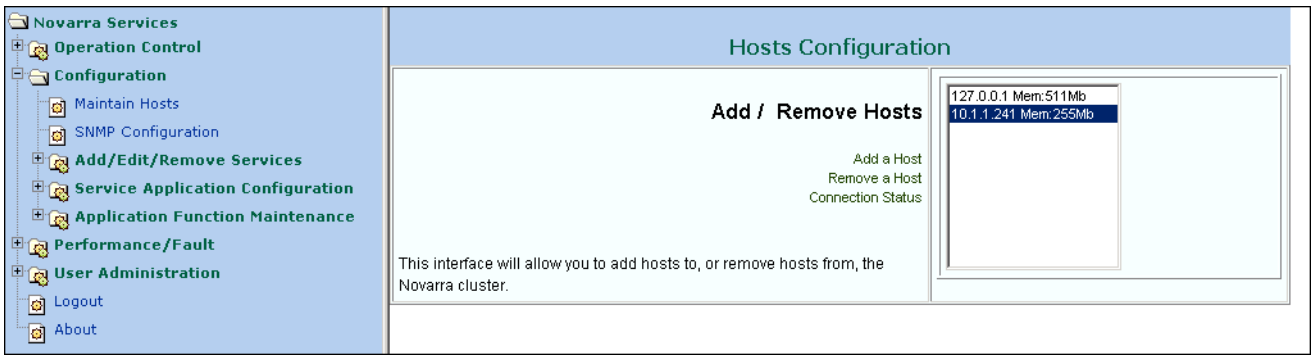
3.3.1 Maintain Hosts

This interface will allow you to add and remove hosts in the Novarra cluster. You can also check the connection status. To access, click the **Maintain Hosts** link in the navigation frame. The **Hosts Configuration** frame appears.

3.3.1.1 Add a host

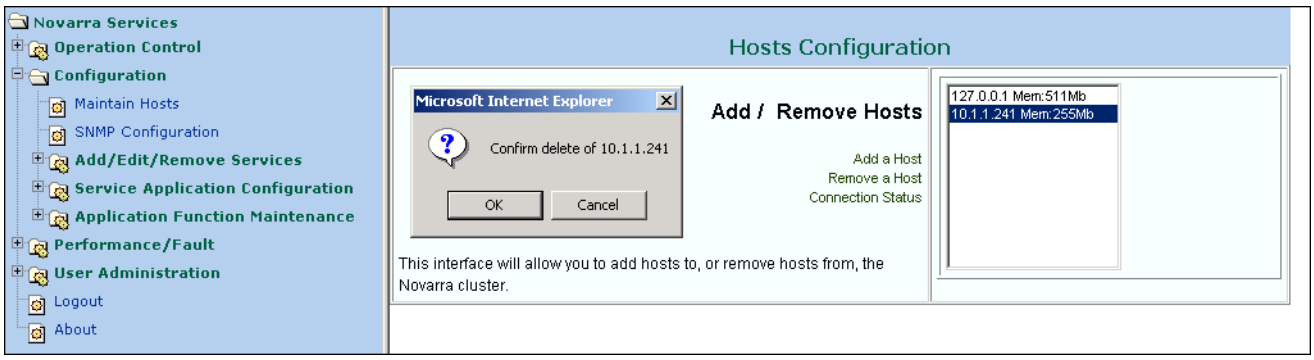
1. In the **Host Configuration** frame, click the **Add a host** link. The **Host Creation** frame appears.

2. Enter the new host's address and click the Add Host button. The **Host Configuration** frame appears with the new host displayed.



3.3.1.2 Remove a host

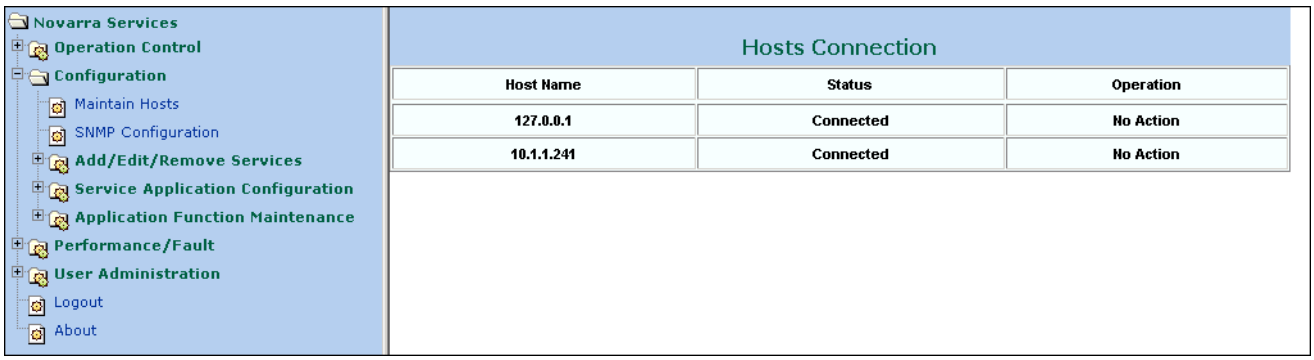
1. In the **Host Configuration** frame, click the host you want to remove. Click the **Remove a Host** link. An alert appears asking you to confirm deletion of the host.



2. Click OK. The **Host Configuration** frame no longer displays the removed host.

3.3.1.3 *Connection Status*

In the **Host Configuration** frame, click the **Connection Status** link. The **Host Configuration** frame displays the host's status.



3.3.2 SNMP Configuration

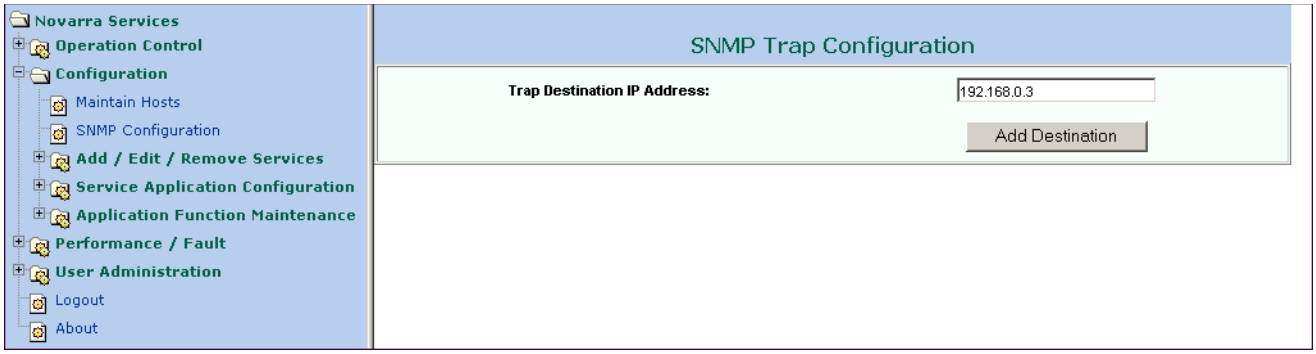
This interface allows you to change the SNMP configuration for a given Novarra server.

1. Click the **SNMP Configuration** link in the navigation frame. The **SNMP Trap Configuration** frame appears.

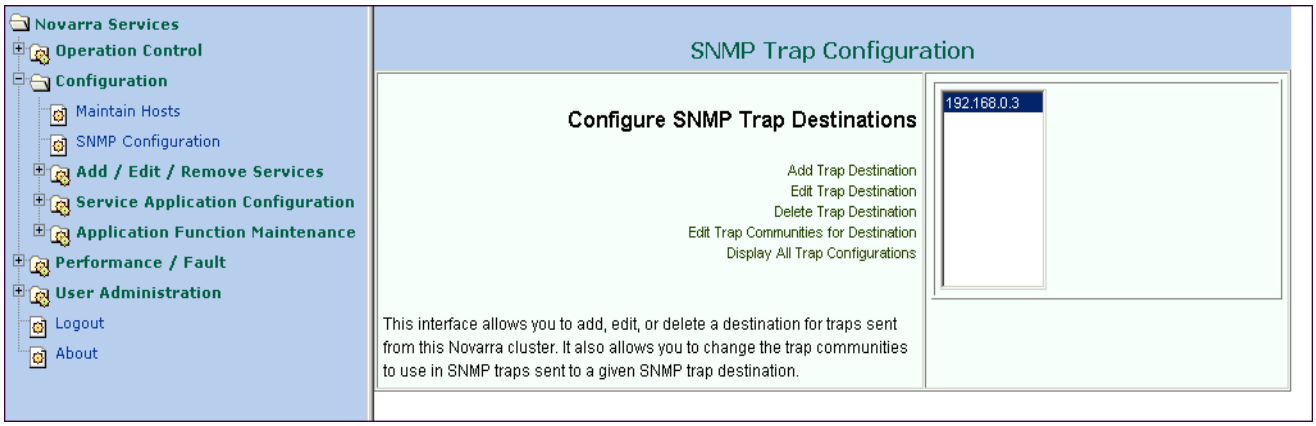
2. The following items are available in the **SNMP Trap Configuration** frame:
   - "Add Trap Destination"
   - "Edit Trap Destination"
   - "Delete Trap Destination"
   - "Edit Trap Communities for Destination"
   - "Display All Trap Configurations"

3.3.2.1 Add Trap Destination

1. In the **SNMP Trap Configuration** frame, click the **Add Trap Destination** link**.**
2. Enter in the **Trap Destination IP Address** and click the Add Destination button.



3. The **Trap Destination IP Address** now appears in the **SNMP Trap Configuration** frame.



3.3.2.2 Edit Trap Destination

1. In the **SNMP Trap Configuration** frame, select the Trap Destination you want to edit. Click the **Edit Trap Destination** link.
2. Change the IP address of the Trap Destination.

3.3.2.3 Delete Trap Destination

1. In the **SNMP Trap Configuration** frame, select the Trap Destination you want to remove. Click the **Delete Trap Destination** link.

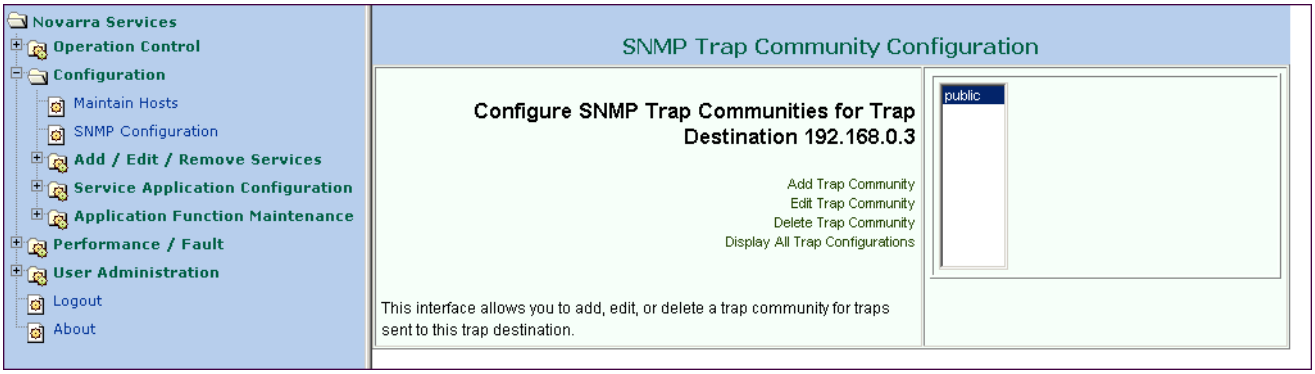
2. An alert appears asking you to confirm deletion of the Trap Destination. Click OK. The **SNMP Trap Configuration** frame no longer displays the removed Trap Destination.

3.3.2.4 Edit Trap Communities for Destination

This interface allows you to add, edit, or delete a trap community for traps sent to this trap destination from this Novarra host. It also allows you to commit SNMP Trap configuration changes to either the current Novarra host, or to all Novarra hosts

1. In the **SNMP Trap Configuration** frame, select a Destination.

2. Click the **Edit Trap Communities for Destination** link. The **SNMP Trap Community Configuration** frame appears.

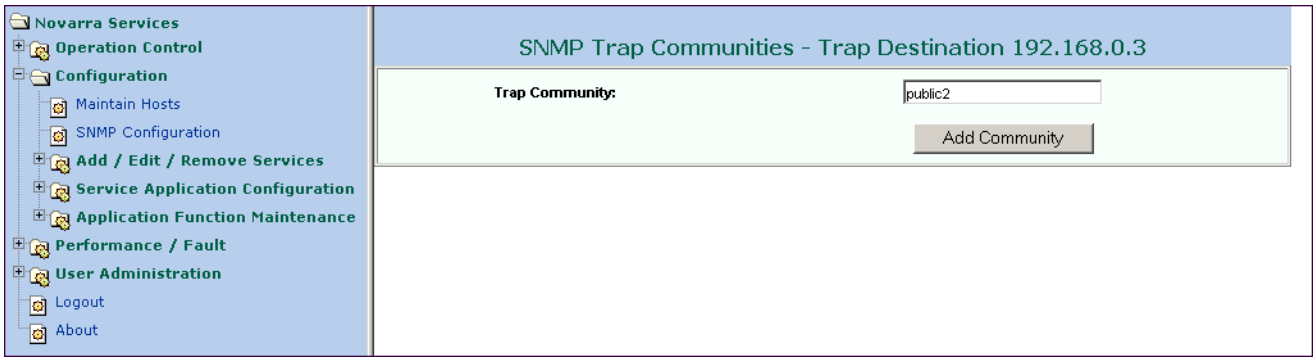


3. The following items are available in the **SNMP Trap Community Configuration** frame:

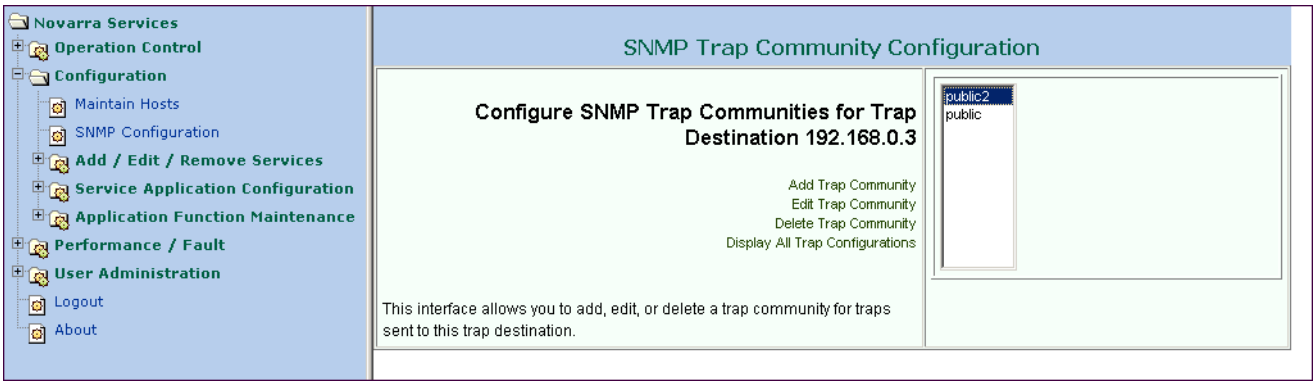
- "Add Trap Community"
- "Edit Trap Community"
- "Delete Trap Community"
- "Display all Trap Configurations"

3.3.2.4.1 Add Trap Community

1. In the **SNMP Trap Community Configuration** frame, click the **Add Trap Community** link.
2. Enter a **Community name**.



3. Click the Add Community button. The community now appears in the list for that Trap Destination.



3.3.2.4.2 Edit Trap Community

1. In the **SNMP Trap Community Configuration** frame, select the Trap Community you want to edit. Click the **Edit Trap Community** link.
2. Change the Trap Community name and click the Change Community button.

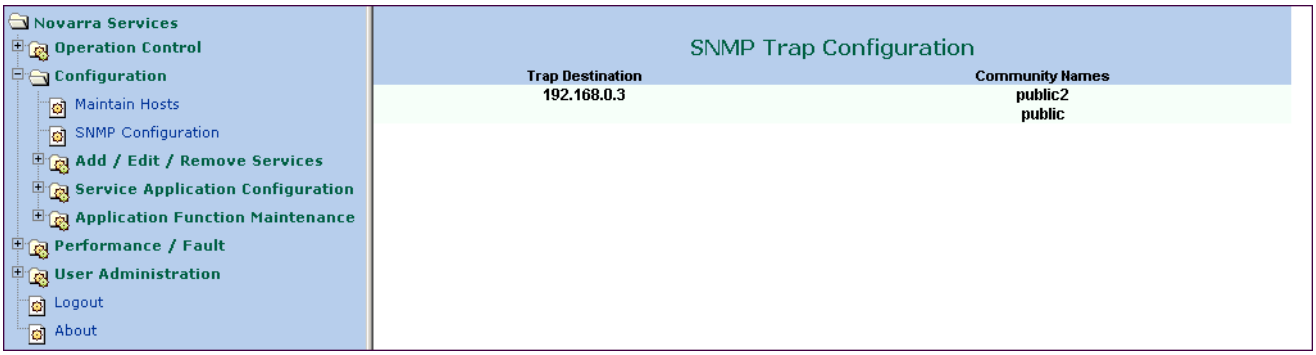
3.3.2.4.3 Delete Trap Community

1. In the **SNMP Trap Community Configuration** frame, select the Trap Community you want to remove. Click the **Delete Trap Community** link.
2. An alert appears asking you to confirm deletion of the Trap Destination. Click OK. The **SNMP Trap Configuration** frame no longer displays the removed Trap Community.

3.3.2.4.4 Display all Trap Configurations

1. In the **SNMP Trap Community Configuration** frame, click the **Display All Trap Configurations** link.

2. A display of all Trap Configuration parameters in the Novarra cluster appears.



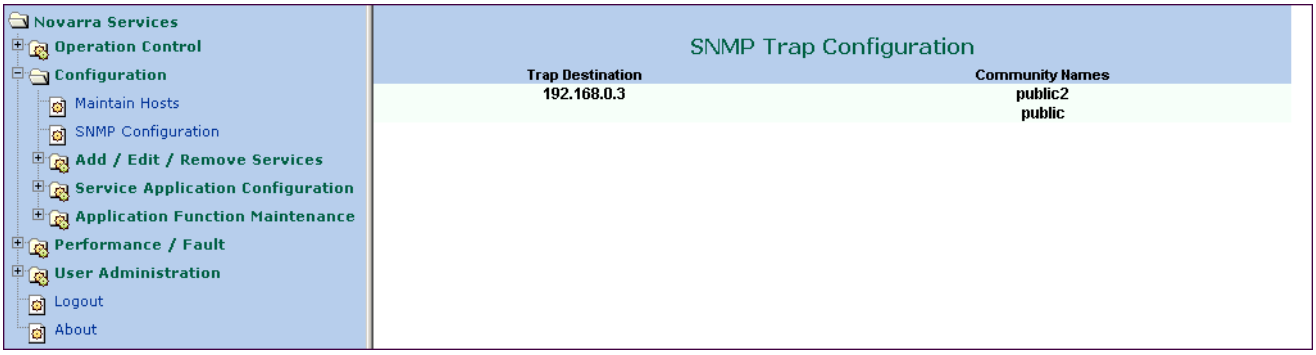
Note:

This is the same information as found when you click the **Display All Trap Configurations** link in the **SNMP Trap Configuration** frame (see below).

3.3.2.5 Display All Trap Configurations

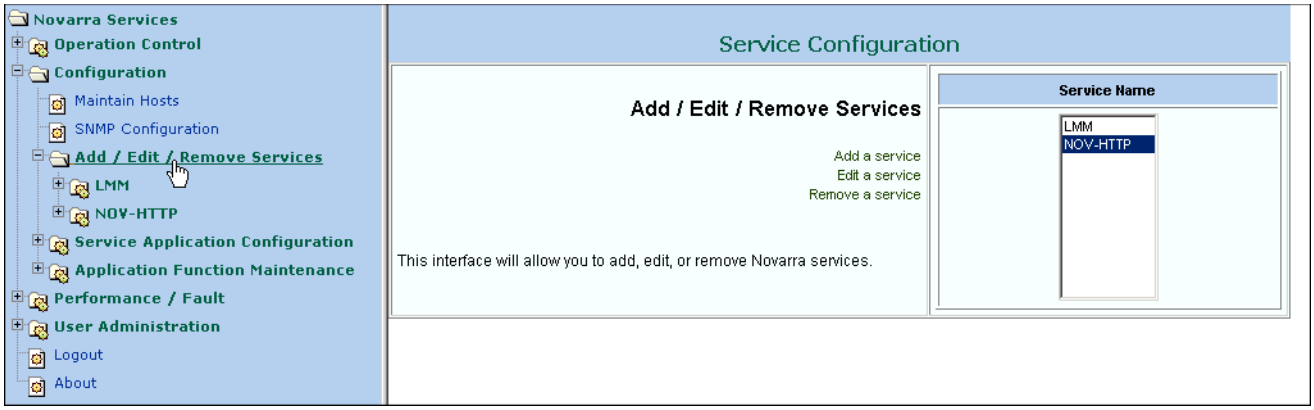
1. In the **SNMP Trap Configuration** frame, click the **Display All Trap Configurations** link.

2. A display of all Trap Configuration parameters in the Novarra cluster appears.



3.3.3 Add/Edit/Remove Services

This interface will allow you to add, edit and remove services. To access, click the **Add/Edit/Remove Services** link in the navigation frame. The **Service Configuration** frame appears.



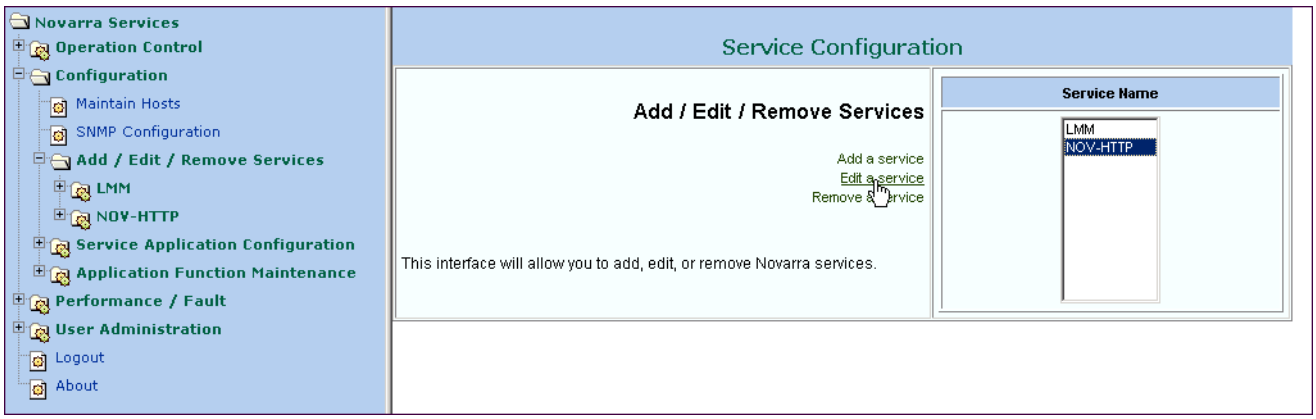
3.3.3.1 Add a service

Note:

Novarra recommends that service additions and deletions not be performed. Rather, new components be added to the existing Novarra service (example: NOV-HTTP) or existing components can be edited or removed. Components are added, edited or removed via the **Edit a service** link.

3.3.3.2 Edit a service

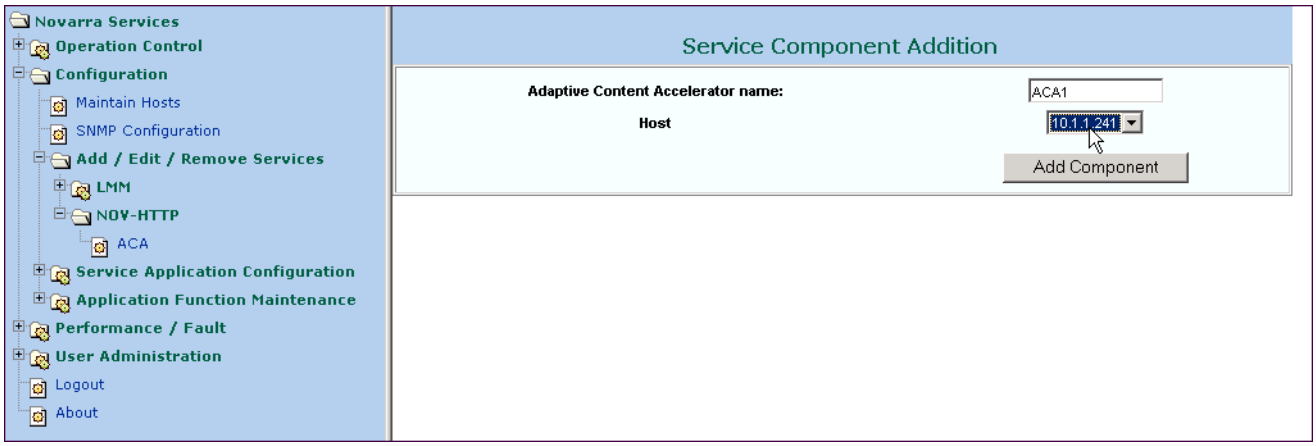
1. In the **Service Configuration** frame, click the Service Name you want to edit (example: NOV-HTTP).



2. In this **Service Configuration** frame, you can Add, Edit or Remove Components.

3.3.3.2.1 Add a component

1. Click the **Add a component** link. The **Service Component Add** frame appears.

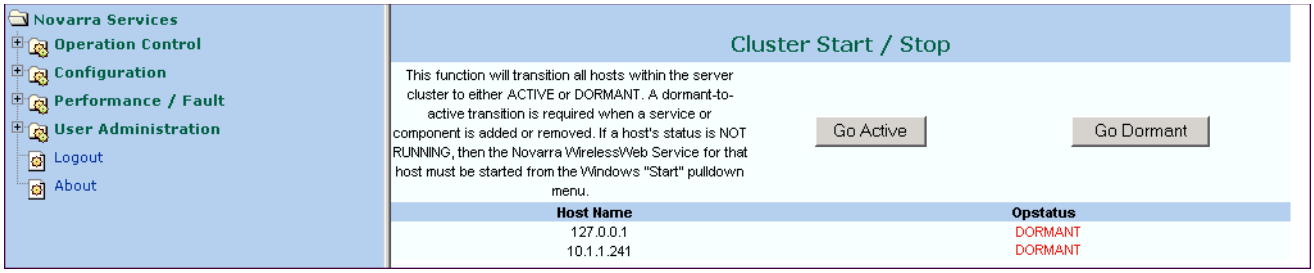


2. Enter a new name for the Adaptive Content Accelerator (ACA). Select a Host from the list.
3. Click the Add Component button. The **Cluster Start/Stop** frame appears.

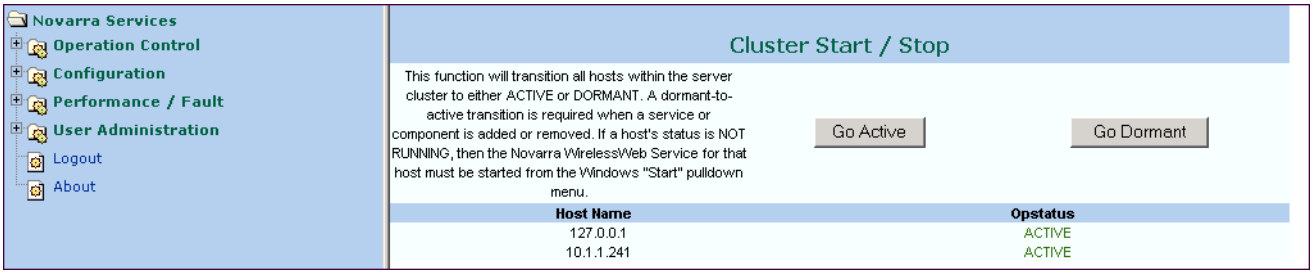
Note:

In order for the add to take effect, the cluster must be stopped and restarted.

4. Click the Stop button and wait for the Opstatus to change to **DORMANT**.

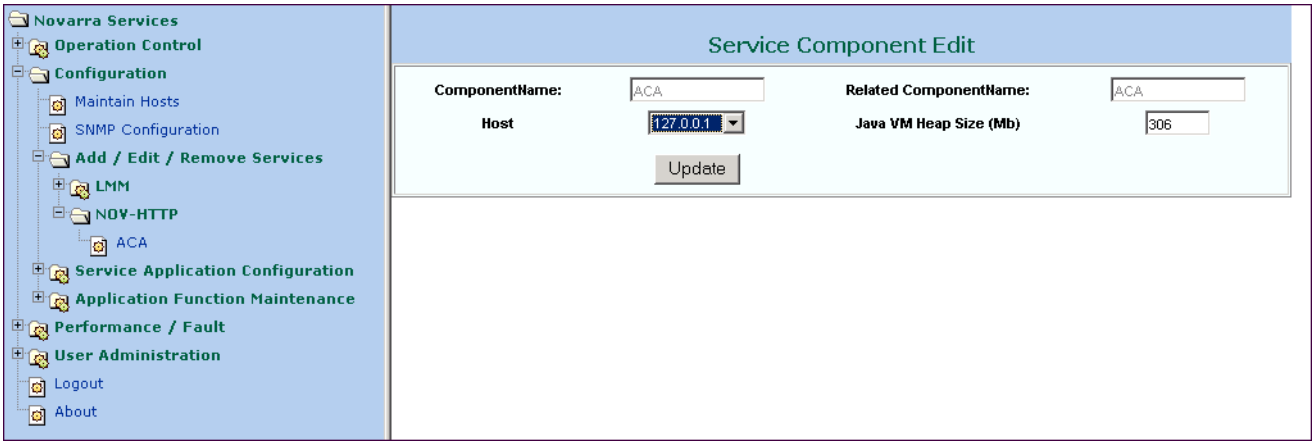


5. Click the Start button and wait for the Opstatus to change to **ACTIVE.**



3.3.3.2.2 Edit a Component

1. Click the **Edit a component** link. The **Service Component Edit** frame appears.

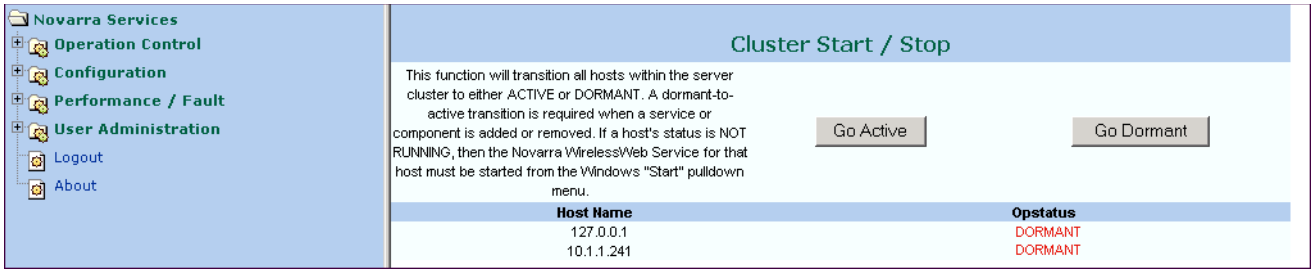


2. Edit the **Host** address and/or **Java VM Heap Size**.
3. Click the Update button. The **Cluster Start/Stop** frame appears.

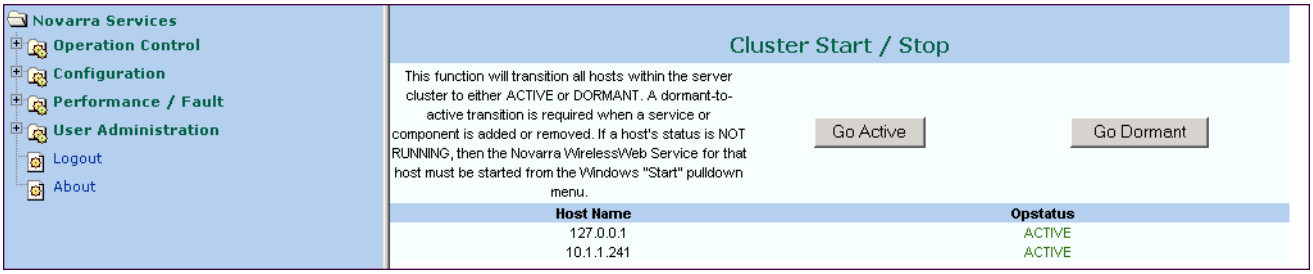
Note:

In order for the edit to take effect, the cluster must be stopped and restarted.

4. Click the Go Dormant button and wait for the Opstatus to change to **DORMANT**.

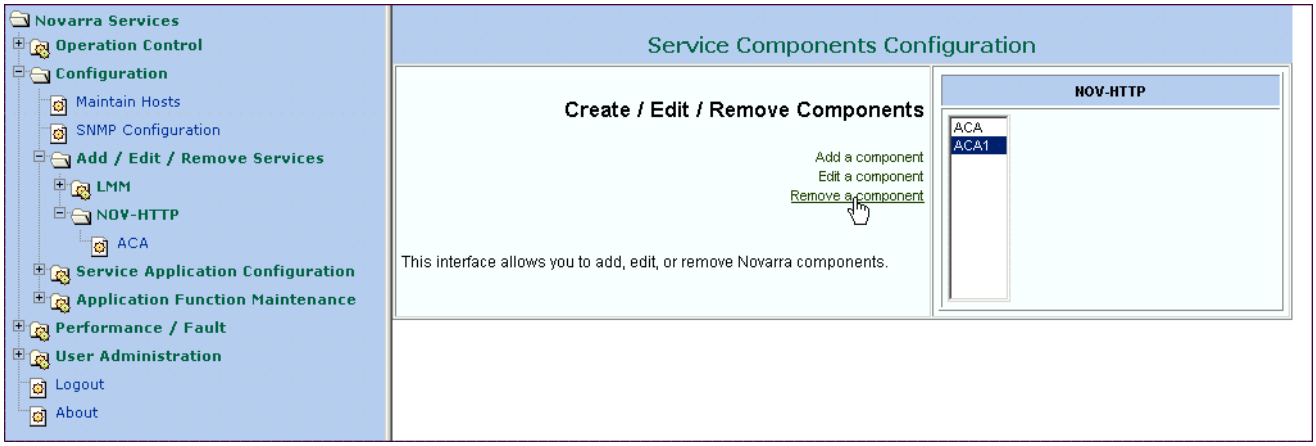


5. Click the Go Active button and wait for the Opstatus to change to **ACTIVE.**

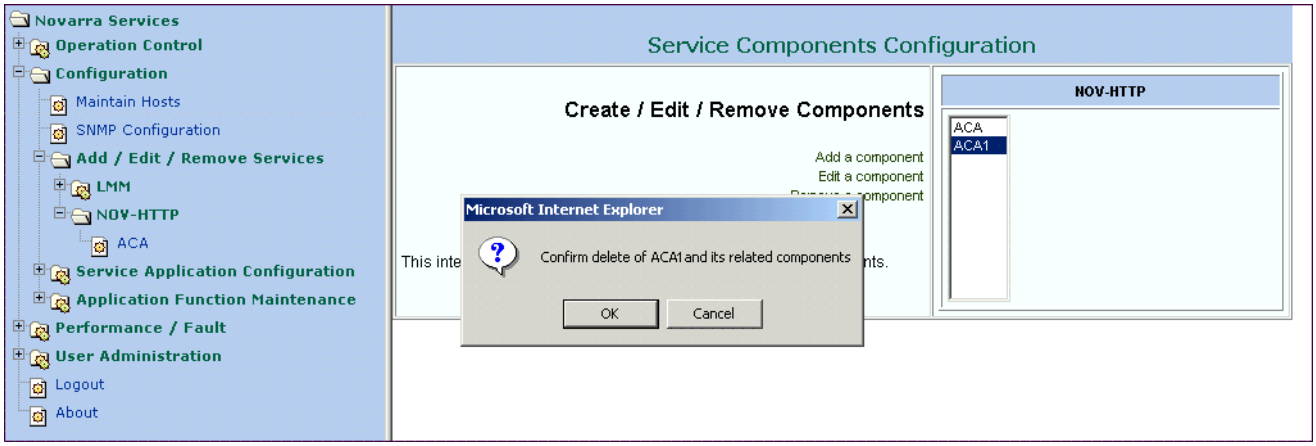


3.3.3.2.3 Remove a Component

1. In the **Service Configuration** frame, select the Component Name you want to remove (example: ACA1) and click the **Remove component** link.



2. An alert appears asking you to confirm deletion of the component.

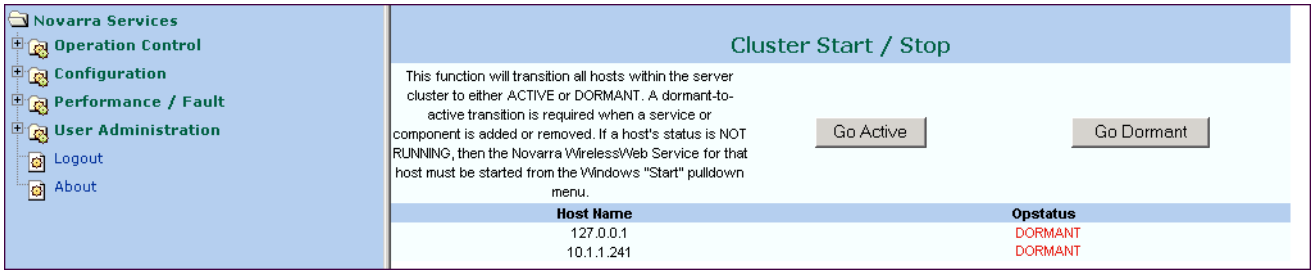


3. Click the OK button. The **Cluster Start/Stop** frame appears.

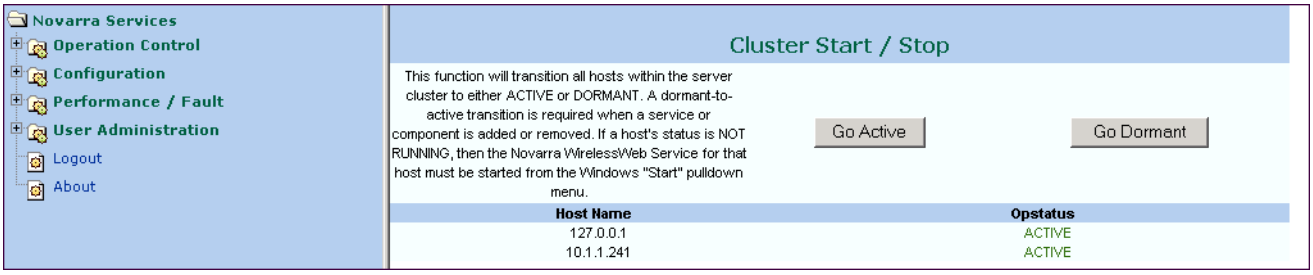
Note:

In order for the removal to take effect, the cluster must be stopped and restarted.

4. Click the Go Dormant button and wait for the Opstatus to change to **DORMANT**.



5. Click the Go Active button and wait for the Opstatus to change to **ACTIVE.**



3.3.3.3 Remove a service

Note:

Novarra recommends that service additions and deletions not be performed. Rather, new components be added to the existing Novarra service (example: NOV-HTTP) or existing components can be edited or removed. Components are added, edited or removed via the **Edit a service** link.

3.3.4 Service Application Configuration

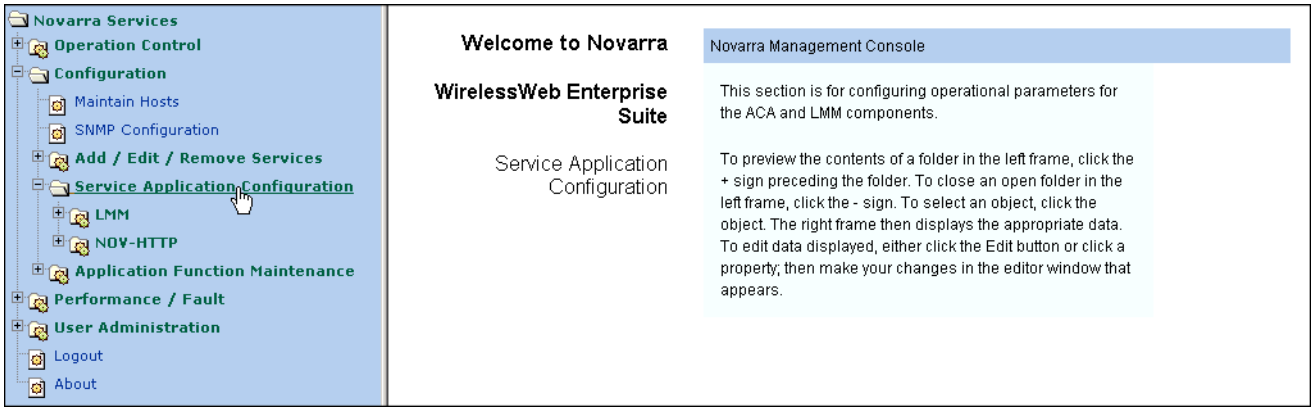
This section is for application specific configuration. Such as the configuration of the LMM, line handlers, device managers, ACAs, etc.

Note:

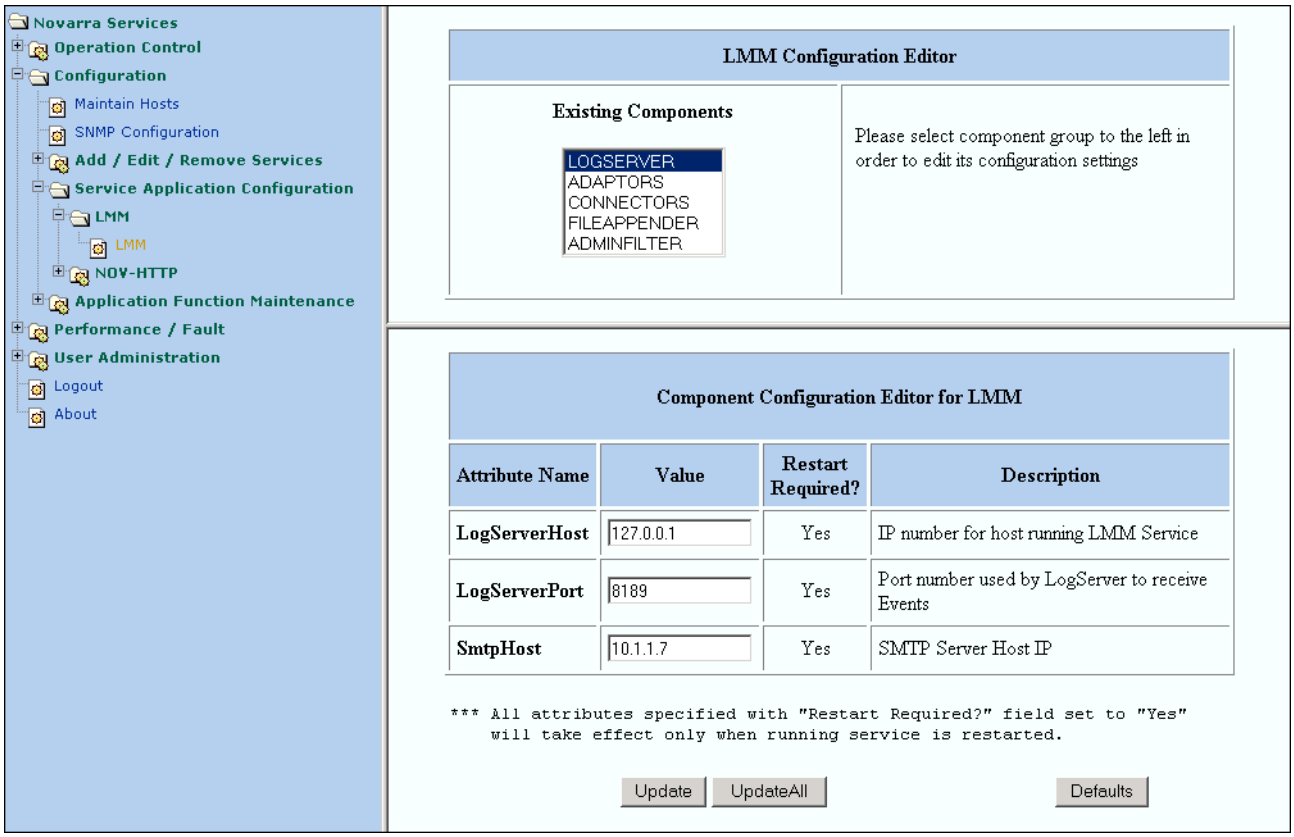
Services can be configured only when the entire cluster is **DORMANT** or when the entire cluster is **ACTIVE** and the service us up and running.

3.3.4.1 Configure Logging/Monitoring Module (LMM)

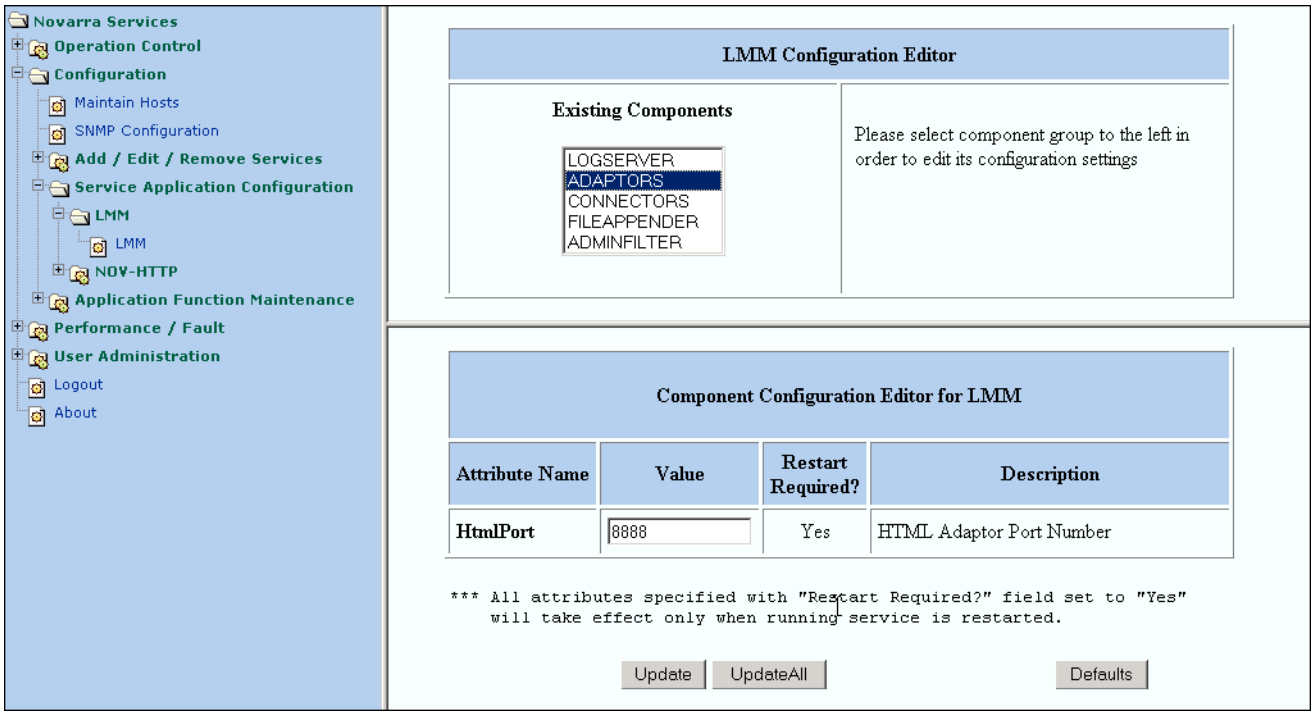
1. To access, click the **Service Application Configuration** link in the navigation frame. The **Application Configuration Section** welcome frame appears.



1. Click the **LMM** (folder) link and the **LMM** (document) link. The **LMM Configuration Editor** frame appears.



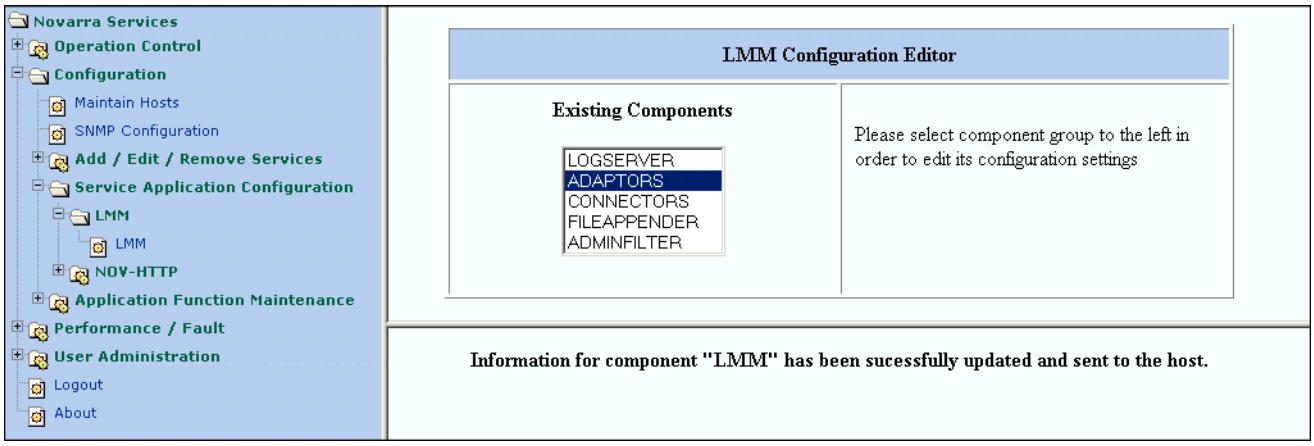
2. Select a component group by clicking on the component's name (Example: ADAPTORS). The **Component Configuration Editor for LMM** frame for that component appears.



The components that can be configured are:

Components	
LOGSERVERS	FILEAPPENDER
ADAPTORS	ADMINFILTER
CONNECTORS	

3. Edit the appropriate fields and click the Update button. The bottom frame displays “Information for component "LMM" has been successfully updated and sent to the host.”



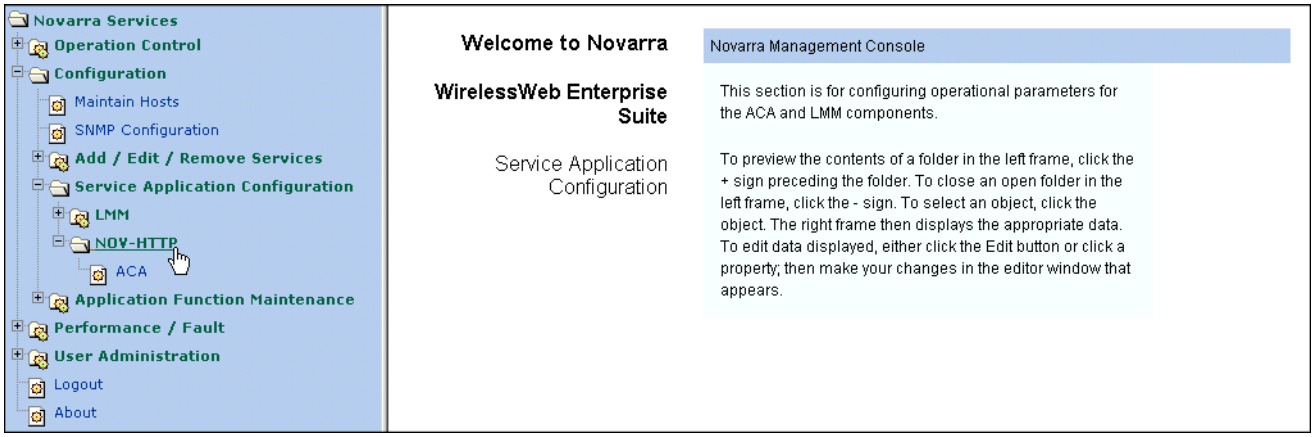
Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

4. Restart the service (see section 3.2.3.1, “Start/Stop LMM” on page 3-8.)

3.3.4.2 Configure NOV-HTTP

In the navigation frame, click **NOV-HTTP**. The navigation frame expands beneath the service application selected. The Adaptive Content Accelerator (ACA) link for that service appears.

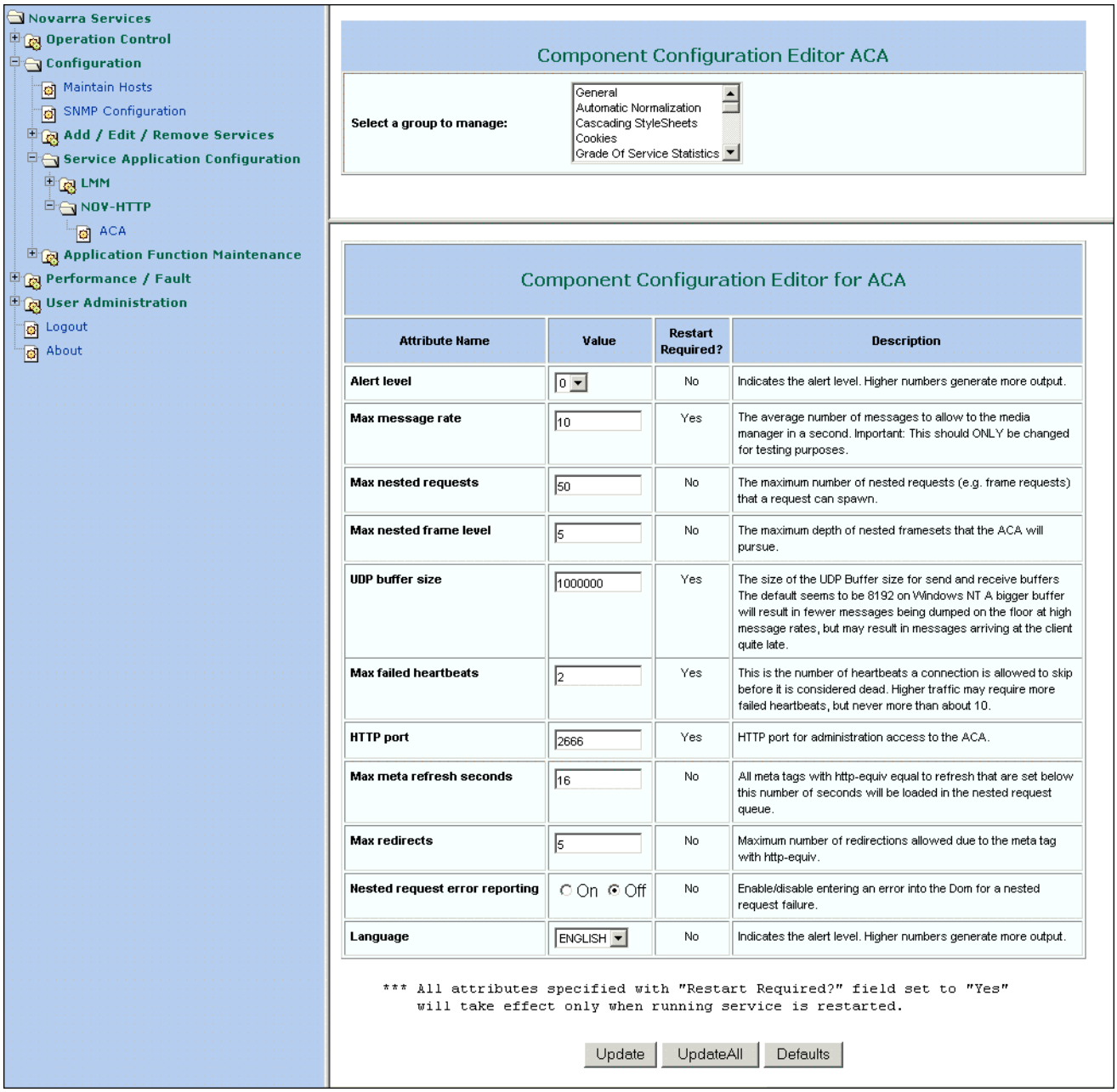


3.3.4.2.1 Configure Adaptive Content Accelerator

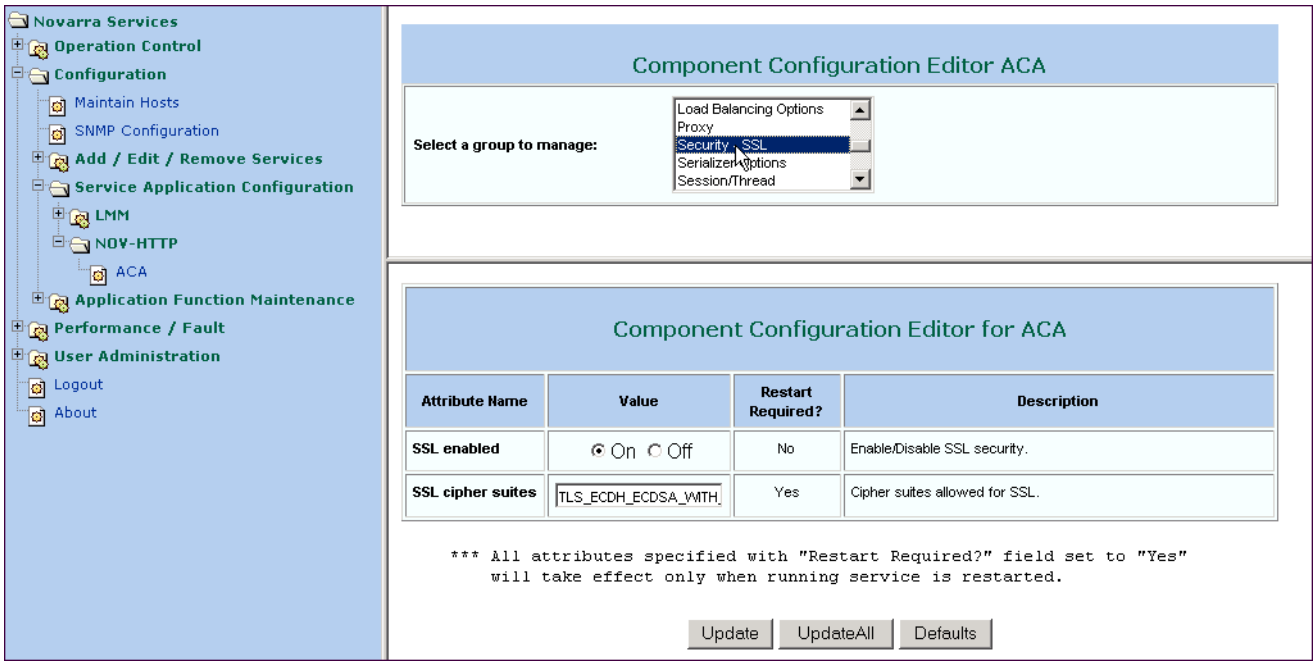
Note:

The Adaptive Content Accelerator is a shared component. Changes made in the ACA for one service will be reflected in all other services.

1. Click the **ACA** link. The **Component Configuration Editor for ACA** frame appears.



2. Select a group to manage by clicking on the group's name (Example: **Security - SSL**). The **Component Configuration Editor for ACA** frame for that group appears.



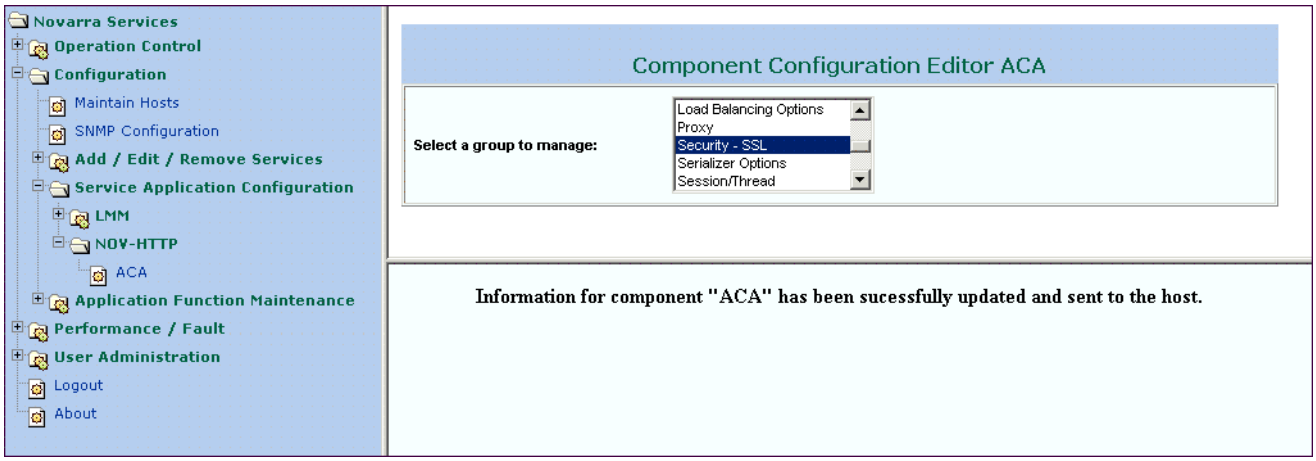
The groups that can be configured are:

Groups		
General	Http Wireless Connector	System
Automatic Normalization	Load Balancing Options	Templates
Cascading Style Sheets	Proxy	Trace
Cookies	Security-SSL	Trace Override
Grade of Service Statistics	Serializer Options	User Agent
Image Support	Session/Thread	WML
Javascript	Subscriber Authorization	

Note:

The Update All button is used for updating all components of this type throughout the Novarra cluster.

3. Edit the appropriate fields and click the Update button (or Update All button if appropriate). The bottom frame displays “Information for component "ACA" has been successfully updated and sent to the host.”



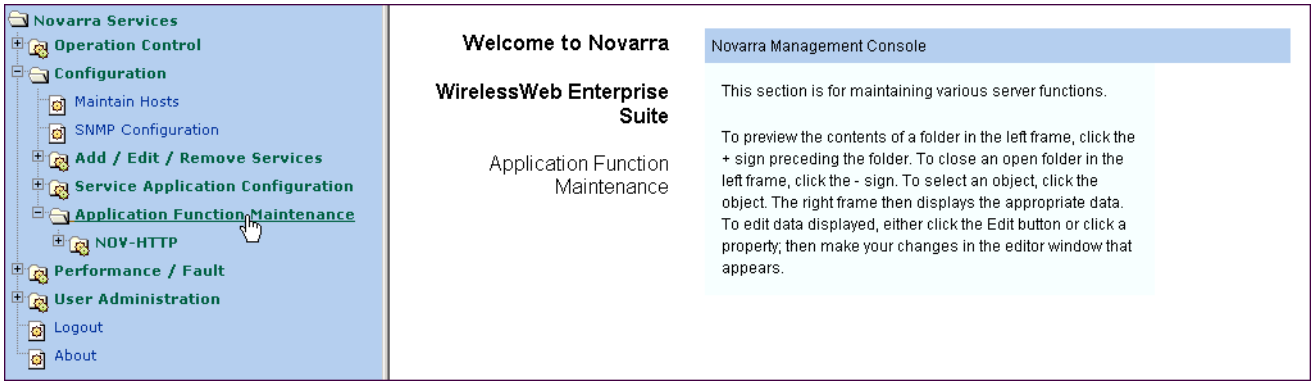
Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

4. Restart the service (see section 3.2.3.2, “Start/Stop NOV-HTTP” on page 3-9.)

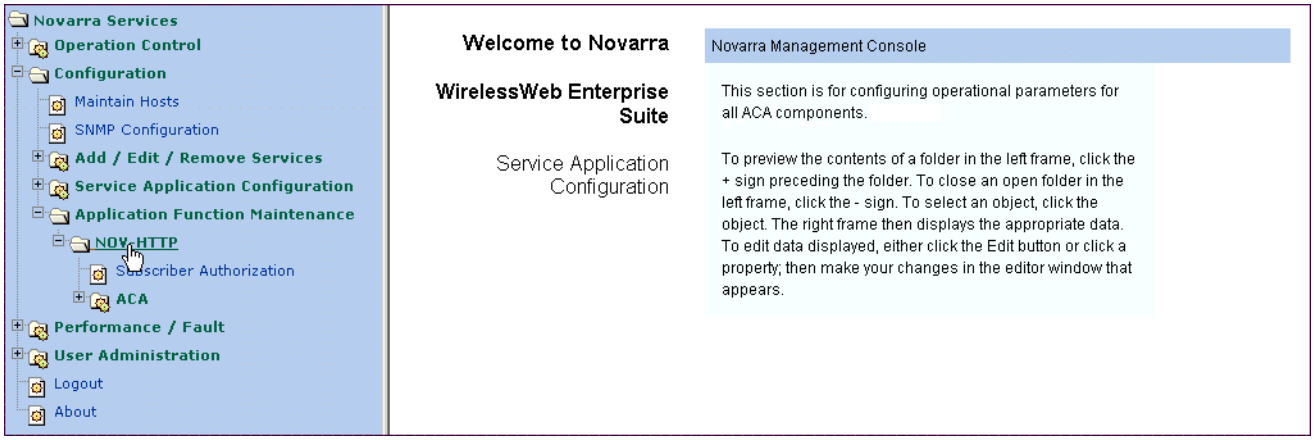
3.3.5 Application Function Maintenance

This section is for maintaining various server functions.



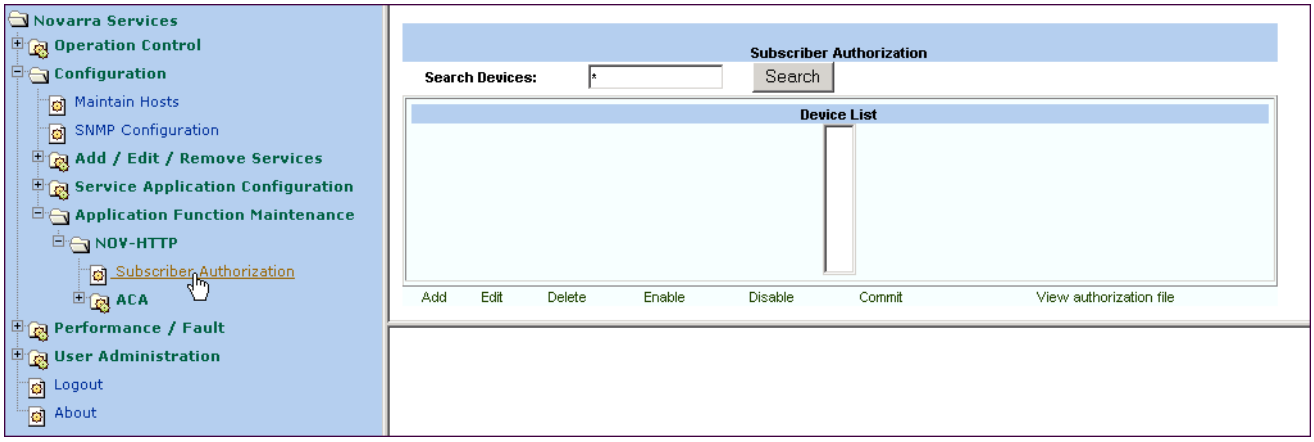
3.3.5.1 Maintenance on a Service Application

In the navigation frame, click the service application (example: **NOV-HTTP**). The navigation frame expands beneath the service application selected. Subscriber Authorization and Adaptive Content Accelerator (ACA) links for that service appear.



3.3.5.1.1 Subscriber Authorization

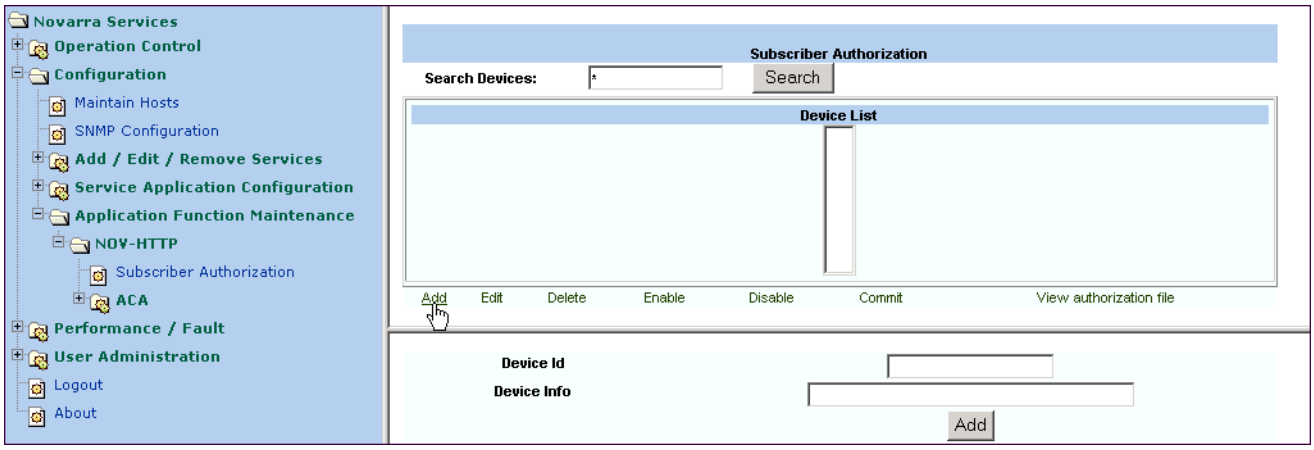
1. Click the **Subscriber Authorization** link. The **Subscriber Authorization** frame appears.



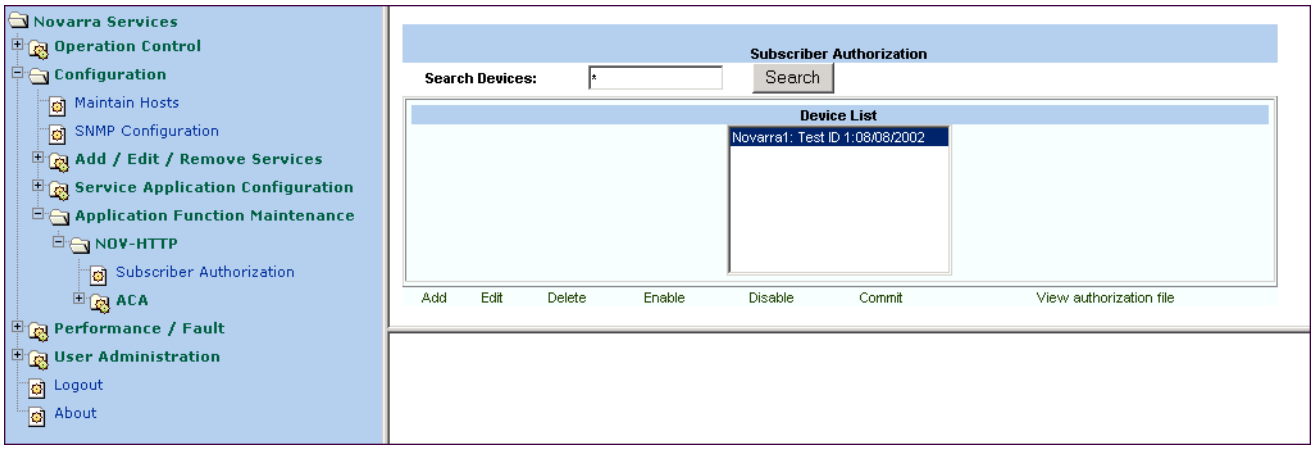
2. To search for a device, enter the device name (or a wildcard * for all devices) and click the Search button.

3.3.5.1.1.1 Add a Device

1. Click the **Add** link.The frame beneath **Subscriber Authorization** now has Device ID and Device Info editable fields.

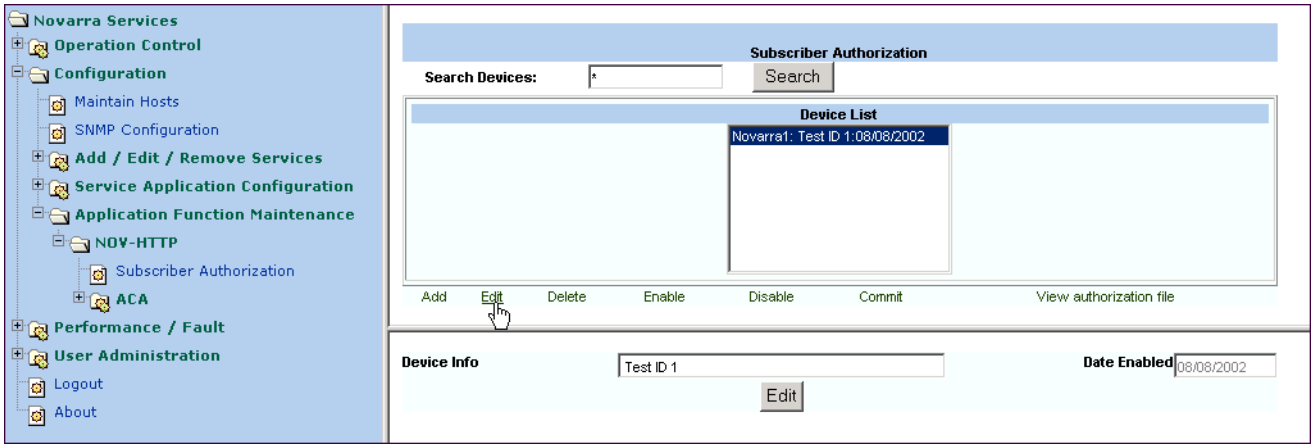


2. Enter the appropriate information and click the Add button. The device now appears in the Device List.



3.3.5.1.1.2 Edit a Device

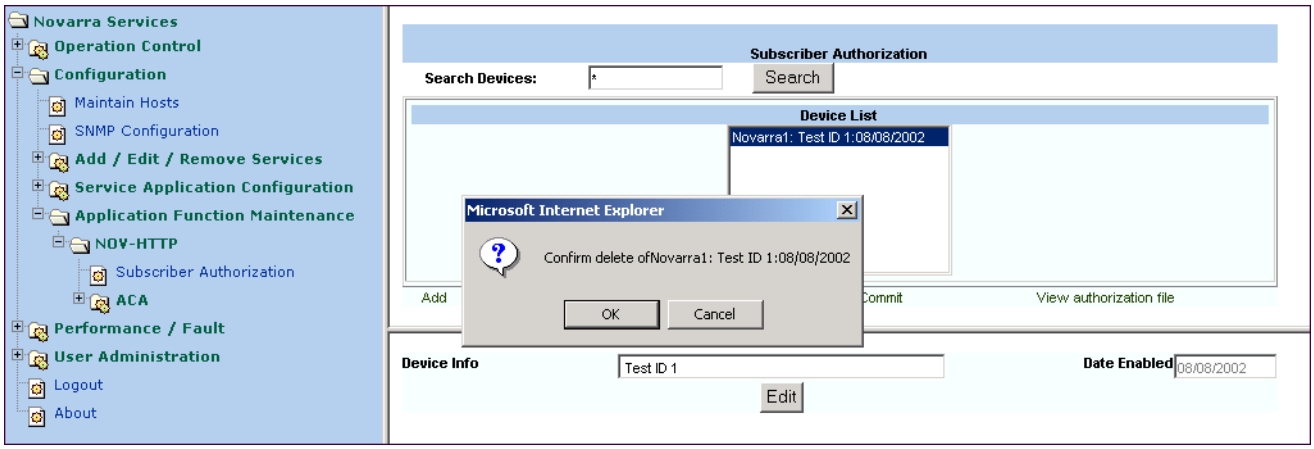
1. Click the device in the Device List that you want to edit. Click the **Edit** link in the **Subscriber Authorization** frame. The frame beneath **Subscriber Authorization** now has a **Device Info** editable field.



2. Make your changes and click the Edit button.

3.3.5.1.1.3 Delete a Device

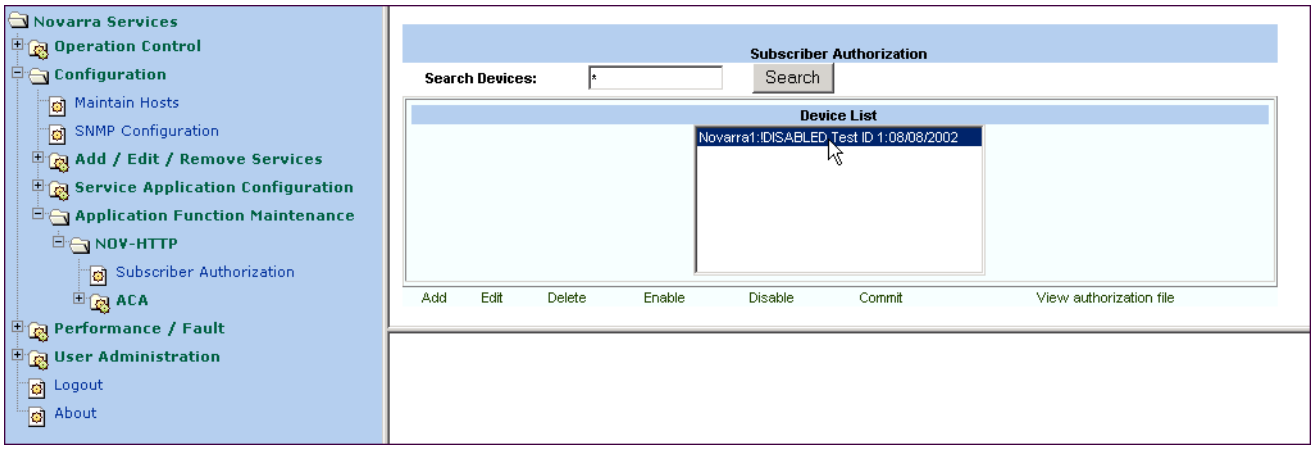
1. Click the device in the Device List that you want to delete. Click the **Delete** link in the **Subscriber Authorization** frame. An alert box appears confirming the deletion of the selected device.



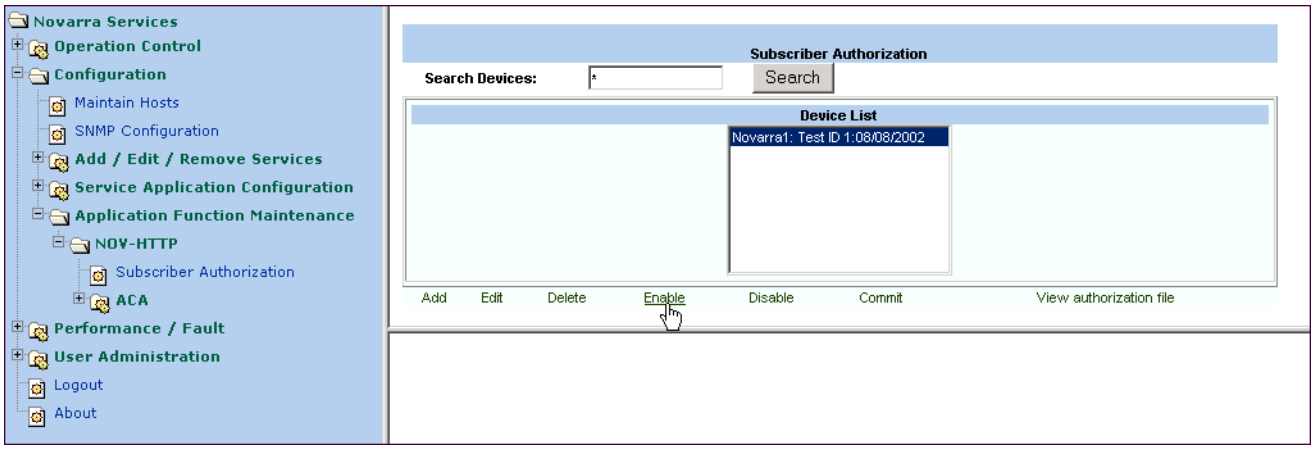
2. Click the OK button. The device no longer appears in the Device List.

3.3.5.1.1.4 Enable

1. Click the device in the Device List that is currently disabled (the word DISABLED appears in the name on the Device List).

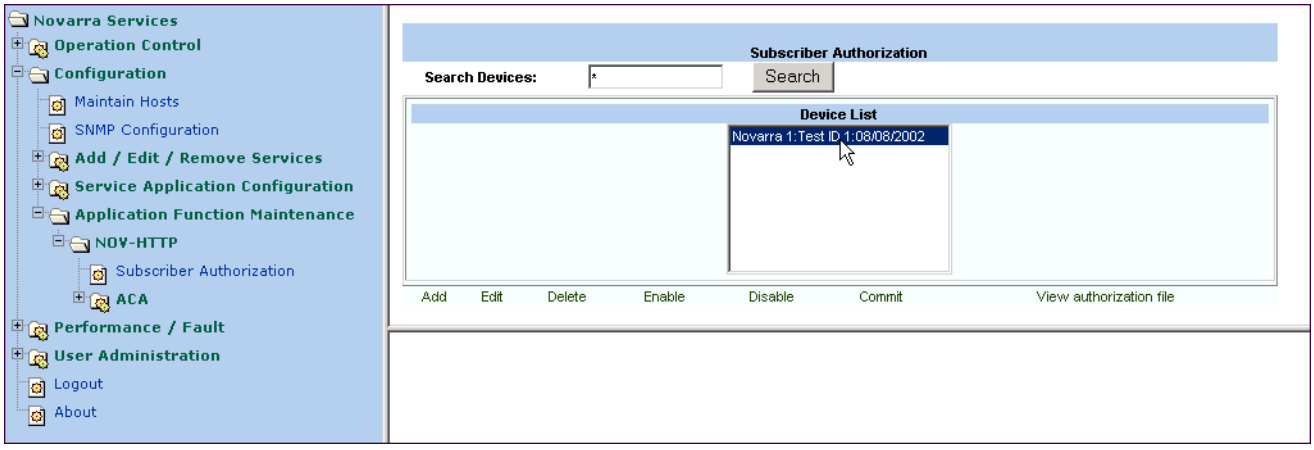


2. Click the **Enable** link. The device is now enabled.

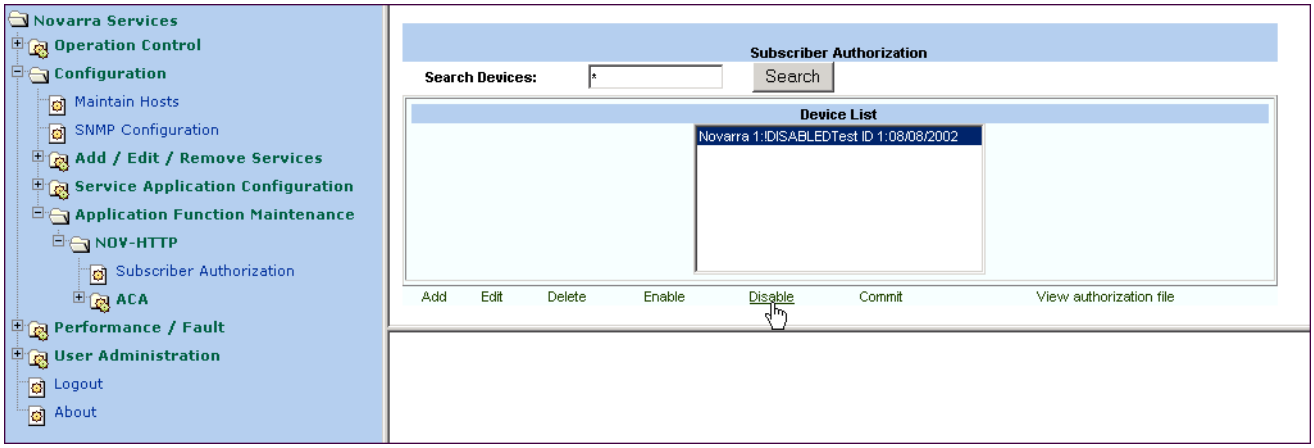


3.3.5.1.1.5 Disable

1. Click a device in the Device List that is currently enabled (the word DISABLED does not appear in the name on the Device List).

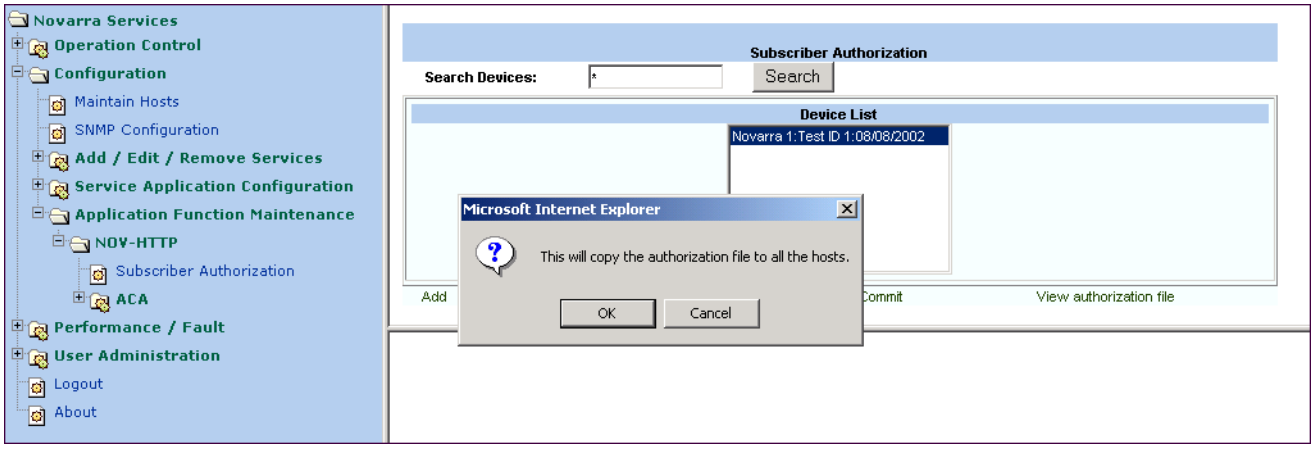


2. Click the **Disable** link. The device is now disabled (the word DISABLED appears within the name on the Device List).



3.3.5.1.1.6 Commit

Click the **Commit** link. An alert appears confirming the authorization file will be copied to all hosts. Click the OK button.



3.3.5.1.1.7 View Authorization File

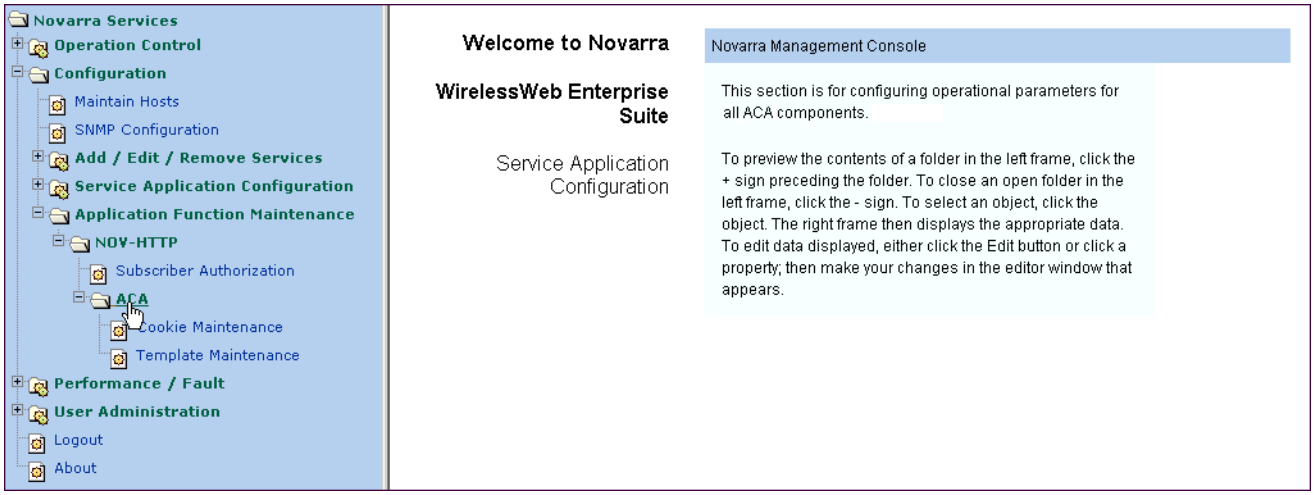
1. Click the **View Authorization File** link. A window opens with the Authorization file.

```
Novarra 1:Test ID 1:08/08/2002
#Novarra1: Test ID 1:08/08/2002
```

2. To close the window, click on the **X** in the upper right-hand corner of the window.

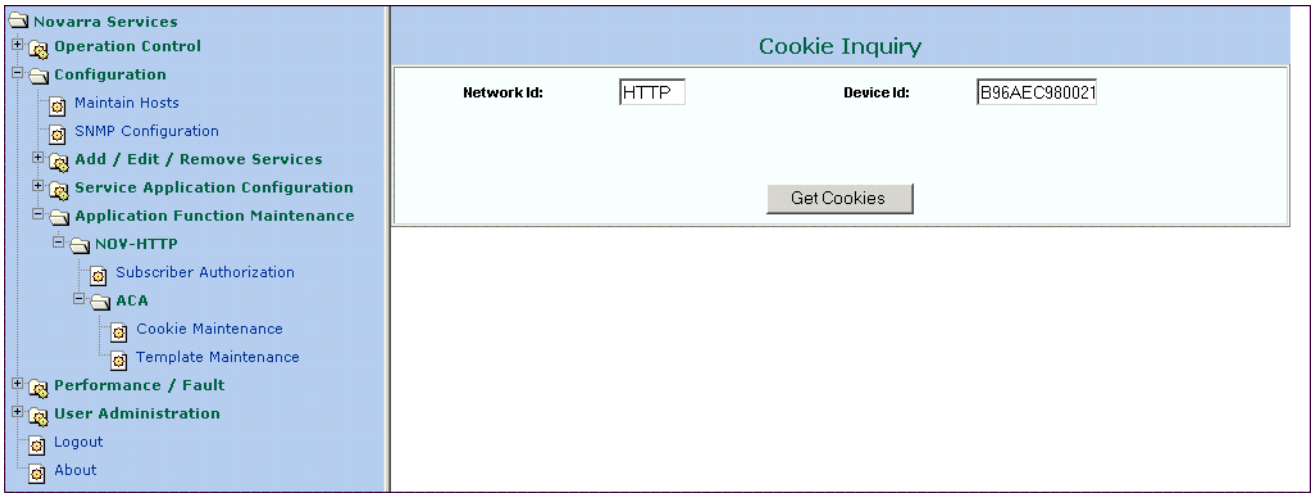
3.3.5.1.2 ACA Maintenance

Click the + next to the ACA folder or click the ACA link. The navigation frame expands beneath ACA. The Cookie Maintenance and Templates Maintenance links appear.



3.3.5.1.2.1 Cookie Maintenance

1. Click the **Cookie Maintenance** link. The **Cookie Inquiry** frame appears.



2. Enter HTTP in the **Network ID**.
3. Enter the **Device ID**.

Note:

Do not use the Device ID in the example. To determine the Device ID, see section 4.2.1, "Determining the Device ID" on page 4-3.

4. Click the Get Cookies button. The **Cookie Maintenance for Device** frame appears

5. Click the **Delete?** checkbox for the cookies you want to delete.

Note:

Once a cookie is deleted, it cannot be recovered.

6. Click the Update Cookies button.
7. Those cookies are now deleted from the cache.

3.3.5.1.2.2 Template Maintenance

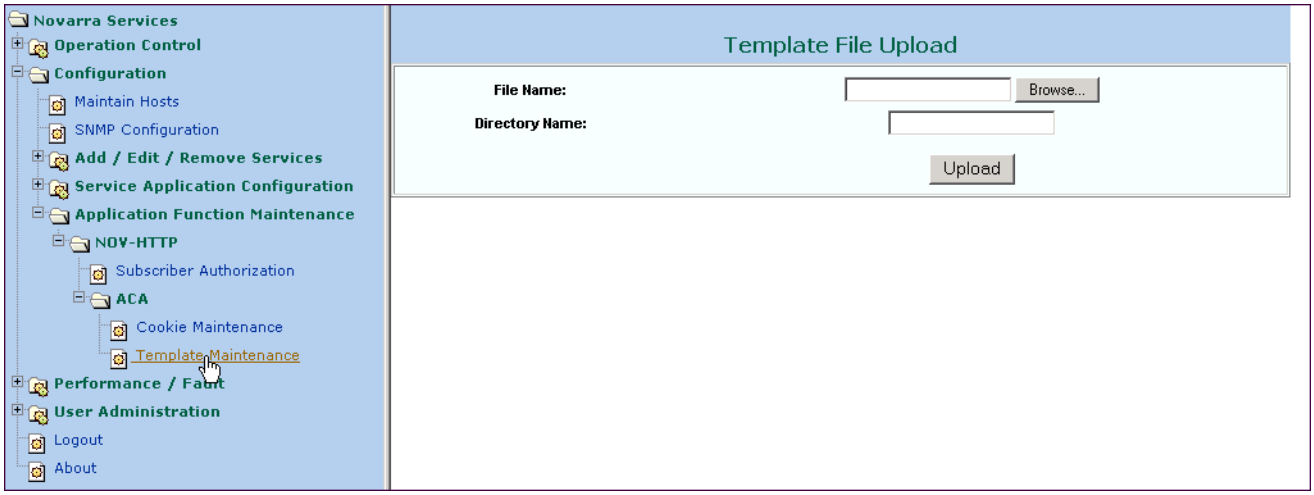
The template maintenance function provides a simple file upload facility for uploading template files to the WirelessWeb Server. The file specified in the "FileName" field will be copied from the filesystem of the administrator and placed into the filesystem of the WirelessWeb Server in the directory specified in the "DirectoryName" field (relative to <WirelessWebLocation>\config.

Note:

This is not a very useful function if the filesystem containing the templates is the same as (or is on the same networked file system as) the filesystem for the WirelessWeb Server.

For more information on Templates, see the WirelessWeb Enterprise Suite Developer's Guide.

1. Click the **Template Maintenance** link. The **Template File Upload** frame appears.

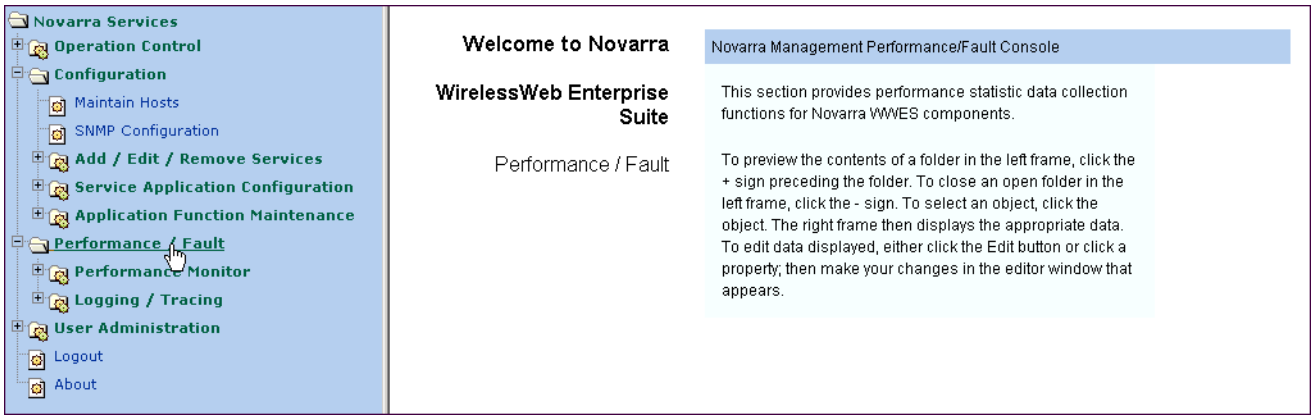


2. Enter the **File Name** and **Directory Name** and click the Upload button.

3.4 Performance/Fault Folder

This section provides statistics data collection functions for Novarra WirelssWeb Enterprise Suite components.

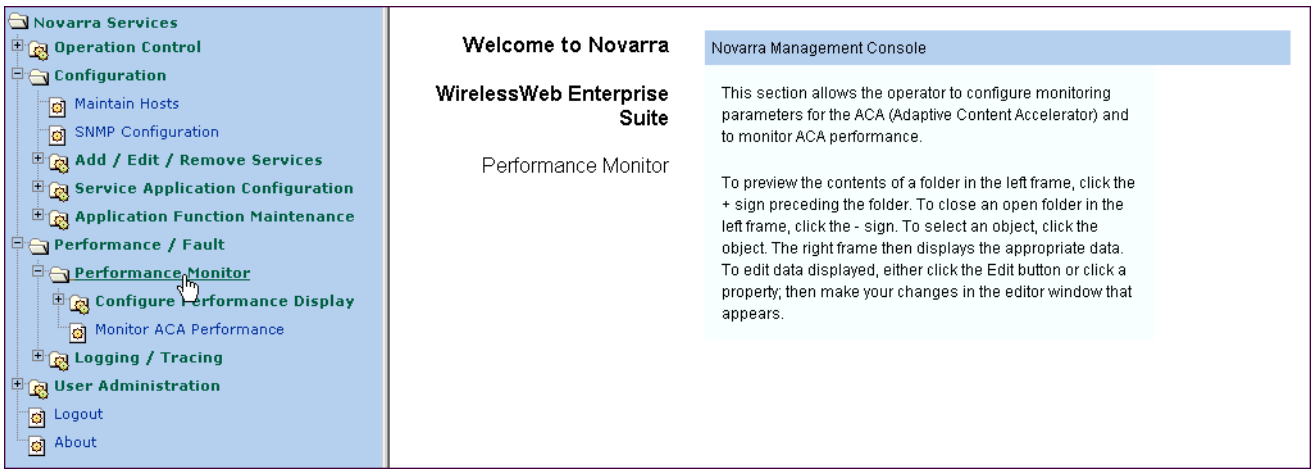
1. To access, click the **Performance/Fault** link in the navigation frame. The **Performance/Fault Section** welcome frame appears.



2. The following item is available in the **Performance/Fault** folder:
   - "Performance Monitor"
   - "Logging/Tracing"

3.4.1 Performance Monitor

This section allows the operator to configure monitoring parameters for the ACA (Adaptive Content Accelerator) and to monitor ACA performance. To access, click the **Performance Monitor** link in the navigation frame. The **Configure Performance Display** welcome frame appears.



The following items are available in the **Performance Monitor** folder:

- "Configure Performance Display"
- "Monitor ACA Performance"

3.4.1.1 Configure Performance Display

This section allows the operator to configure monitoring parameters for the ACA.

1. Navigate to the **Status Display Preferences** frame for the service you want to configure. (Example: HTTP):
   Performance/Fault→Performance Monitor→Configure Performance Display→NOV- HTTP→ACA
2. Select the Grade Of Service (GoS) attributes for each created service's component by clicking the appropriate Yes/No radio button.
3. Click the Update button.
4. The **ACA Performance Monitor** frame appears with a table containing the GoS attributes and their values.

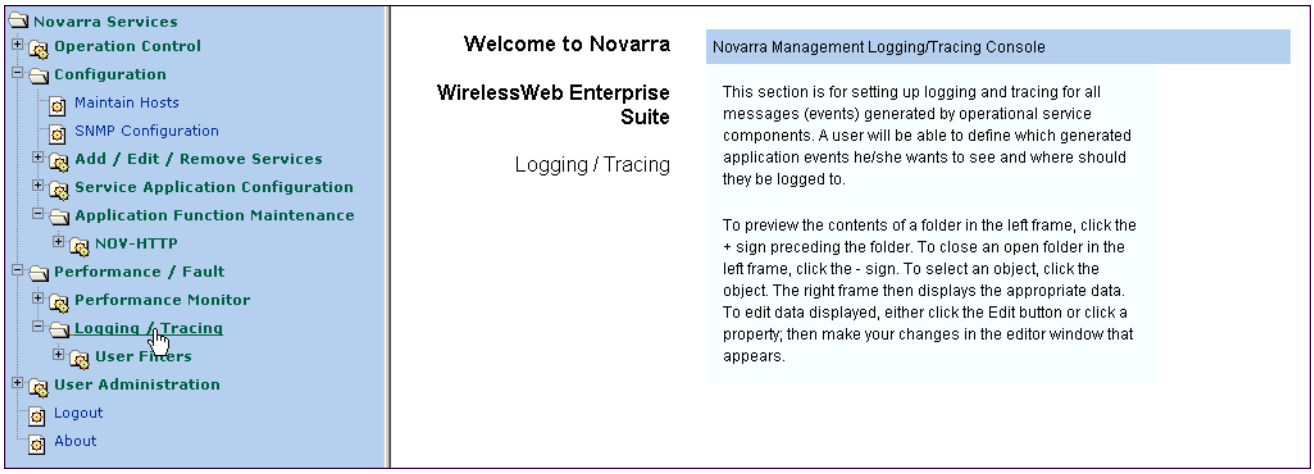
3.4.1.2 Monitor ACA Performance

This page displays performance parameters for each ACA component. These parameters are configured from the **Configure Performance Display** folder.

1. Navigate to the **ACA Performance Monitor** frame:
   Performance/Fault→Performance Monitor→Monitor ACA Performance
2. The **ACA Performance Monitor** frame appears with a table containing the GoS attributes and their values for each service.

3.4.2 Logging/Tracing

This section is for setting up logging and tracing for all messages (events) generated by operational service components. A user will be able to define which generated application events they want to see and where should they be logged to. To access, click the **Logging/Tracing** link in the navigation frame. The **Configuration Section** welcome frame appears.



3.4.2.1 User Filters

LMM Filters are available for each registered user of this application to enable advanced tracing and logging for all messages (events) processed by each operational service component. Each user can create their own filters by specifying filter criteria that they want to use to filter incoming messages.

When an event is generated by one of the components of the WirelessWeb Server, it is received by the LMM Service. Each of the filter's criteria is applied to the event. If the event meets the criteria, then it is sent to the web-based logging client application running on the user's machine for his review. If not, it is dropped.

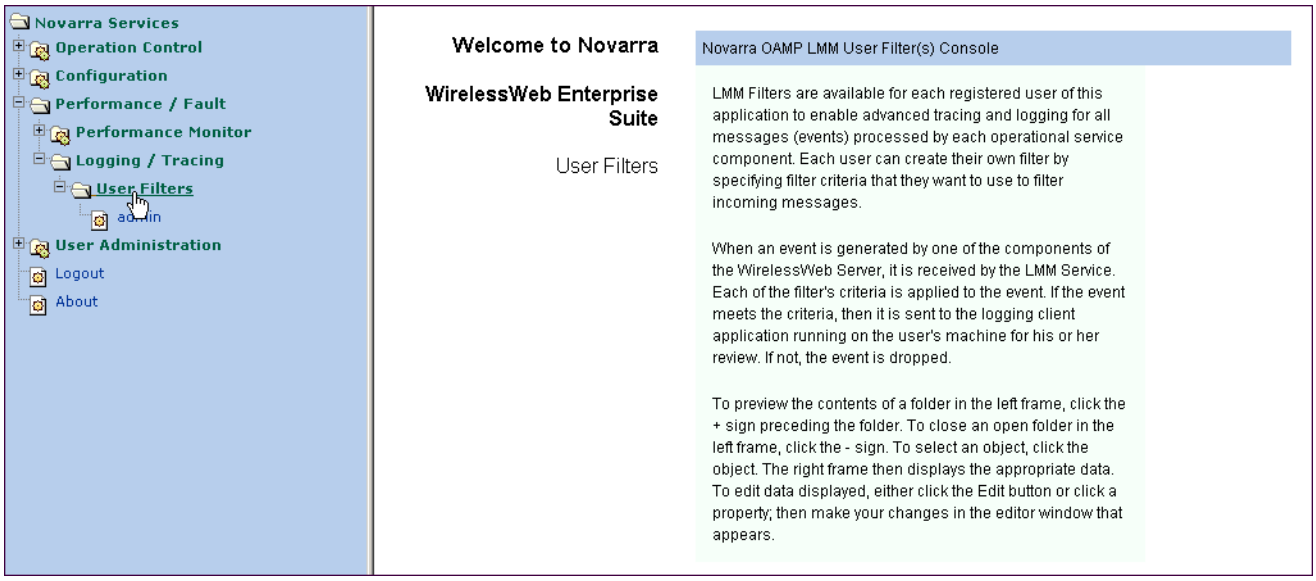
Use this interface to add new LMM filters or to modify, delete, or remove existing filters.

For information on using the LMM Log Client, see section B.1.3, “Using the LMM Log Client” on page B-9.

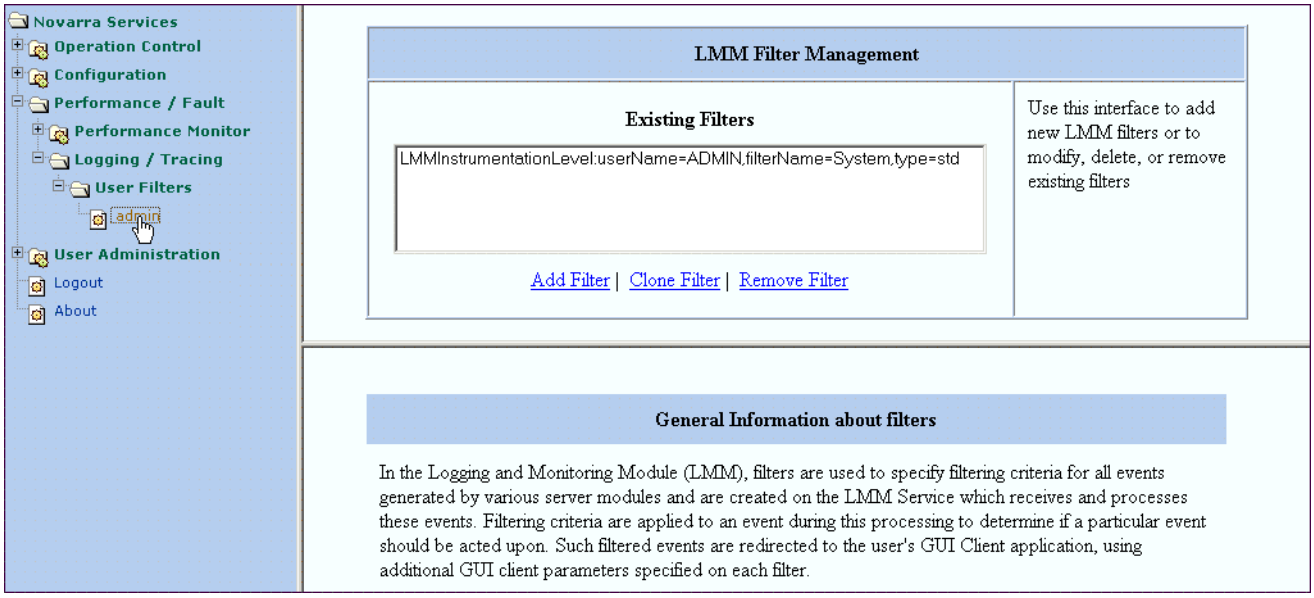
Note:

A default filter “System” is supplied with the Novarra Management Console.

1. Click the **User Filters** link. The LMM User Filter(s) Console welcome frame appears.

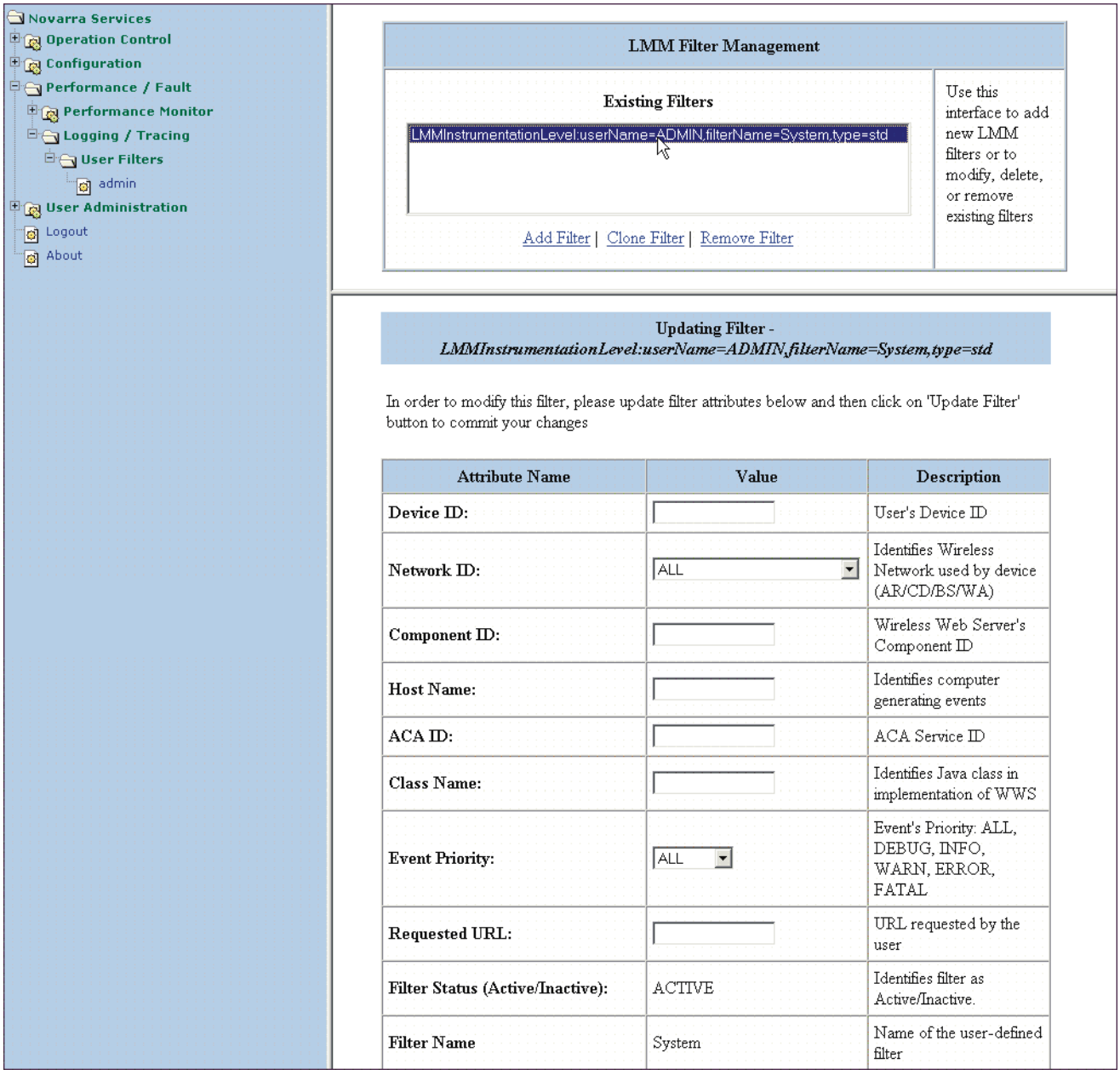


2. Click the user's link below **User Filters** (Example: **admin**). The **LMM Filter Management** frame appears for that user.



3.4.2.1.1 Viewing/Editing a Filter

1. Click on a filter in the Existing Filters list. The list of attributes for that filter appear in the Updating Filter frame.



(Screen shot continued on next page)

TraceEvents:	On Off	Trace on Events info
TraceSystem:	On Off	Trace on System info
TraceSessionManagement:	On Off	Trace on Session Management info
TraceSubscriberAuthorization:	On Off	Trace on Subscriber Authorization info
TraceCookies	On Off	Trace on Cookies
TraceException:	On Off	Trace on Exceptions
TraceNormException:	On Off	Trace on Normalizer exceptions
TraceJavaScript:	On Off	Trace on Java Script information
TraceOutputStream:	On Off	Trace on output stream data
TraceRequestHeaders:	On Off	Trace on request headers
TraceResponseHeaders:	On Off	Trace on response headers
TraceTreeDumpAfterNormalize:	On Off	Trace on a normalized DOM tree
TraceTreeDumpBeforeNormalize:	On Off	Trace on a pre-normalized DOM tree
TraceTreeDumpOnLoad:	On Off	Trace on load time DOM tree
TraceAlert:	On Off	Trace generated Alerts
TraceRF:	On Off	Trace RF events

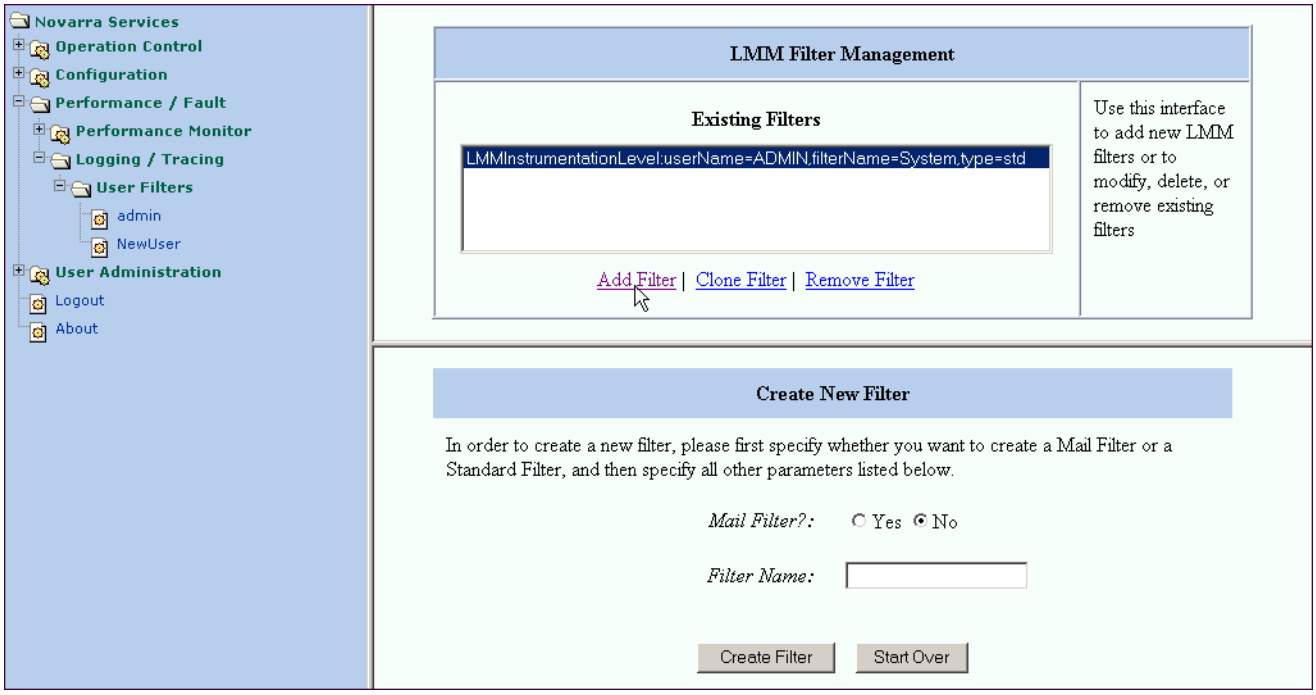
Update

2. Change the information you want to log to the Log Client Console by selectively turning on or off different trace levels.

   You can filter the amount of information by restricting the logged messages to those that match information that you supply here. Example: Entering a Device ID will show only messages that match that device ID. A blank field will match any message.
3. To save the changes you have made, click the Update button.

3.4.2.1.2 Add a Filter

1. Click the **Add Filter** link in the **LMM Filter Management** frame. The **Create New Filter** frame appears.



2. Enter in the information and click the Create Filter button. The filter now appears in the Existing Filters list.

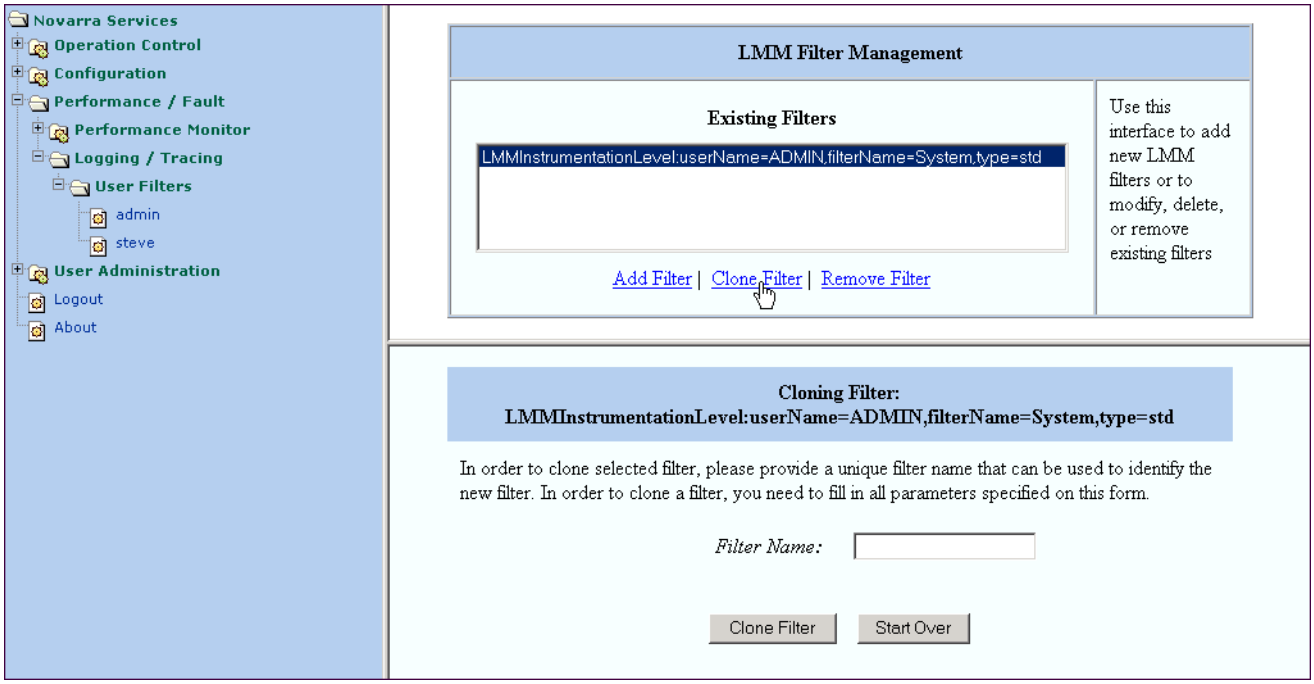
Note:

By default, a filter is off until started by a user.

3. Click on the new filter's name in the list of Existing Filters.
4. Click the Start Filter button at the bottom of the Updating Filter frame to start it.

3.4.2.1.3 Clone a Filter

1. Click the filter you want to clone (copy) in the Existing Filters list. Click the **Clone Filter** link. The **Cloning Filter:** frame appears.



2. Enter a unique name to be used for the cloned filter.
3. Click the Clone Filter button. The cloned filter can now be modified and started. See "Viewing/Editing a Filter" on page 3-42.

3.4.2.1.4 Remove a Filter

1. Click the filter you want to remove in the Existing Filters list. Click the **Remove Filter** link.
2. An alert appears confirming the deletion of the filter. Click the OK button.

3.5 User Administration Folder

This section provides controls for administration of the users of the Novarra Management Console. System administrators are able to add and remove users, modify passwords, and classify a new user as an LMM user or as an administrator.

1. To access, click the **User Administration** link in the navigation frame. The **User Administration Section** welcome frame appears.

2. The following item is available in the **Performance/Fault** folder:
   - "Add/Remove Users"
   - "Change Password"

3.5.1 Add/Remove Users

Click the **Add/Remove Users** link. The **User Maintenance** frame appears.

3.5.1.1 Add User

1. Click the **Add a User** link. The **User Creation** frame appears.

2. Select a **User Group**.

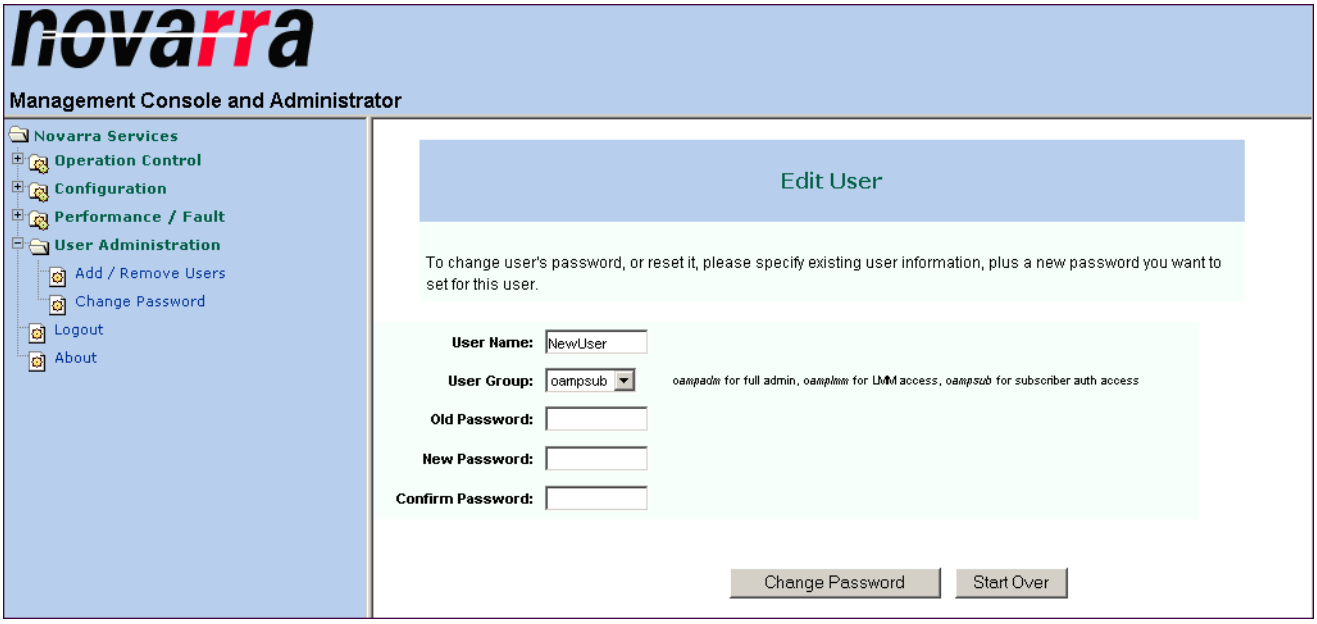
User Group	Type of User	Access Rights
oampadm	System Administrator	Full access rights.
oamplmm	LMM User	Rights limited to creating and updating filters for this user only and the viewing and cloning filters of other users.
oampsub		Subscriber Authorization access

3. Enter the **User Name**.
4. Enter the **User Password**. A minimum of six alphanumeric characters must be used.
5. Enter the password in the **Confirm Password** field.
6. Click the Add User button. The new user has been added.

3.5.1.2 Edit User

1. In the **User Maintenance** frame, click the User you want to edit.

2. Click the **Edit a User** link. The **Edit User** frame appears.



3. Enter the **Old Password**.

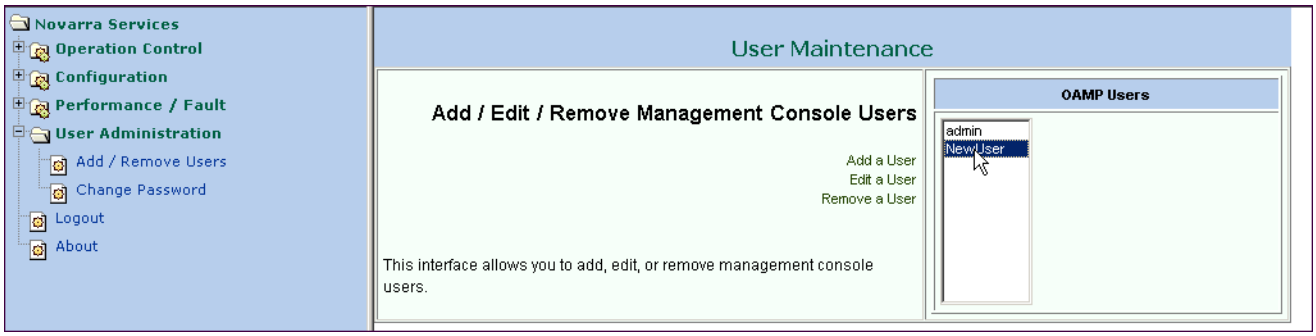
Note:

If the Old Password is not known, the User would need to be removed and then re-added. To remove see 3.5.1.3, "Remove User," below. To add, see section 3.5.1.1, "Add User" on page 3-47.

4. Enter the **New Password**. A minimum of six alphanumeric characters must be used.
5. Enter the new password in the **Confirm Password** field.
6. Click the Change Password button. A message confirming the Password was successfully changed for the user appears.

3.5.1.3 Remove User

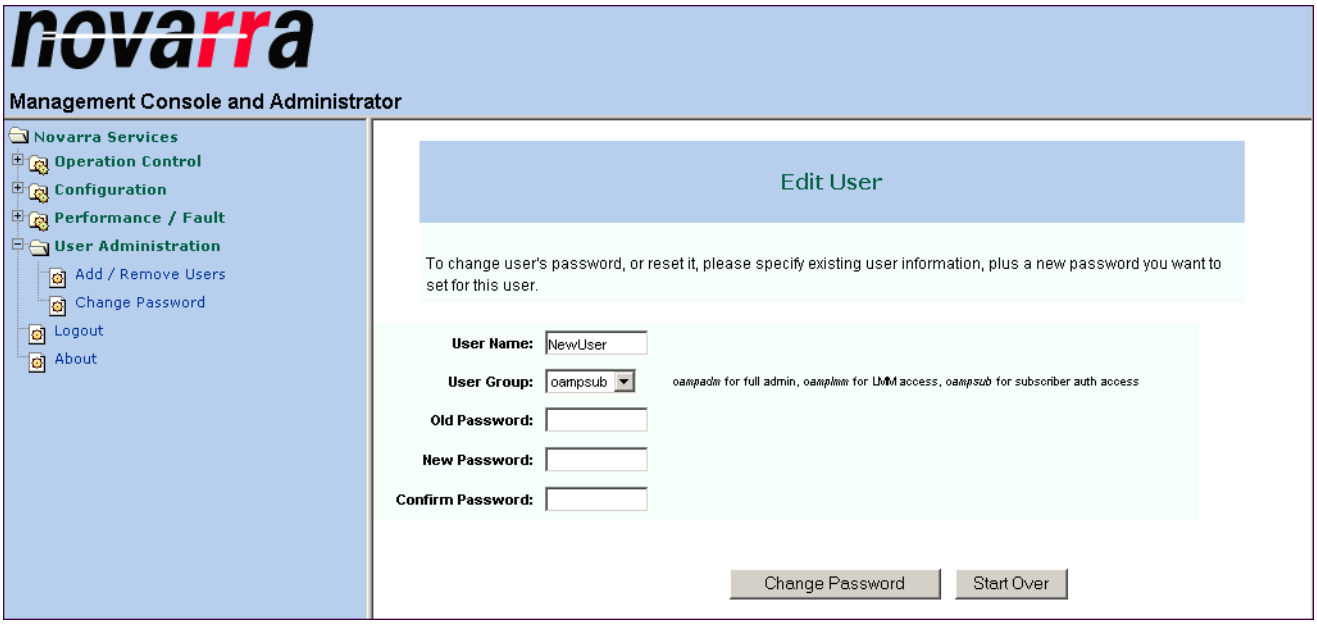
1. In the **User Maintenance** frame, click the User you want to remove.



2. Click the **Remove Users** link. An alert appears confirming the deletion of the user. Click the OK button. The user is removed from the list of Users.

3.5.2 Change Password

1. Click the **Change Password** link. The **Edit User** frame appears.



2. Enter the **User Name**.
3. Select the **User Group**.
4. Enter the **Old Password**.

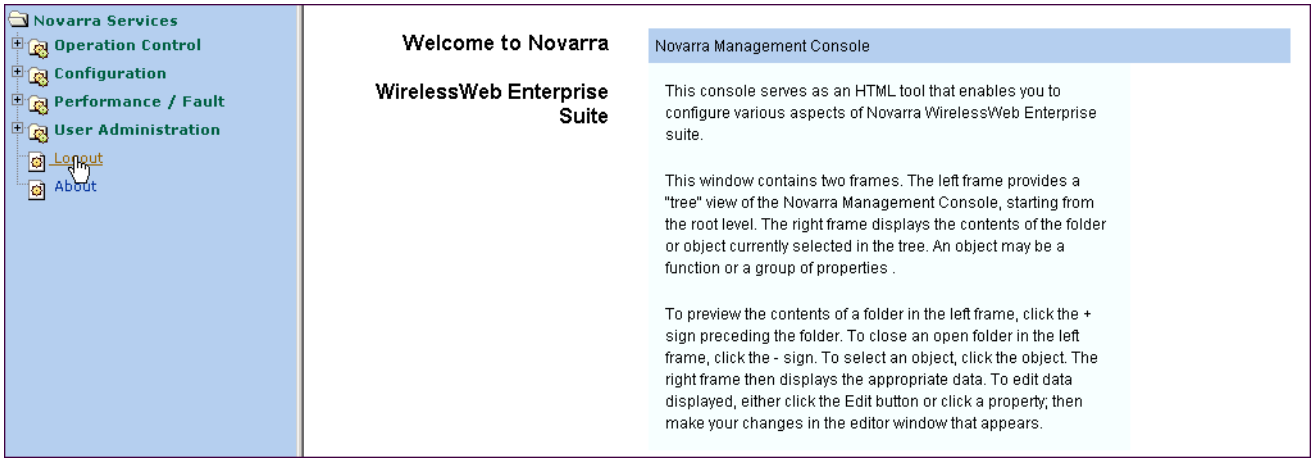
Note:

If the Old Password is not known, the User would need to be removed and then re-added. To remove see section 3.5.1.3, "Remove User" on page 3-48. To add, see section 3.5.1.1, "Add User" on page 3-47.

5. Enter the **New Password**. A minimum of six alphanumeric characters must be used.
6. Enter the new password in the **Confirm Password** field.
7. Click the Change Password button. A message confirming the Password was successfully changed for the user appears.

3.6 Logout

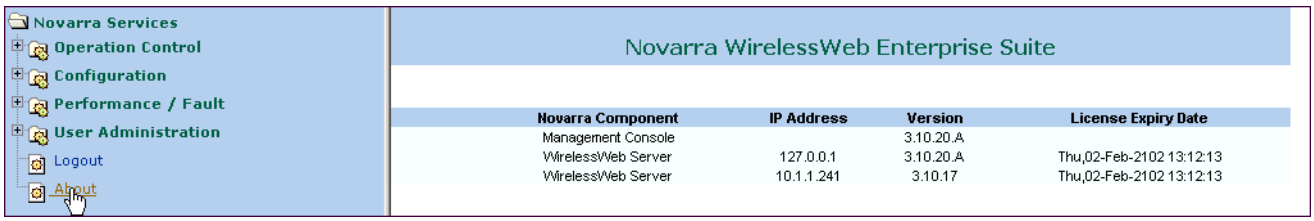
1. Click the **Logout** link at the bottom of the navigation frame.



2. You are logged out of Management Console and the Login screen appears.

3.7 About

1. Click the **About** link at the bottom of the navigation frame.
2. The right frame displays information about WirelessWeb Enterprise Suite.



Administering WirelessWeb Server 4

WirelessWeb Server settings are exposed through various configuration files. The following sections describe the steps you must take to configure each administrative option.

Table 4-1: Most common configuration options

Item	Description	Section
Client Side Secure Sockets Layer (SSL)	Allows secure transactions between WirelessWeb Server and a secure Web site.	4.1.1
Device authorization	Authorizes known devices before allowing access to WirelessWeb Server.	4.2
Proxy server settings	Restricts Internet access by passing requests through a third-party proxy server.	4.3.1
SNMP agent	Reports data about WirelessWeb server to an SNMP 2.0 management information base (MIB)	4.4
Cookies	Store cookies for each browser session.	4.5
JavaScript administration	Enable JavaScript support and control error handling.	4.6

4.1 Security Configuration

Novarra WirelessWeb Server supports encryption/decryption in two phases:

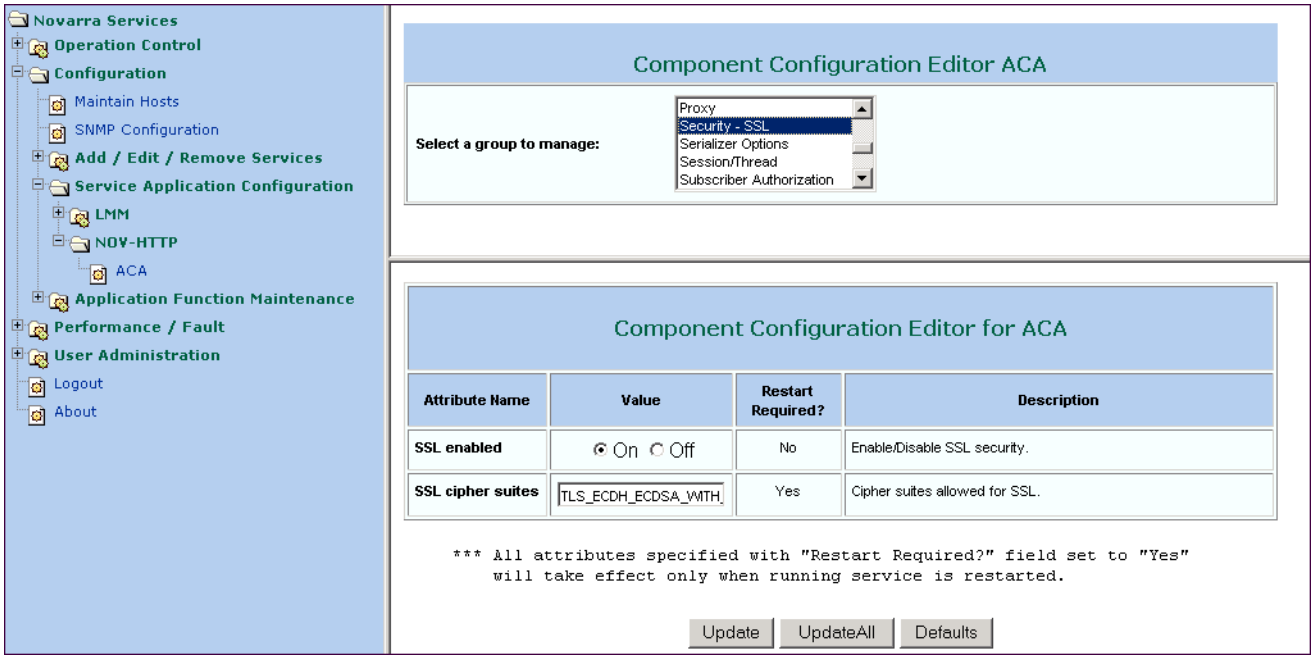
- Secure Sockets Layer (SSL) 3.0 and earlier between secure Web sites and WirelessWeb Server.
- Certicom's Elliptic Curve Cryptography (ECC) technology between the wireless device and the server.

Using the Novarra Management Console, you can turn SSL encryption on and off, and specify which content is secure between Novarra WirelessWeb Server and the client devices.

4.1.1 SSL Configuration

WirelessWeb Server is capable of establishing secure connections with an SSL server.

1. Navigate to the **Component Configuration Editor for ACA** for the the service you want to configure. (Example: NOV-HTTP):
   Configuration→Service Application Configuration→NOV-HTTP→ACA
2. Click on **Security - SSL**. The SSL **Component Configuration Editor for ACA** appears in the bottom frame.



3. Make the necessary changes in the fields and click the Update button. The bottom frame displays the message “Information for component "ACA" has been successfully updated and sent to the host.”

Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

4. Restart the service (see section 3.2.3.2, “Start/Stop NOV-HTTP” on page 3-9.)

4.2 Device Authorization

Device authorization offers you an added layer of security. By specifying a list of authorized subscribers, you can determine precisely which wireless devices have access to Novarra WirelessWeb Server, and therefore your company's Intranet. Any device that connects to WirelessWeb Server must be listed in your directory of authorized subscribers:

4.2.1 Determining the Device ID

Each handheld device exposes its device ID in a different manner.

4.2.2 Enable Subscriber Authorization

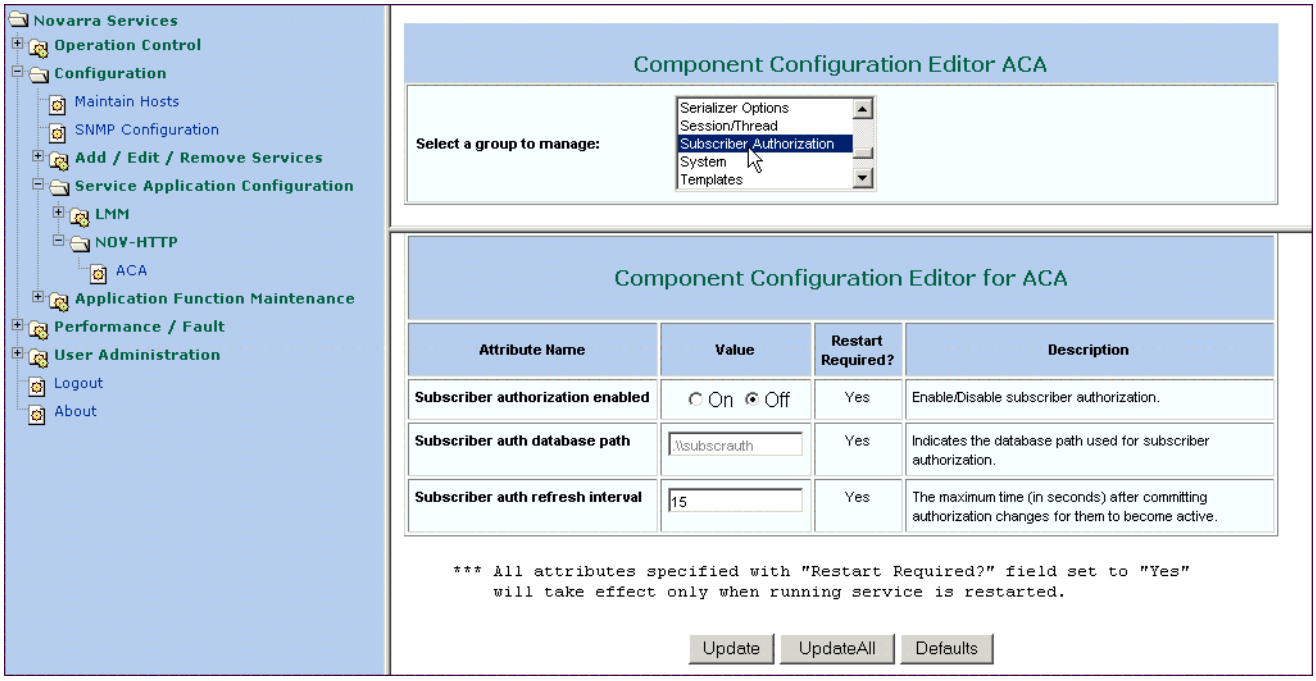
Subscriber Authorization for a service must be enabled in order to deny access to the WirelessWeb server by devices not listed on that service's **Device List**.

Note:

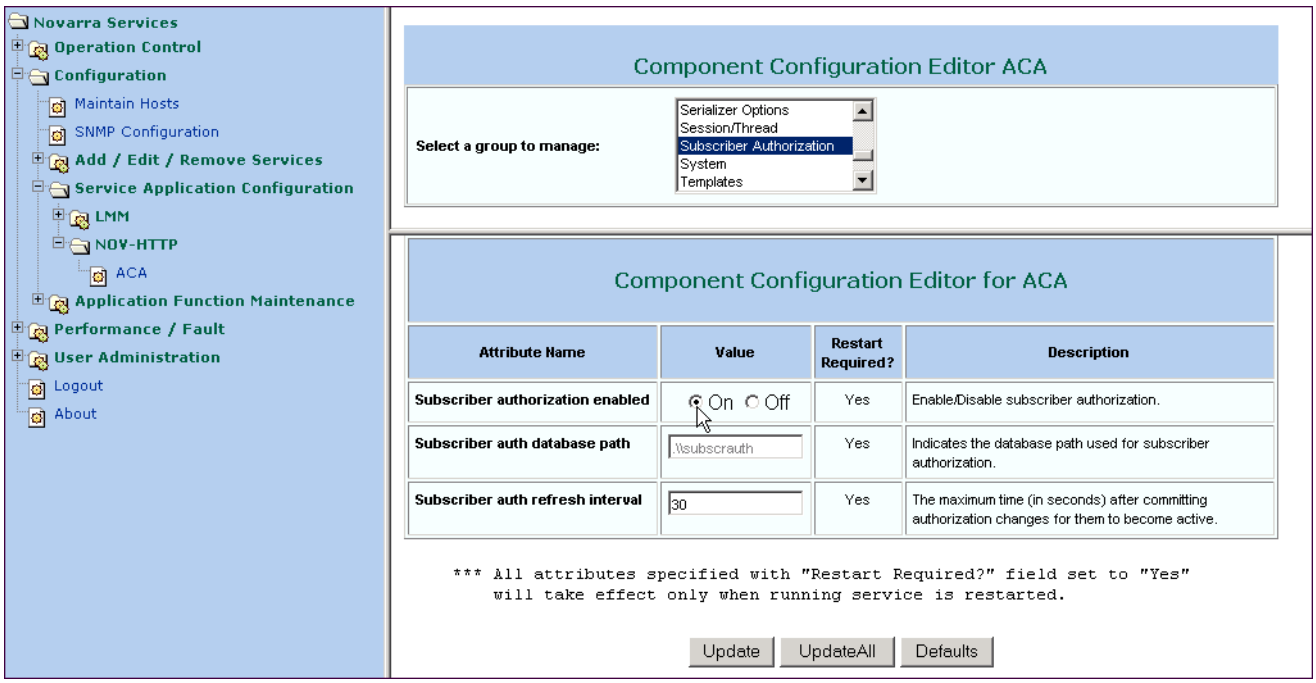
When a service is initially added, disabled is the default for Subscriber Authorization.

1. Navigate to the **Component Configuration Editor for ACA** for the the service you want to enable Subscriber Authorization (Example: NOV-HTTP):
   Configuration→Service Application Configuration→NOV-HTTP→ACA

2. Click **Subscriber Authorization** in the **Select a group to manage:** list box.



3. Click the **Subscriber authorization enabled On** radio button and set the **Subscriber auth refresh interval** to 30.



4. Click the Update button. The bottom frame displays the message “Information for component "ACA" has been successfully updated and sent to the host.”

Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

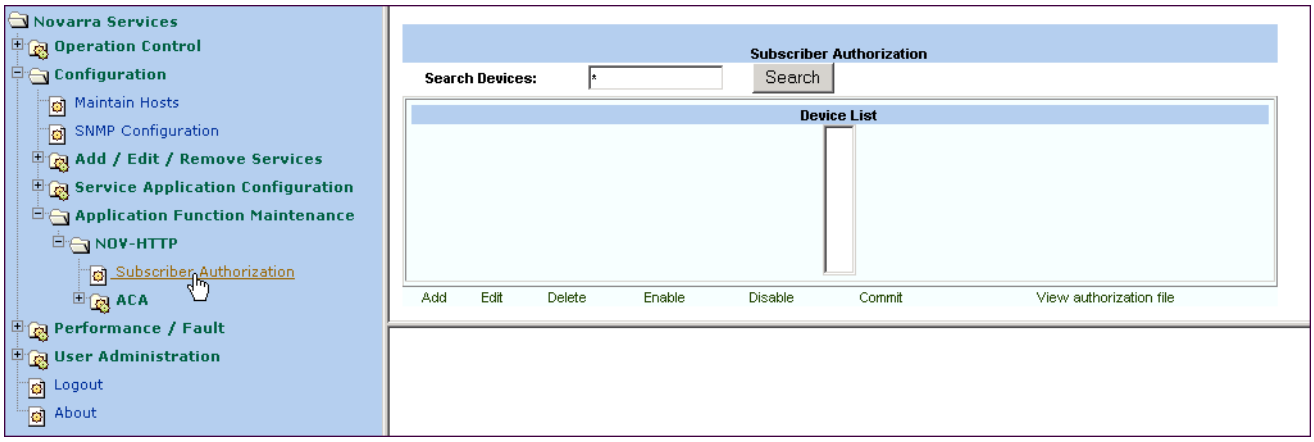
5. Restart the service (see section 3.2.3.2, “Start/Stop NOV-HTTP” on page 3-9.)
6. The service is now **UP** again and the subscriber authorization change is in effect.

4.2.3 Add Devices

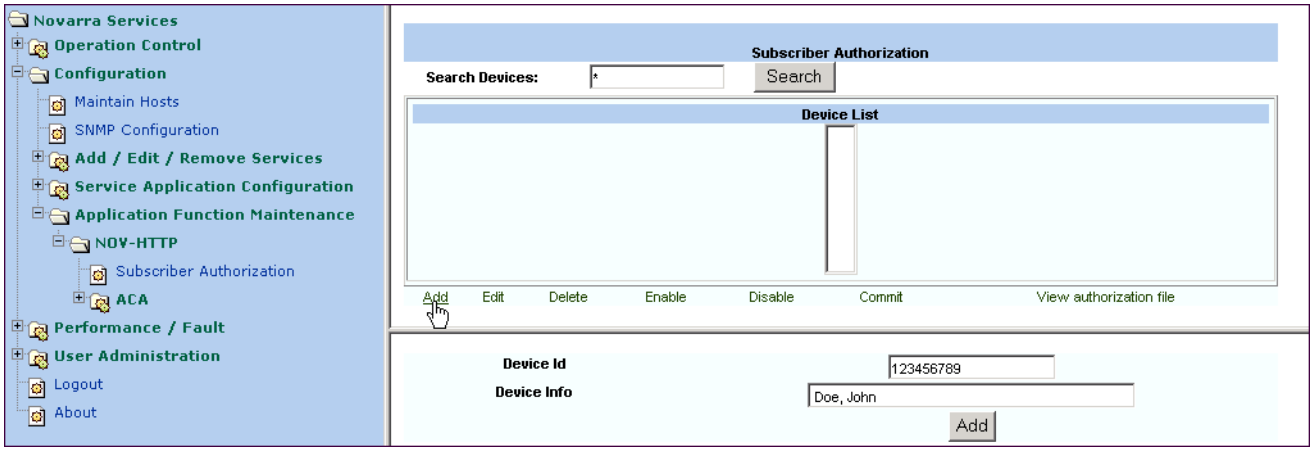
The following procedure shows you how to add devices to a service.

1. Navigate to the **Subscriber Authorization** frame for the service you want to authorize devices (Example: NOV-HTTP):

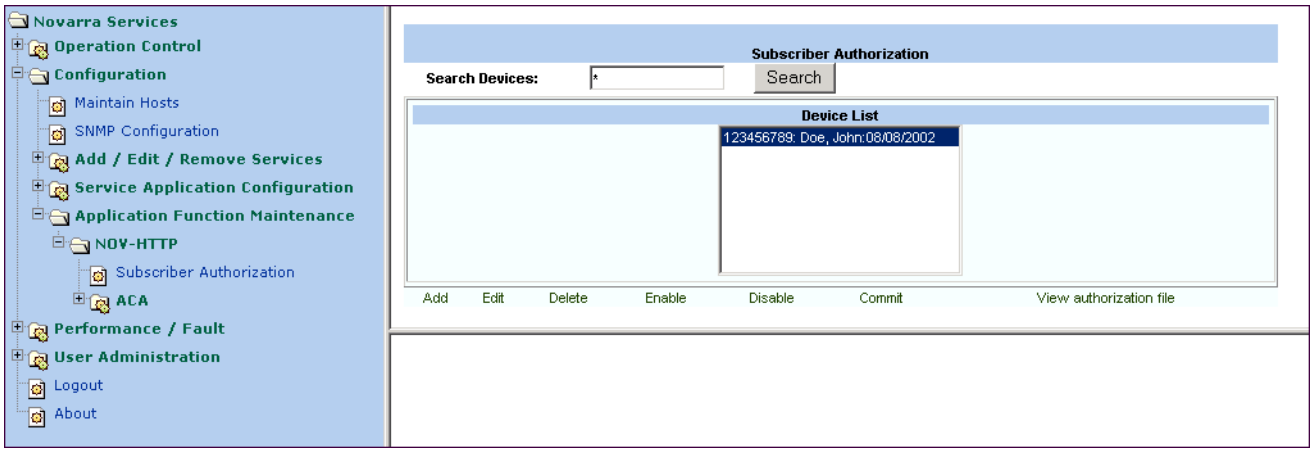
   Configuration→Application Function Maintenance→NOV-HTTP→Subscriber Authorization



2. Click the **Add** link.The frame beneath **Subscriber Authorization** now has **Device ID** and **Device Info** editable fields.



3. Enter the **Device ID** and **Device Info**. To determine the device's ID, see section 4.2.1, "Determining the Device ID" on page 4-3. The **Device Info** is whatever you decide (e.g. salesman's name).
4. Click the Add button. The device name now appears in the **Device List**.



Note:

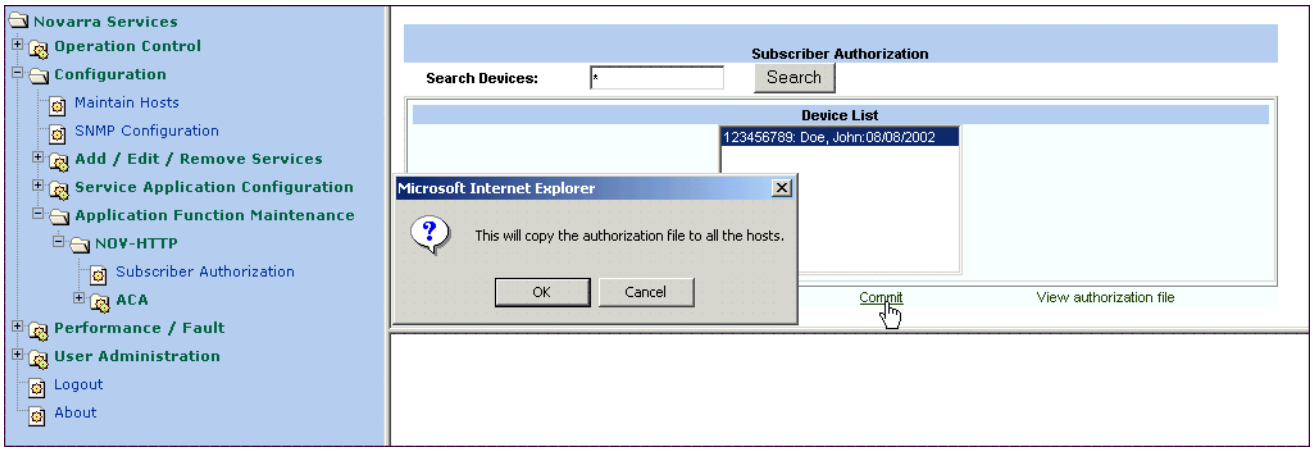
The devices entered are automatically in the ENABLED mode

5. Repeat steps 2 through 4 for each device you need to add on this service.

Note:

Changes to the **Subscriber Authorization** will not take effect until they are committed.

6. Click the **Commit** link. An alert appears confirming the authorization file will be copied to all hosts. Click the OK button.

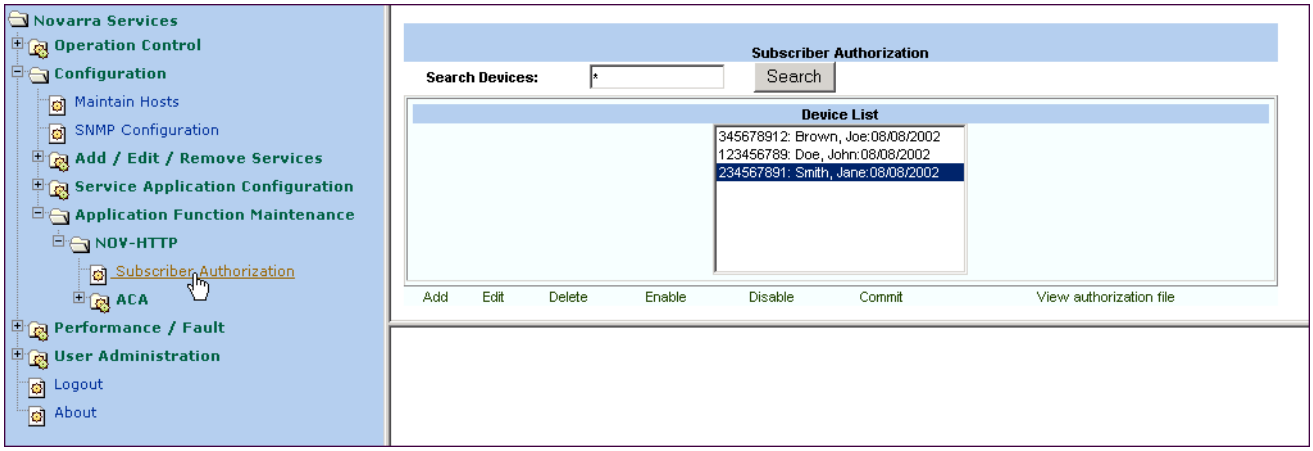


4.2.4 Disable Devices

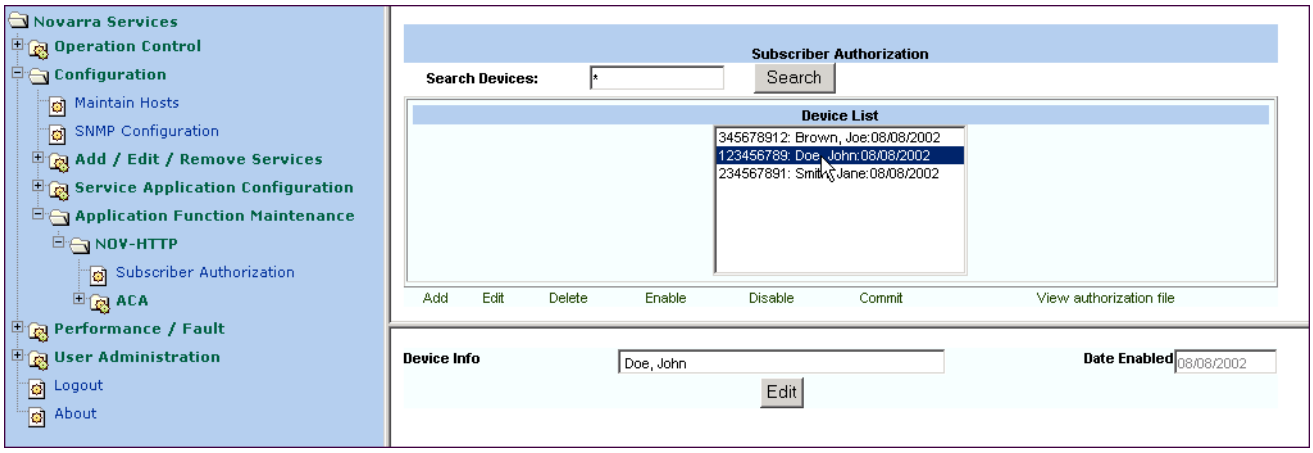
At times you may have devices listed on a service, but want to disable their ability to access the WirelessWeb server.

1. Navigate to the **Subscriber Authorization** frame for the service you want to disable devices (Example: NOV-HTTP):

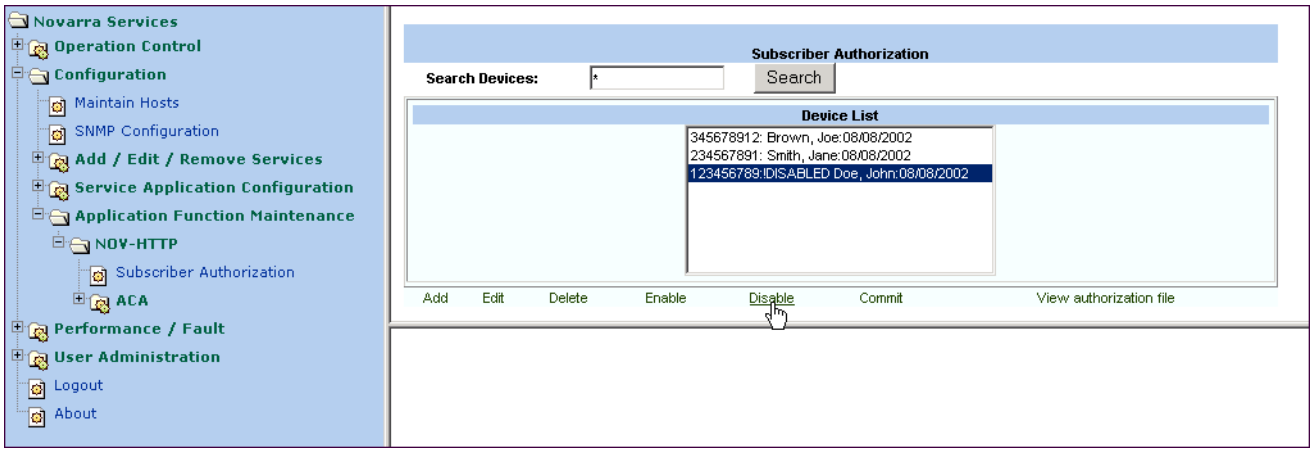
   Configuration→Application Function Maintenance→NOV-HTTP→Subscriber Authorization



2. Click a device in the Device List that is currently enabled (the word DISABLED does not appear in the name on the Device List).



3. Click the **Disable** link. The device name is now displayed with the word DISABLED within the name on the Device List.

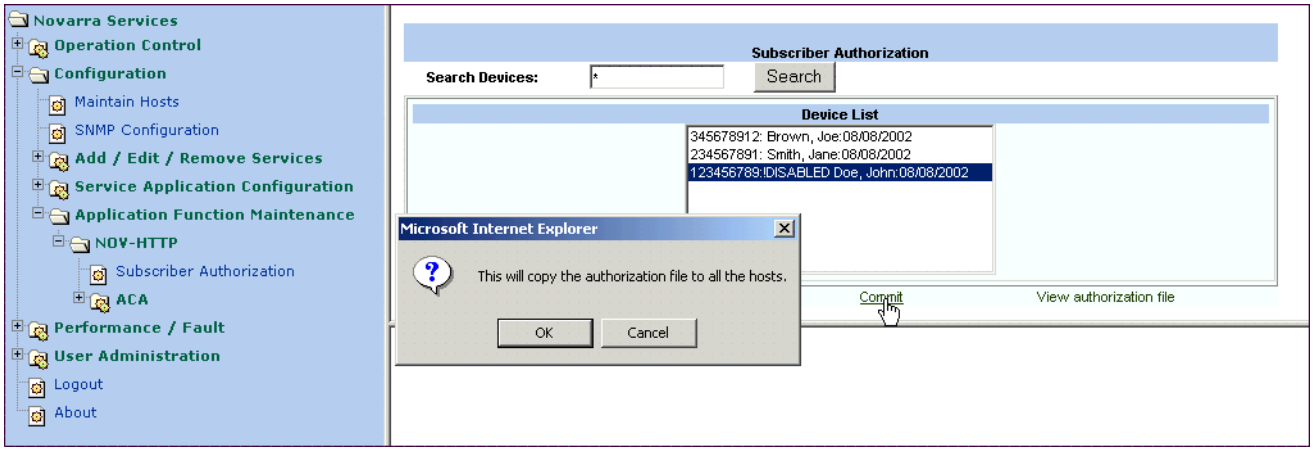


4. Repeat steps 2 and 3 for each device you need to disable on this service.

Note:

Changes to the **Subscriber Authorization** will not take effect until they are committed.

5. Click the **Commit** link. An alert appears confirming the authorization file will be copied to all hosts. Click the OK button.

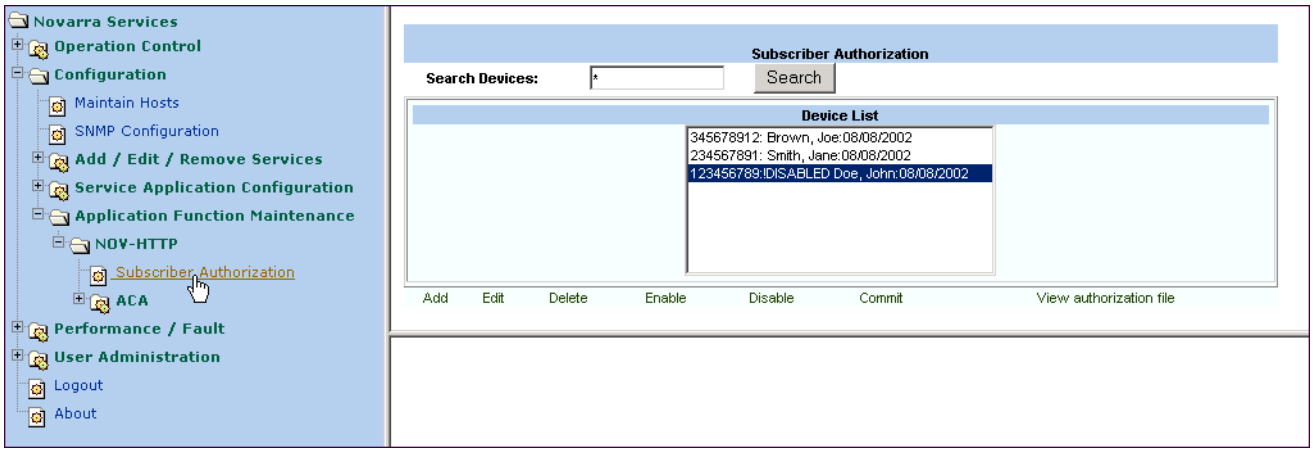


4.2.5 Enable Devices

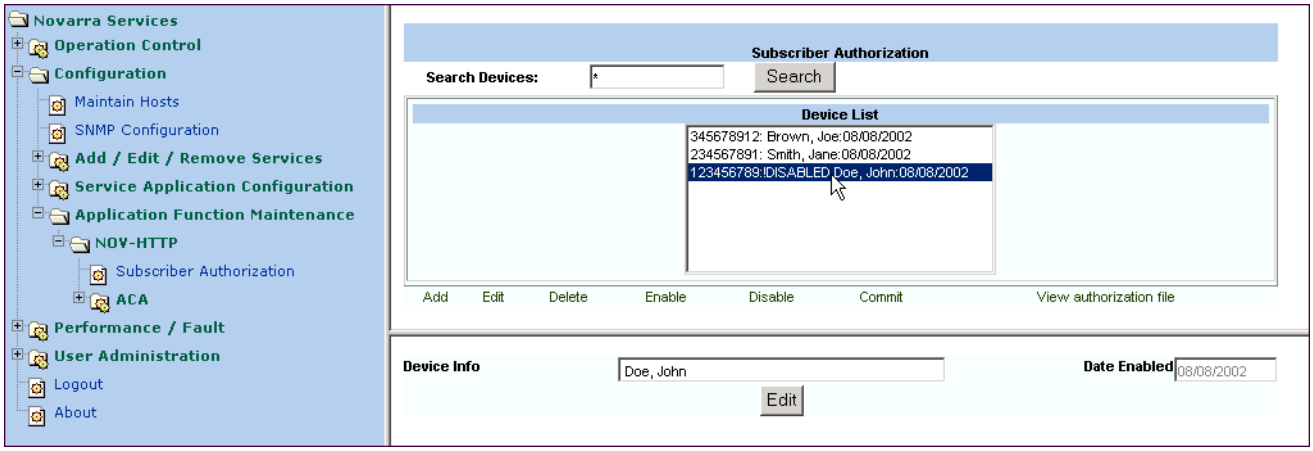
At times you may have disabled devices listed on a service, but now want to enable their ability to access the WirelessWeb server.

1. Navigate to the **Subscriber Authorization** frame for the service you want to enable devices (Example: NOV-HTTP):

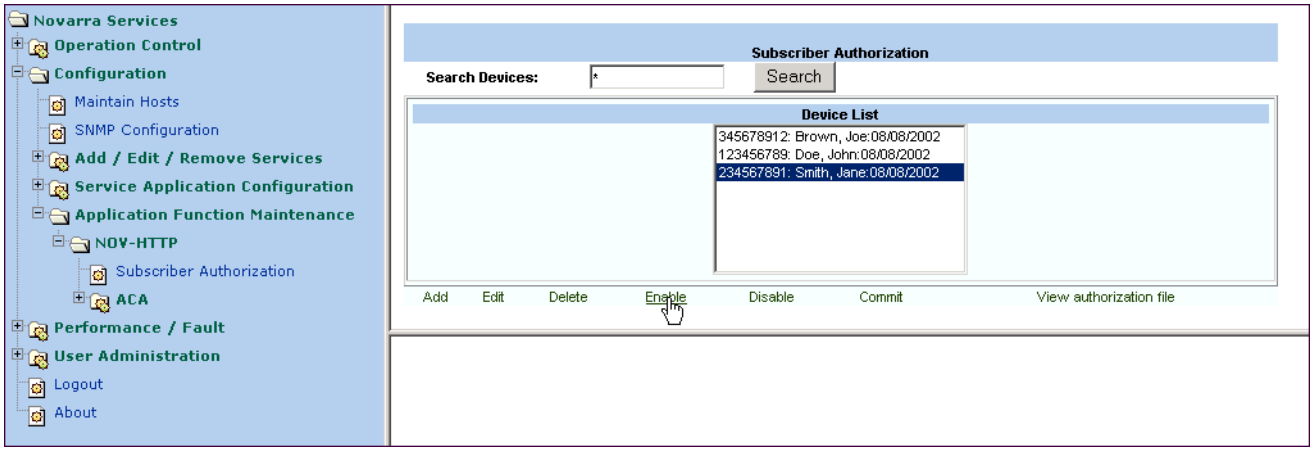
Configuration→Application Function Maintenance→NOV-HTTP→Subscriber Authorization



2. Click a device in the Device List that is currently disabled (the word DISABLED appears in the name on the **Device List**).



3. Click the **Enable** link. The device name no longer displays the word DISABLED within the name on the **Device List**.

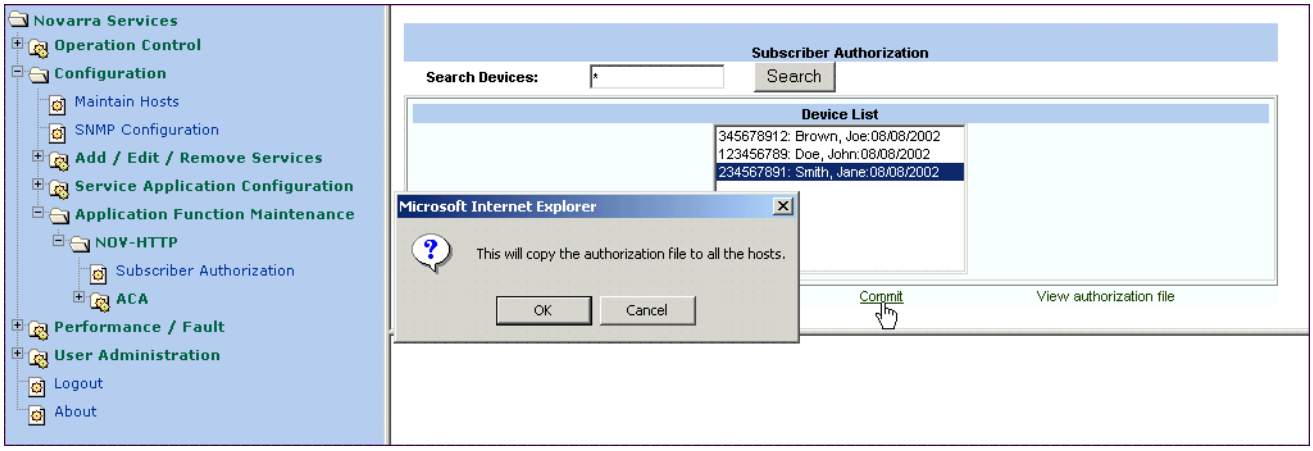


4. Repeat steps 2 and 3 for each device you need to enable on this service.

Note:

Changes to the **Subscriber Authorization** will not take effect until they are committed.

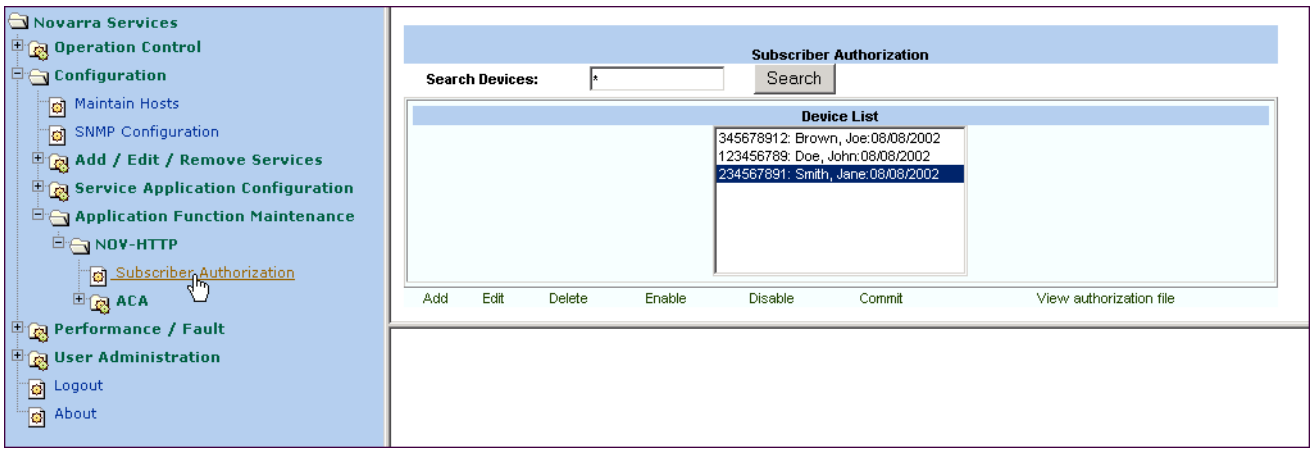
5. Click the **Commit** link. An alert appears confirming the authorization file will be copied to all hosts. Click the OK button.



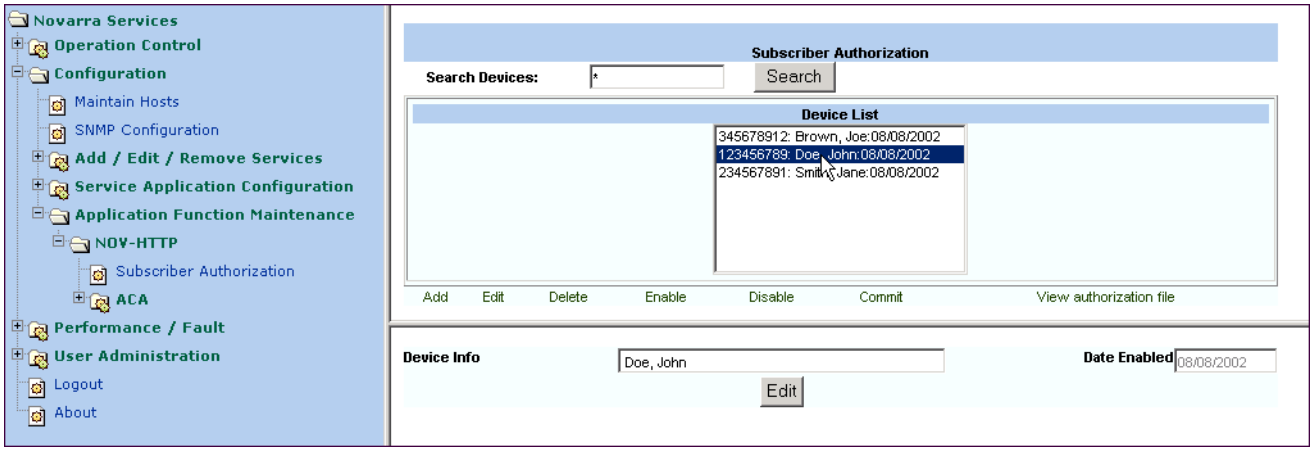
4.2.6 Edit a Device

At times you may need to edit the Device Info for a particular Device ID. An example would be that the device was given to another salesman and you need to reflect this in your **Device List**.

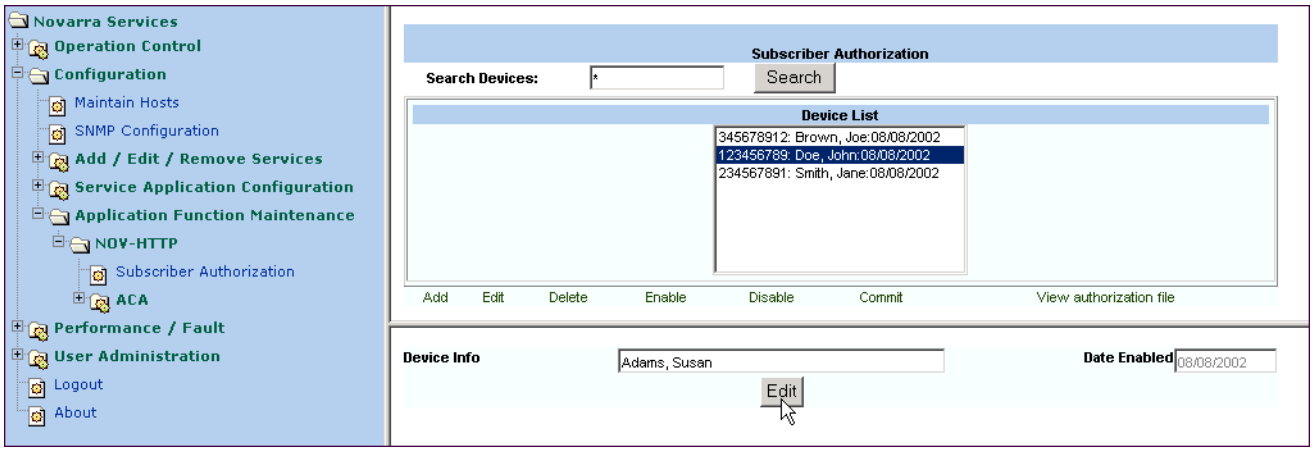
1. Navigate to the **Subscriber Authorization** frame for the service you want to edit devices (Example: NOV-HTTP):
   Configuration→Application Function Maintenance→NOV-HTTP→Subscriber Authorization



2. Click the device in the **Device List** that you want to edit.



3. Change the information in the **Device Info** field and click the Edit button.

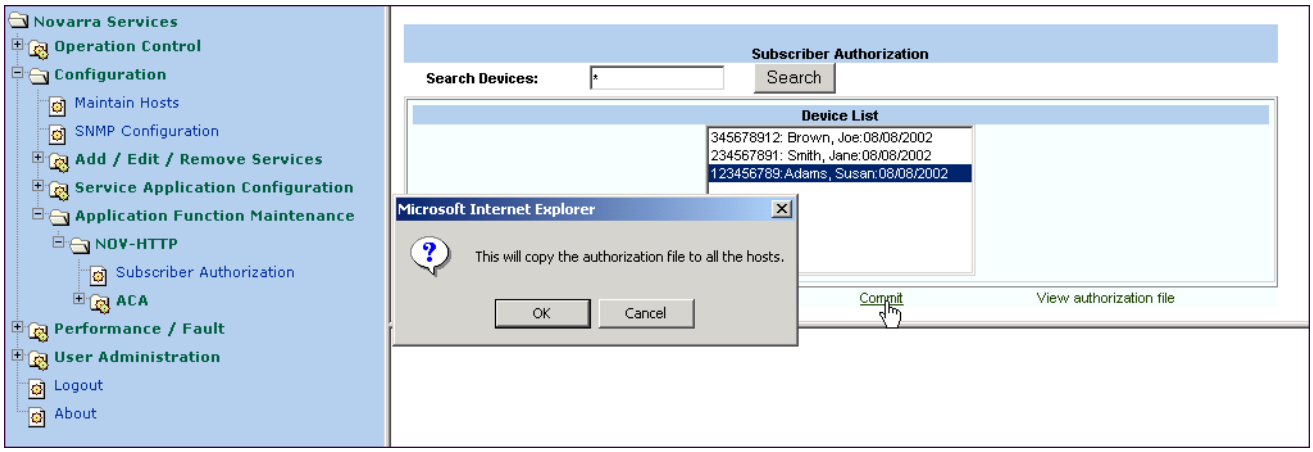


4. Repeat steps 2 and 3 for each device you need to edit on this service.

Note:

Changes to the **Subscriber Authorization** will not take effect until they are committed.

5. Click the **Commit** link. An alert appears confirming the authorization file will be copied to all hosts. Click the OK button.

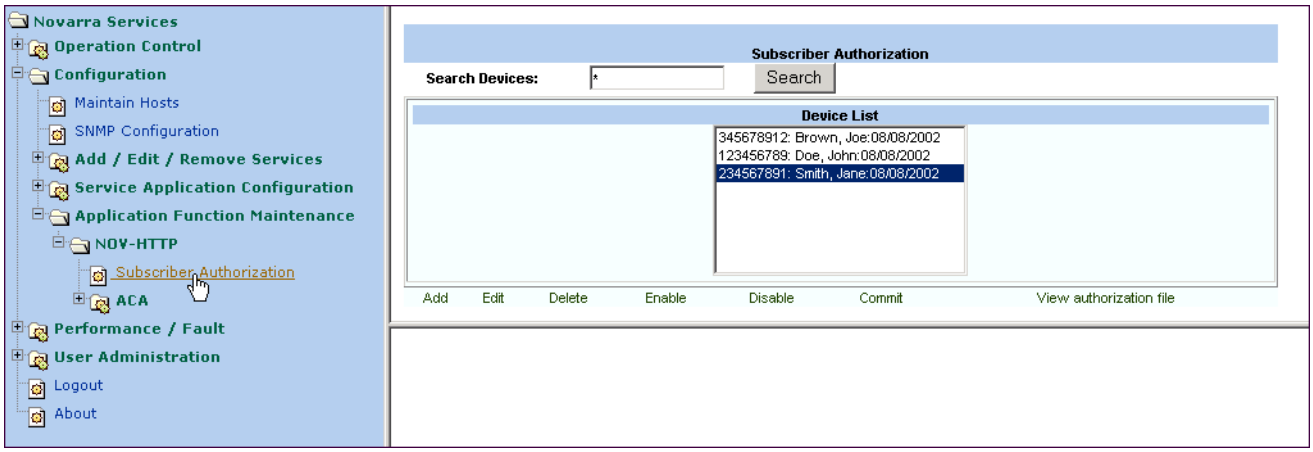


4.2.7 Delete a Device

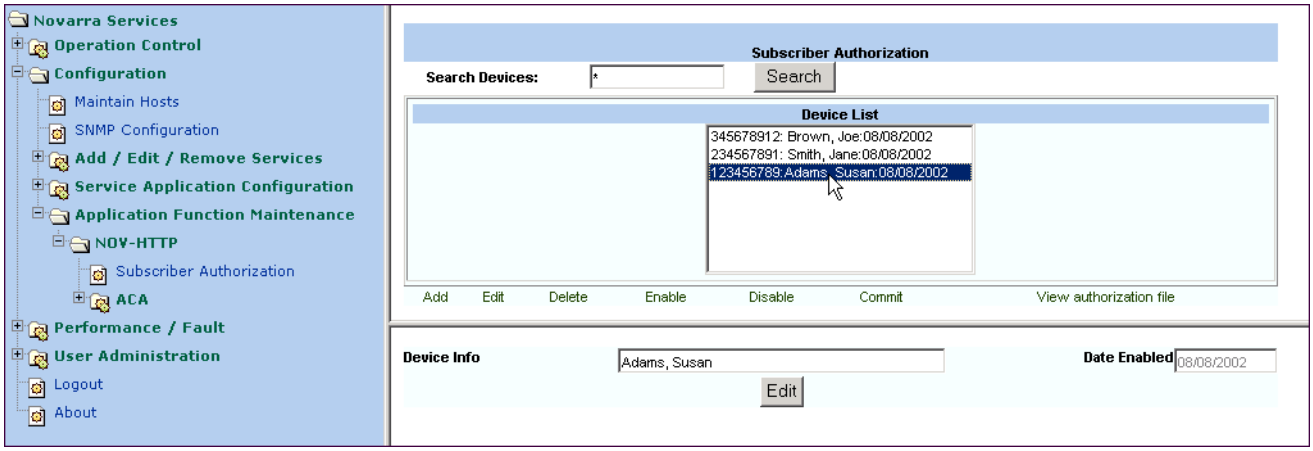
At times you may need to delete devices from your Device List. An example would be if a salesman left your company and the device on the Device List was his personal property.

1. Navigate to the **Subscriber Authorization** frame for the service you want to edit devices (Example: NOV-HTTP):

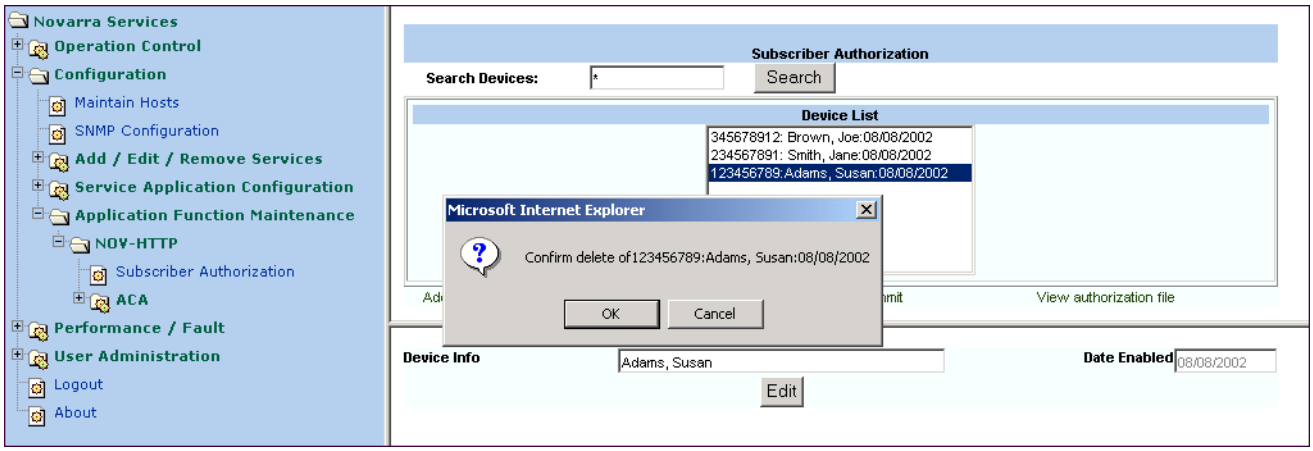
   Configuration→Application Function Maintenance→NOV-HTTP→Subscriber Authorization



2. Click on the device in the **Device List** that you want to delete.



3. Click the **Delete** link. An alert appears confirming the deletion of the device. Click the OK button.

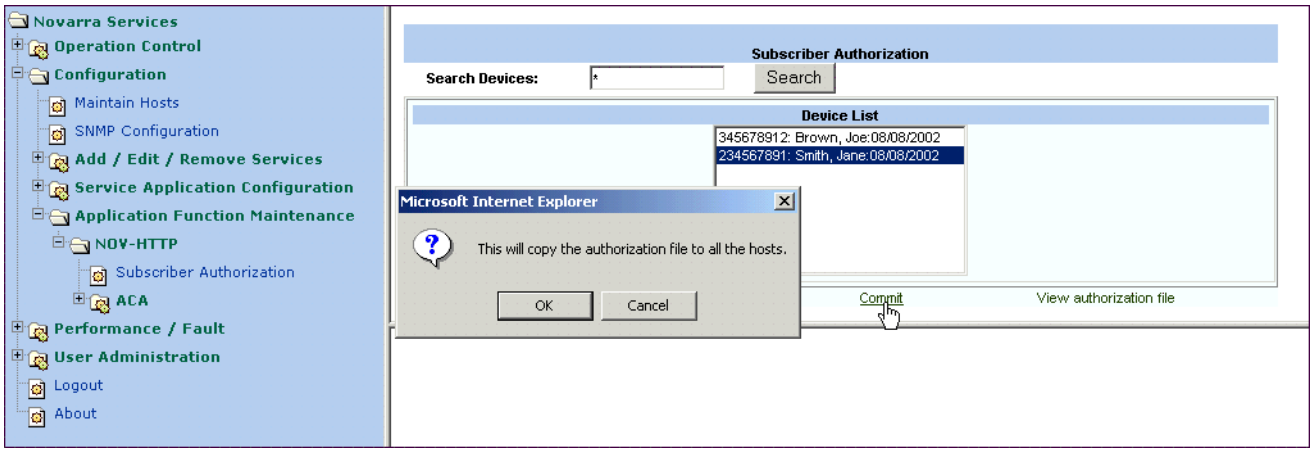


4. Repeat steps 2 and 3 for each device you need to delete on this service.

Note:

Changes to the **Subscriber Authorization** will not take effect until they are committed.

5. Click the **Commit** link. An alert appears confirming the authorization file will be copied to all hosts. Click the OK button.



4.3 Internet Access Restriction

Through WirelessWeb Server you have the option of denying or allowing individual subscribers Internet access. You can also control the availability of specific sites, depending upon the level of sophistication required. In conjunction with Novarra WirelessWeb Server, you can set up a proxy server or firewall to limit subscriber access to content.

Firewalls are not described below, since they are vendor-specific and you need not configure WirelessWeb Server to work through a firewall.

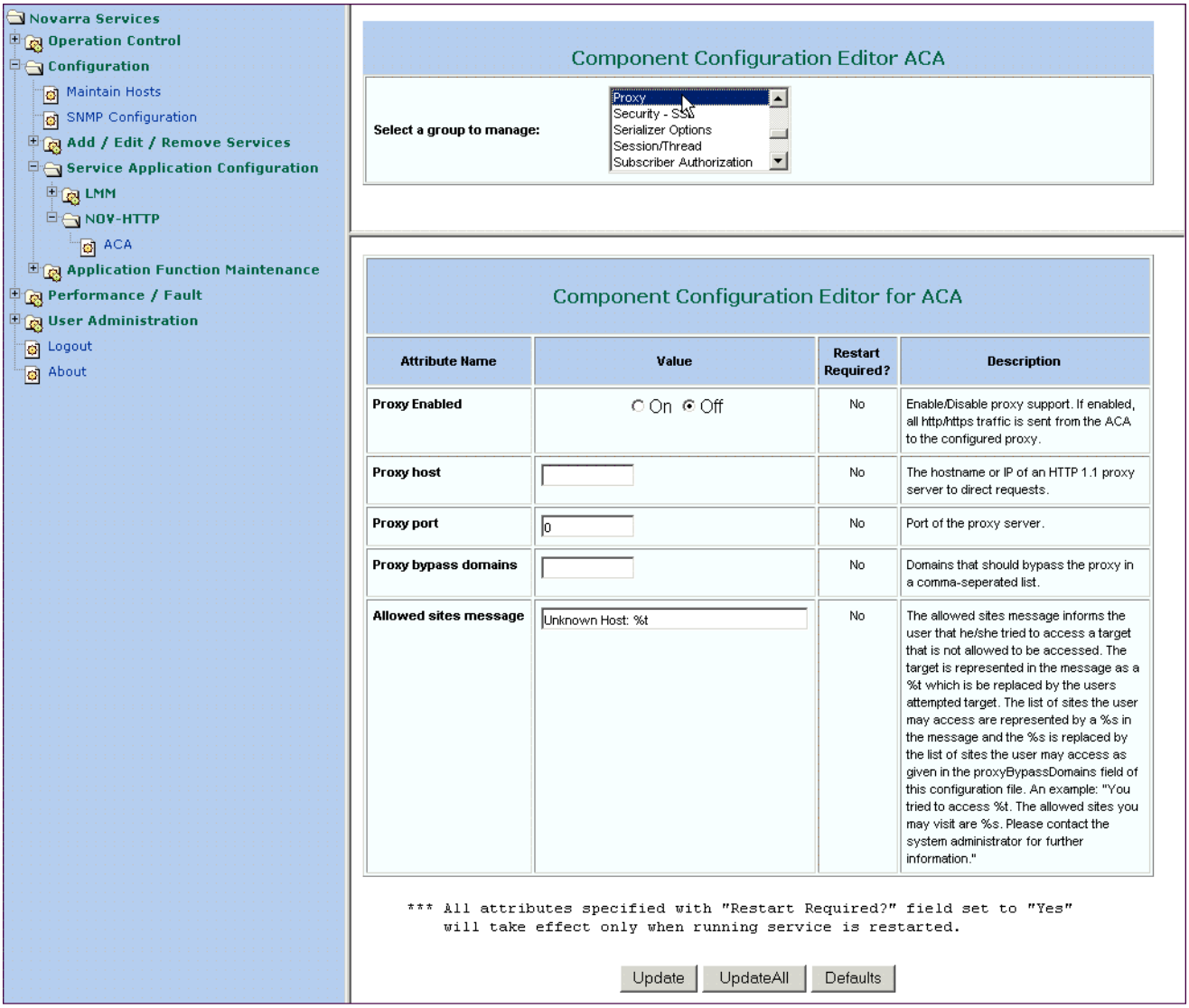
4.3.1 Proxy Server

The optimal solution for restricting Internet is through an HTTP 1.1 proxy server. You can easily connect WirelessWeb Server to your proxy server, which would allow or deny access to all content on the Internet or to specific sites. A proxy server gives you the most flexibility in controlling access to the Internet.

You must specify the address of the proxy server by using the Novarra Management Console:

1. Navigate to the **Component Configuration Editor for ACA** for the the service you want to configure. (Example: NOV-HTTP):
   Configuration→Service Application Configuration→NOV-HTTP→ACA

2. Click on **Proxy**. The Proxy **Component Configuration Editor for ACA** appears in the bottom frame.



3. Make the necessary changes in the fields and click the Update button. The bottom frame displays the message “Information for component "ACA" has been successfully updated and sent to the host.”

Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

4. Restart the service (see section 3.2.3.2, “Start/Stop NOV-HTTP” on page 3-9.)

4.4 Novarra Agent

When you install Novarra WirelessWeb Server, you have the option to include the Simple Network Management Protocol (SNMP) 2.0 component. For more information about running the setup and starting Novarra WirelessWeb Server, see Chapter 2, “Installing Novarra WirelessWeb Enterprise Suite.”

To start Novarra Agent:

Start→Programs→Novarra WirelessWeb→Start Novarra Agent

To stop Novarra Agent:

Start→Programs→Novarra WirelessWeb→Stop Novarra Agent

Novarra Agent uses Java Management eXtensions (JMX) to support both SNMP and Web-based management. Novarra Agent reports data about WirelessWeb Server’s status against a custom Novarra management information base (MIB). This MIB is supplied as part of the release, and you can compile it through any commercial SNMP management utility. Note that you must configure your SNMP manager to talk to the Novarra Agent on SNMP/UDP port 8085.

4.5 Cookies

Novarra WirelessWeb Server can be configured to host cookies for each device's session.

A cookie stores user information that a Web server can access. Typical uses are for shopping-cart applications or to store buying preference information. Most cookies have lifetimes associated with them. The Novarra WirelessWeb Server can handle cookies that have no specified lifetime, or that have specified lifetimes which may or may not be longer than the length of the device's browsing session.

The Novarra Management Console can be used to control:

- the length of a device's browsing session;
- whether or not WirelessWeb Server handles cookies;
- whether or not longer-lived cookies are persisted to the server's disk;
- the maximum number of cookies each device is allowed to have stored by the WirelessWeb Server.

4.5.1 Browser Session Length

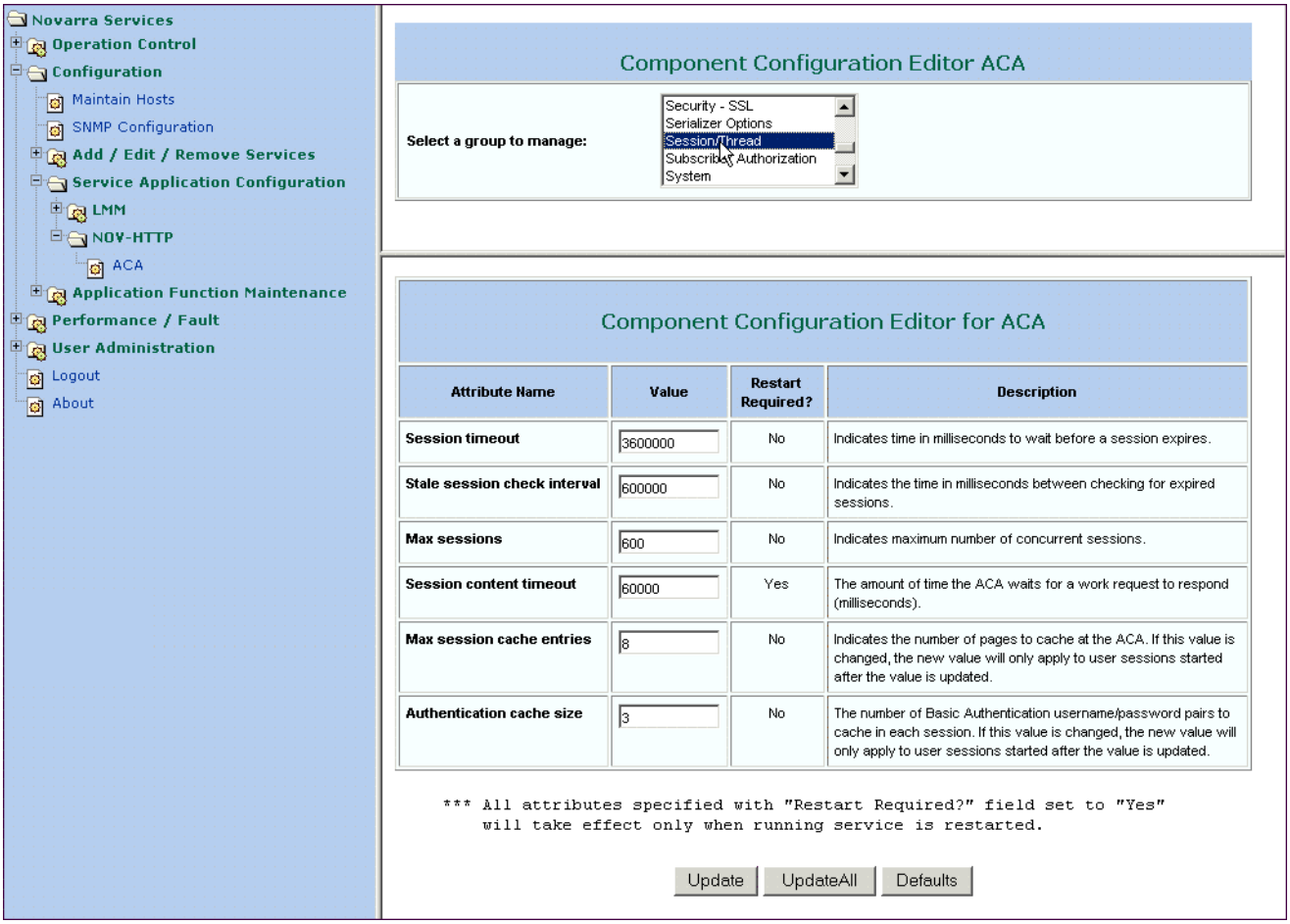
A Novarra browsing session for a given device starts when a user begins using the device's microBrowser and ends when that device's microBrowser is inactive for a predefined length of time.

Note:

The length of a device's session affects not only cookie storage but other aspects of the browsing experience, such as folderization and history storage.

To set the session timeout, perform the following steps:

1. Navigate to the **Component Configuration Editor for ACA** for any of the services. (Example: NOV-HTTP):
   Configuration→Service Application Configuration→NOV-HTTP→ACA
2. Click on **Session/Thread** in the **Select a group to manage:** box. The configuration editor appears in the bottom frame.



3. You can configure the session's timeout value by the **Session timeout** attribute. The value is stored in milliseconds, so 60000 would be one minute. The recommended length for timing out is one hour, or 3600000 milliseconds.
4. Other attributes that can be edited are in the left-hand column and their descriptions are found in the right-hand column. Make the appropriate changes and click the Update button. The bottom frame displays the message "Information for component "ACA" has been successfully updated and sent to the host."

Note:

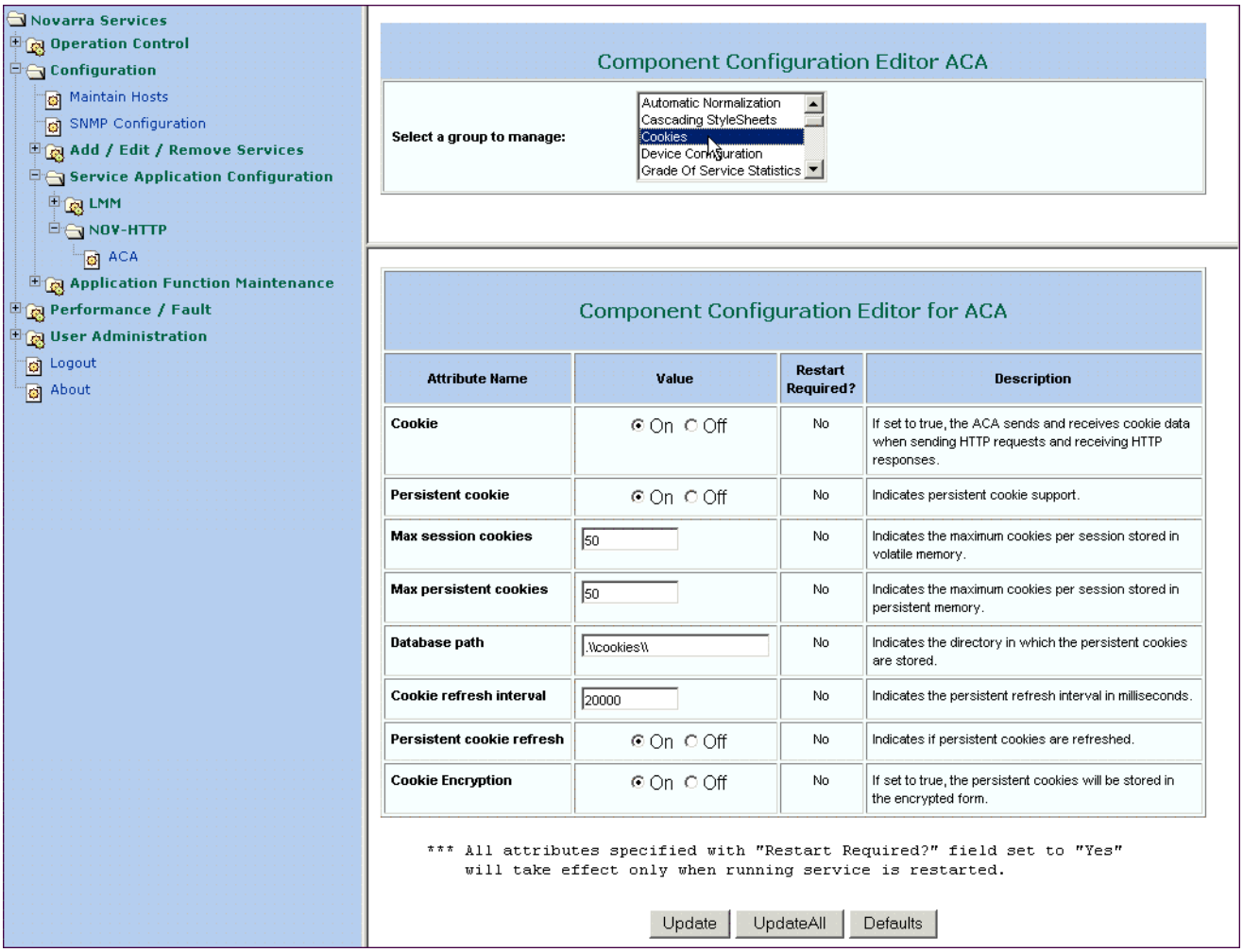
All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

5. Restart the service (see section 3.2.3.2, "Start/Stop NOV-HTTP" on page 3-9.)

4.5.2 Cookie Support

1. Navigate to the **Component Configuration Editor for ACA** for any of the services. (Example: NOV-HTTP):

   Configuration→Service Application Configuration→NOV-HTTP→ACA
2. Click on **Cookies** in the **Select a group to manage:** box. The configuration editor for cookies appears in the bottom frame.



3. The attributes that can be edited are in the left-hand column and their descriptions are found in the right-hand column:

   Cookie - Enables cookie support when set to On.

   Persistent cookie - A WirelessWeb Server cookie is persistent when the lifetime specified by the internet web server which creates it is longer than the length of the browser session as specified above. Cookies that outlast their session may be persisted to disk by setting Persistent cookie to On.

   Max session cookies - The number of short-lived (session) cookies allowed per device by the Novarra WirelessWeb Server may be specified by changing the "Max session cookies" attribute.

   Max persistent cookies - The number of long-lived (persistent) cookies allowed per device by the Novarra WirelessWeb Server may be specified by changing the "Max persistent cookies" attribute.

   Database path - The operator may change the location of persistent cookie storage relative to the <WirelessWebLocation>\config directory by changing the Database path.

Cookie refresh interval - A background task which will periodically write all cookies that should be persisted to disk (in case of ACA shutdown). The interval that this task operates within may be controlled with the "Cookie refresh interval" attribute**.**

Persistent cookie refresh - Refreshes persistent cookies when set to On.

4. Make the appropriate changes and click the Update button. The bottom frame displays the message “Information for component "ACA" has been successfully updated and sent to the host.”

Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

5. Restart the service (see section 3.2.3.2, “Start/Stop NOV-HTTP” on page 3-9.)

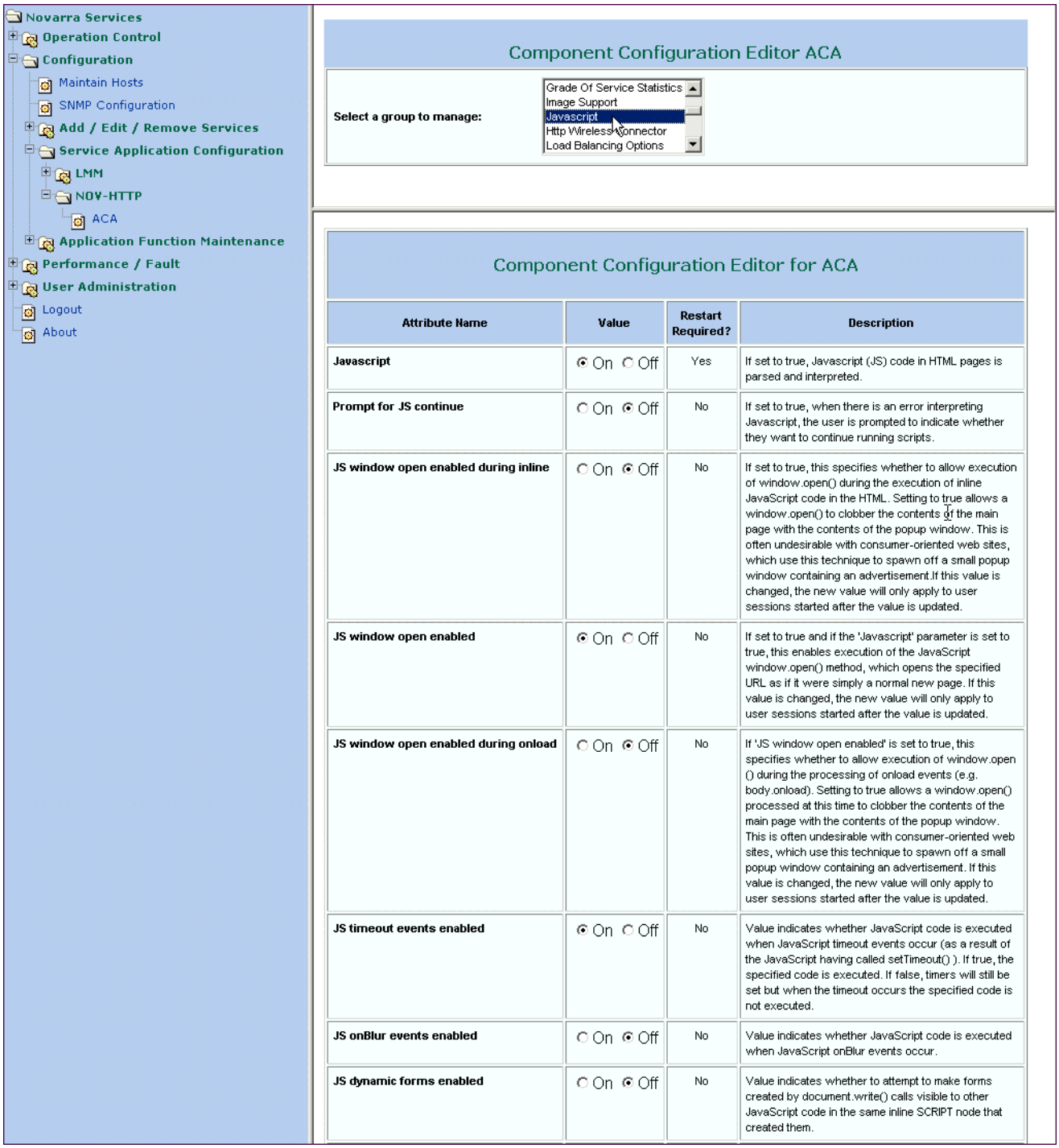
4.6 JavaScript Administration

Novarra WirelessWeb Enterprise Suite supports JavaScript 1.3 and exposes the most commonly used browser (DOM) JavaScript extensions.

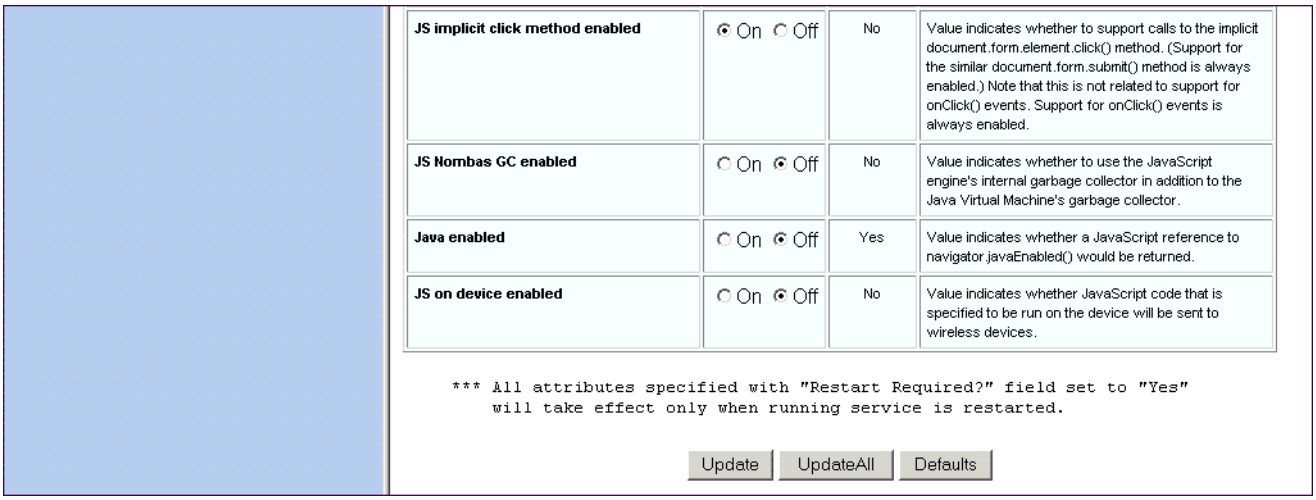
1. Navigate to the **Component Configuration Editor for ACA** for any of the services. (Example: NOV-HTTP):

   Configuration→Service Application Configuration→NOV-HTTP→ACA

2. Click on **Javascript** in the **Select a group to manage:** box. The configuration editor for Javascript appears in the bottom frame.



(Screen shot continued on next page)



Note:

The user can also disable scripting by configuring the properties of WirelessWeb microBrowser.

3. To select how the server will handle any scripting errors it encounters, set the attribute **Prompt for JS continue** to On. The user is notified that there is a scripting error and asked if it is OK to continue running scripts on the page. Set the value to Off to disable all of the scripts on the page if there is a JavaScript error.

Warning:

Be aware that you can turn off JavaScript processing both at the server and browser levels. Make sure scripting is enabled before testing.

4. Other attributes that can be edited are in the left-hand column and their descriptions are found in the right-hand column. Make the appropriate changes and click the Update button. The bottom frame displays the message “Information for component "ACA" has been successfully updated and sent to the host.”

Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

5. Restart the service (see section 3.2.3.2, “Start/Stop NOV-HTTP” on page 3-9.)

4.6.1 Controlling window.open() Calls

The JavaScript method `window.open()` launches a URL in another window on a desktop browser. It is commonly used for "popup" windows that contain help screens, advertisements, or related information.

Given the nature of the screens on handheld devices, it is not practical to open a new browser window. Hence, WirelessWeb microBrowser treats these popup windows almost as if they were hyperlinks. For example, picture a Web page that opens a popup window when you click on a hyperlink. When you view that page in microBrowser, it behaves precisely as if you followed an ordinary hyperlink—the current page exits, and the new page opens.

Web developers also frequently call `window.open()` when a page first loads. Therefore, users may confuse the popup window with the page they intended to load. Since popup windows can be intrusive and since the user cannot distinguish between a secondary window and the main browser on a wireless device, you may want to consider limiting their use.

1. Navigate to the **Component Configuration Editor for ACA** for any of the services. (Example: NOV-HTTP):

   Configuration→Service Application Configuration→NOV-HTTP→ACA
2. Click on **Javascript** in the **Select a group to manage:** box. The configuration editor for Javascript appears in the bottom frame.
3. To turn on the overall functionality, set the attribute **JS window open enabled** to On.
4. To prevent popup windows from automatically opening when the `onLoad` event of the page fires, set the attribute **JS window open enabled during onload** to Off. The advantage of disabling them is that many Web sites use this technique to open third-party ads, and the customer may never see original the page on a wireless device. To allow the new page to be displayed, set the value to On.
5. Finally, you can specify whether popup windows open when they are found in a `SCRIPT` tag that is outside of a function, and therefore executed when the page is first loaded. Set the attribute **JS window open enabled during inline** to On to allow the page to open in microBrowser:
6. Click the Update button. The bottom frame displays the message "Information for component "ACA" has been successfully updated and sent to the host."

Note:

All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

7. Restart the service (see section 3.2.3.2, “Start/Stop NOV-HTTP” on page 3-9.)

Glossary

A

A

Adaptive Content Accelerator (ACA) A Novarra Wireless Web Server component that performs real-time adaptation of web content for optimal presentation on wireless devices.

agent A program that performs some information gathering or processing task in the background. Typically, an agent is given a very small and well-defined task.

Application Program Interface (API) A set of routines, protocols, and tools for building software applications.

Application Service Provider (ASP) A third-party entity that manages and distributes software-based services and solutions to customers across a wide area network from a central data center.

attribute A part of an element that provides additional information about that element. Defines a characteristic or specifies a value within an HTML tag. For instance, attributes of the HTML body tag determine specifics of the appearance of the page body, such as background color and text color.

B

batch file A file that contains a sequence, or batch, of commands that are executed together.

bit The smallest unit of information on a machine. A single bit can hold only one of two values: 0 or 1.

browser Short for Web browser, a software application used to find and display Web pages.

byte A unit of storage capable of holding a single character. A byte is equal to 8 bits.

C

call To invoke a routine in a programming language. Calling a routine consists of specifying the routine name and, optionally, parameters.

Cascading Style Sheets (CSS) A simple style sheet mechanism that allows authors and readers to attach style (e.g. fonts, colors and spacing) to HTML documents. The Cascading Style Sheet language expresses style in common desktop publishing terminology.

cHTML Compact HyperText Markup Language. A specification for a restricted subset of HTML.

cluster A group of servers that the Novarra WirelessWeb Server has been distributed over. A cluster always has at least one of the servers running the Novarra management application within the Tomcat web server.

Code Division Multiple Access (CDMA) A digital cellular technology that uses spread-spectrum techniques.

COM port The name of a serial communications port (e.g. COM1, COM2 etc.).

compact disc (CD) A polycarbonate with one or more metal layers capable of storing digital information.

configure To set up a program or computer system for a particular application.

cookies Cookies are pieces of web server generated information embedded in HTML and stored for future access. The information flows back and forth between the user and the servers. Cookies allow user-side customization of web information.

Customer Relationship Management (CRM)

CRM entails all aspects of interaction a company has with its customer, whether it be sales or service related.

D

Device Manager (DM) A Novarra Wireless Web Server connectivity component controlling delivery of messages to devices to a particular network, including encryption and device authentication.

Digital Certificate An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Document Object Model (DOM) A specification for representing the elements of a hierarchical entity such as a web page. Attributes and rules for each component are governed by the DTD.

Document Type Definition (DTD) A definition of the permissible attribute name and value pairs for components of a DOM.

E

Elliptic Curve Cryptography (ECC) A high performance encryption algorithm owned by Certicom.

encryption A form of cryptography that uses a mathematical algorithm to scramble data for security purposes.

Extensible Markup Language (XML) A generic language format developed by the W3C and used for representing a DOM. Specific examples of XML include xHTML, cHTML and WML.

F

firewall A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

flash memory A special type of electrically erasable programmable read-only memory (EEPROM) that can be erased and reprogrammed in blocks instead of one byte at a time.

folder A means of organizing the content in a web page into a hierarchy. The result is that it is optimized for display on a small screen.

forms Part of a web document containing user input fields such as text entry, selection fields or buttons.

frames A feature supported by most modern Web browsers than enables the Web author to divide the browser display area into two or more sections (frames). The contents of each frame are taken from a different Web page.

G

gateway In networking, a combination of hardware and software that links two different types of networks.

gigabyte (GB) One gigabyte is equal to 1,024 megabytes

Global System for Mobile Communications (GSM) A digital cellular systems that uses narrowband TDMA, which allows eight simultaneous calls on the same radio frequency.

Graphic User Interface (GUI) A program interface that uses a computer's graphics capabilities to make the program easier to use.

H

host A computer that is connected to a TCP/IP network, including the Internet. Each host has a unique IP address.

HyperText Markup Language (HTML) The authoring language used to create documents on the World Wide Web. HTML defines the structure and layout of a Web document by using a variety of tags and attributes.

HyperText Transfer Protocol (HTTP) The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

I

Internet Protocol address (IP address) An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The IP address format is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

Internet Protocol (IP) Protocol that specifies the format of packets, also called datagrams, and the addressing scheme.

J

Java A programming language.

Java Management Extensions (JMX) Sun's Java management technology which encompasses architecture, design patterns, services, and APIs for application and network management in the Java programming language.

JavaBeans A specification developed by Sun Microsystems that defines how Java objects interact. An object that conforms to this specification is called a JavaBean, and is similar to an ActiveX control. It can be used by any application that understands the JavaBeans format.

JavaScript A scripting language developed by Netscape to enable Web authors to design interactive sites. Javascript can interact with HTML source code.

Java Run-Time Environment (JRE) An application or set of applications comprising a JVM and native libraries that enables the execution of applications written in Java.

Java Server Pages (JSP) A presentation layer technology that allows static Web content to be mixed with Java code in a single server page.

Java Virtual Machine (JVM) An interpreter for executing applications written in Java.

K

kilobyte (KB) When used to describe data storage, KB usually represents 1,024 bytes. When used to describe data transfer rates, KB represents 1,000 bytes.

L

link In hypertext systems, such as the World Wide Web, a link is a reference to another document. Sometimes called hot links because they take you to other document when you click on them.

Local Area Network (LAN) A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings.

Login To make a computer system or network recognize you so that you can begin a session. You usually need to enter a username and password before the computer system will allow you to execute programs.

Logging /Monitoring Module (LMM) A Novarra Wireless Web Server component that enables user-defined filtering and that logs/

monitors all run-time events generated by various components of the Novarra Wireless Web Server.

M

megabyte (MB) When used to describe data storage, MB usually represents 1,048,576 bytes. When used to describe data transfer rates, MB represents 1,000,000 bytes.

megahertz (MHz) One MHz represents one million cycles per second.

Management Information Base (MIB) A database of objects that can be monitored by a network management system.

microBrowser A software application used to locate and display Web pages on wireless handheld devices.

microGateway A Novarra application residing on wireless devices that manages cached documents and controls communications between the microBrowser and the wireless network.

N

normalization The process of adapting XML/HTML content for display on handheld devices and to provide the end user with a more efficient/concise browsing experience.

The Normalization process utilizes the presentation characteristics of the content to derive the contextual relationships of the text, links and input elements. The content is then partitioned into "folders" based on the information.

O

Operating System (O/S) The most important program that runs on a computer. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Operating systems provide a software platform on top of which other programs, called application programs, can run. The application programs must be written to run on top of a particular operating system.

P

packet A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Packet Internet Groper (PING) A utility to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

parameter A characteristic. For example, specifying parameters means defining the characteristics of something. In general, parameters are used to customize a program. In programming, the term parameter is synonymous with argument, a value that is passed to a routine.

Personal Communications Service (PCS)

Term used to describe a set of digital cellular technologies used in the United States. PCS works over CDMA, GSM, and North American TDMA air interfaces.

Personal Digital Assistant (PDA) A handheld device that combines computing, telephone/fax, and networking features. A typical PDA can function as a cellular phone, fax sender, and personal organizer.

port An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

protocol An agreed-upon format for transmitting data between two devices. The protocol determines the following:

- the type of error checking to be used

- data compression method, if any
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message

proxy server A server that sits between a client application, such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

R

Radio Frequency (RF) Any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

Random Access Memory (RAM) A type of computer memory that can be accessed randomly (any byte of memory can be accessed without touching the preceding bytes).

root directory (root) Top level directory in a directory hierarchy.

S

Secure Sockets Layer (SSL) A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

server A computer or device on a network that manages network resources. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks.

Simple Network Management Protocol (SNMP) A set of protocols for managing complex networks.

Standard Generalized Markup Language (SGML) A system for organizing and tagging elements of a document. SGML itself does not specify any particular formatting; rather, it specifies the rules for tagging elements. These tags can then be interpreted to format elements in different ways.

System Monitor (Sysmon) A Novarra Wireless Web server application that starts, controls and monitors the Novarra services.

T

tag A name specifying a particular element in an XML or HTML document. The name identifies the type of element and determines how it should be interpreted by applications such as browsers.

text editor A program that enables you to create and edit text files. There are many different types of editors, but they all fall into two general categories:

- **line editors**: A primitive form of editor that requires you to specify a specific line of text before you can make changes to it.
- **screen -oriented editors**: Also called full-screen editors, these editors enable you to modify any text that appears on the display screen by moving the cursor to the desired location.

threshold A limit on a particular parameter. In the Novarra ACA, thresholds can be set to govern behavior such as the amount of content that will be nested inside folders or whether folder content should be withheld until explicitly requested by a user.

tier One of a series of folders (objects that can contain multiple documents) placed one above another.

Time Division Multiple Access (TDMA) A technology for delivering digital wireless service using time division multiplexing (TDM).

Time Division Multiplexing (TDM) A type of multiplexing that combines data streams by assigning each stream a different time slot in a set. TDM repeatedly transmits a fixed sequence of time slots over a single transmission channel.

track wheel A feature on some handheld devices that allows the user to scroll through and select different applications or user interface elements.

Transmission Control Protocol/Internet Protocol (TCP/IP) The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

Transmission Control Protocol (TCP) TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

U

Uniform Resource Locator (URL) The global address of documents and other resources on the World Wide Web.

User Datagram Protocol (UDP) A connectionless protocol that, like TCP, runs on top of IP networks.

W

Web browser A software application used to locate and display Web pages.

Wide Area Network (WAN) A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local area networks (LANs).

Win32 The Windows application program interface for developing 32-bit applications.

Wireless Application Protocol (WAP) A standardized, device-independent protocol that defines the development and operating environment for wireless telephones, pagers and handheld devices. WAP utilizes a lighter version of the TCP/IP protocol for transmission between devices.

Wireless Connectivity Manager (WCM) A Novarra Wireless Web Server component that manages wireless sessions, protocols and content transmission for efficient and secure communication with wireless devices.

Wireless Markup Language (WML) An XML language used to specify content and user interface for Wireless Application Protocol (WAP) devices.

WirelessWeb Enterprise Suite (WWES)

Novarra WirelessWeb Enterprise Suite offers a complete solution that adapts enterprise applications to handheld devices, manages wireless connectivity and delivers end-to-end security.

WirelessWeb microBrowser See “microBrowser” .

WirelessWeb Server (WWS) The Novarra WirelessWeb Server has two main components: Adaptive Content Accelerator and Wireless Connectivity Manager.

World Wide Web Consortium (W3C) An international consortium of companies involved with the Internet and the Web. The organization's purpose is to develop open standards so that the Web evolves in a single direction rather than being splintered among competing factions. The W3C is the chief standards body for HTTP and HTML.

X

xHTML A specification of HTML that conforms to XML standards.

xHTML Basic A restricted subset of xHTML.

XML See “Extensible Markup Language (XML)”

Troubleshooting Wireless Web Server

B

There are four main troubleshooting tools for the Novarra WirelessWeb Server:

Message traces are especially useful for verifying network connectivity. Since certain networks (CDPD, Palm.Net, and WAP) do not establish a persistent connection, observing message traces and making sure no alerts are present provide the only way to check that the system is running properly. For more information on specific alerts, message traces, and installation problems, refer to the following sections.

B.1 Logging and Monitoring Module

The Logging and Monitoring Module (LMM) service provides flexible logging configuration of the LMM server and dynamic filtering of logging output via the Log Client Console. Currently, only ACA logging events are handled via the LMM service; see section B.2 through section B.4 for details on retrieving logging and message traces for the other components of the WirelessWeb Server.

Central to the LMM design is the idea of a filter. The filters specify what logging events should be seen by a client of that filter, and where those logging events should go. In particular, each filter has associated with it two types of "what" attributes and one type of "where" attribute:

- Discriminant attributes ("what") -- these represent data fields within each log event which may serve as a criterion to view or not view the event.
- Trace attributes ("what") -- during content adaptation, there are key points (called tracepoints) at which useful information may be present for trace display. The trace attributes are on/off values which allow the LMM owner of the filter to indicate whether or not she is interested in

data dumps whenever that particular trace point is encountered during content adaptation.

- Destination attributes ("where") -- these attributes specify the host and port that the Log Client will use (in the case of a GUI filter), or the mail headers to use (in the case of a mail filter).

The "what" attributes can be changed at any time during the life of the filter. The "where" information can only be specified at filter creation time, and is discussed further in section B.1.2, “Other filter operations”.

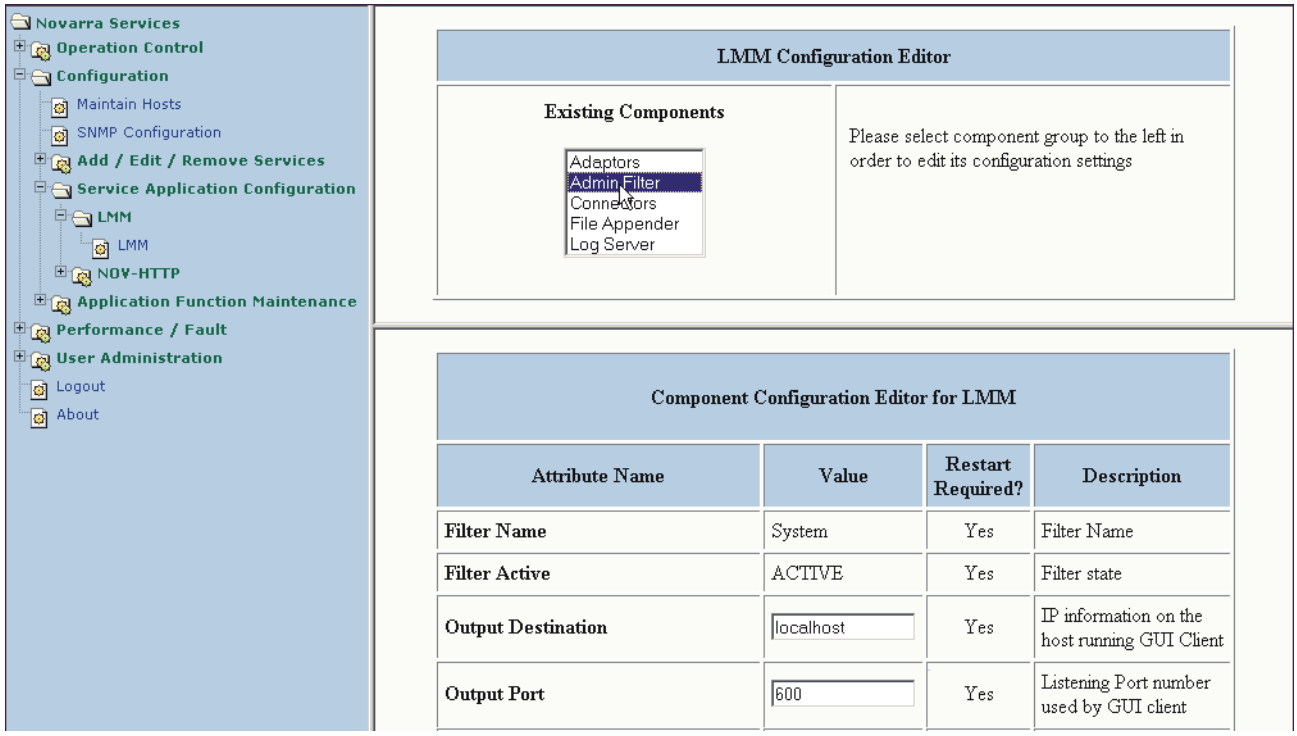
LMM supports a number of different users, each of whom may configure an arbitrary number of filters. The topics of adding or cloning filters associated with LMM users are also addressed in section B.1.2

To better understand the LMM concepts, it may be helpful to first step through the configuration of the default Admin filter.

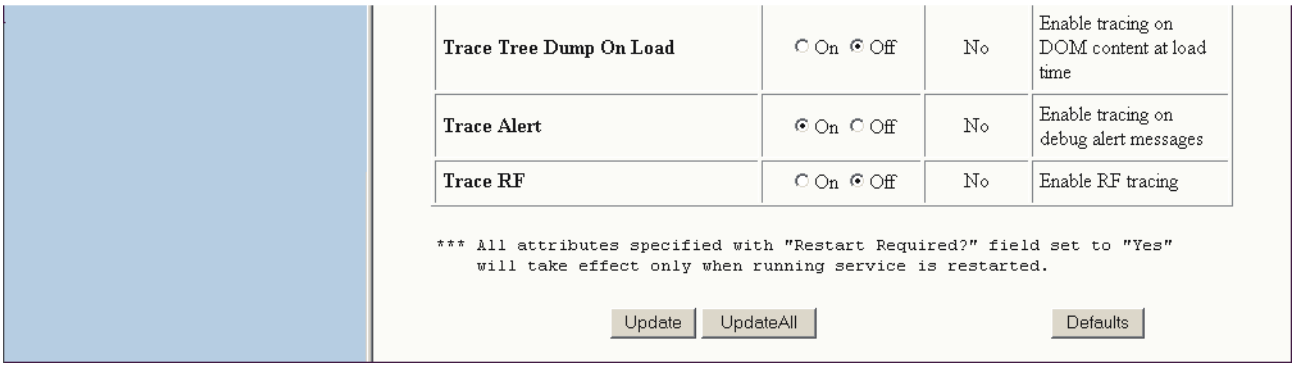
B.1.1 The Admin filter

The Novarra Management Console comes with a pre-configured Admin (System) LMM filter. This filter is owned by the **`admin`** user of the Management Console and cannot be deleted. This section gives a step-by-step description of how to set up the Log Client console for receiving output from the default Admin LMM filter.

1. Navigate to the **LMM Configuration Editor**.
   Configuration→Service Application Configuration→ LMM→LMM
2. Select the **ADMINFILTER** group in the **Existing Components** box.



Filter By Priority	INFO	No	Priority level of events
Filter By Network Id	ALL	No	Events with this NETWORK ID
Filter By Device Id		No	Events with this DEVICE ID
Filter By Class		No	Events generated from this class
Filter By ComponentId		No	Events generated from this component
Filter By URL		No	Events generated while handling this url
Filter By ACA Id		No	Sysmon Name given to ACA
Filter By Host		No	Filter on events from this Host
Trace System	○ On ◉ Off	No	Enable tracing on system parameters
Trace Events	◉ On ○ Off	No	Enable tracing on device event info
Trace Subscriber Authorization	◉ On ○ Off	No	Enable tracing on subscriber authorization info
Trace Session Management	◉ On ○ Off	No	Enable tracing on session management info
Trace Output Stream	○ On ◉ Off	No	Enable tracing on information written to device
Trace Cookies	◉ On ○ Off	No	Enable tracing on cookies' information
Trace Java Script	◉ On ○ Off	No	Enable tracing on JavaScript messages
Trace Request Headers	◉ On ○ Off	No	Enable tracing on incomming request headers' info
Trace Response Headers	◉ On ○ Off	No	Enable tracing on outgoing response headers' info
Trace Exception	◉ On ○ Off	No	Enable tracing on occured exceptions
Trace Norm Exception	◉ On ○ Off	No	Enable tracing on occured normalizer exceptions
Trace Tree Dump After Normalize	○ On ◉ Off	No	Enable tracing on DOM content after normalization
Trace Tree Dump Before Normalize	○ On ◉ Off	No	Enable tracing on a pre-normalized DOM content



3. Change any trace attributes that you want. Click the Update button.

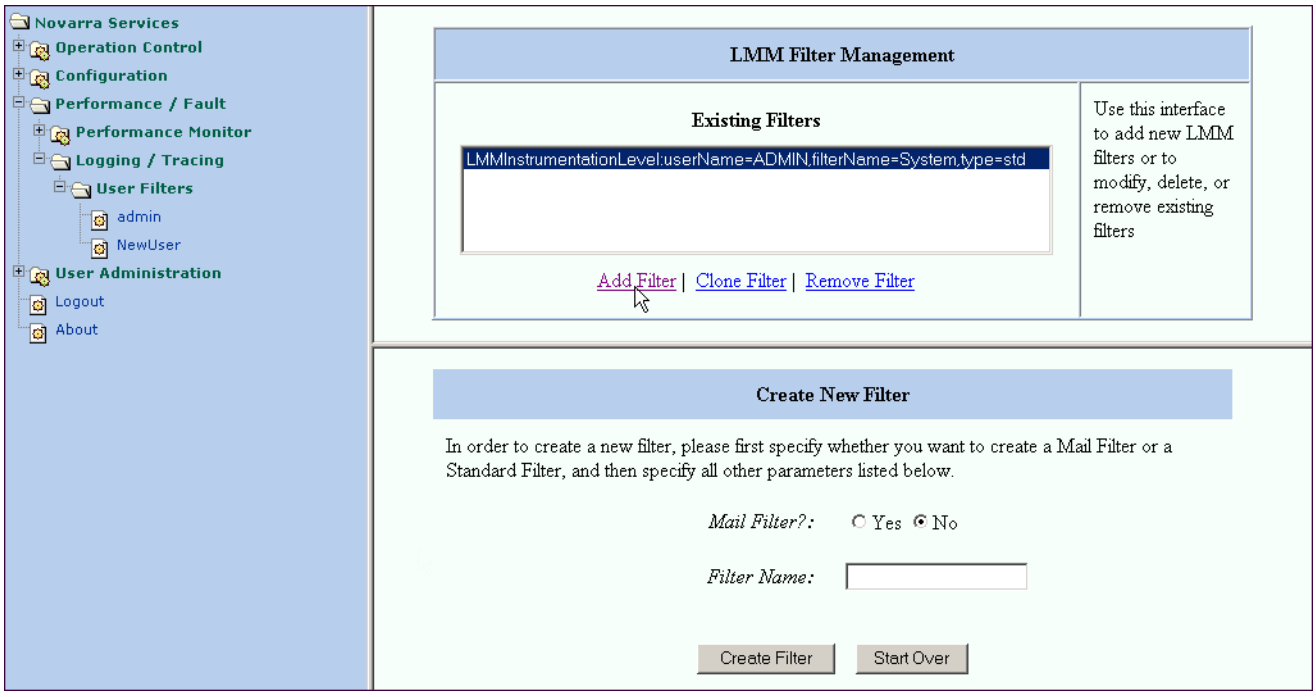
B.1.2 Other filter operations

Novarra Management Console users can add their own filters, or clone filters owned by either themselves or by someone else.

B.1.2.1 Add A Filter

To add a new filter while logged in as **`admin`**:

1. Navigate to the **LMM Filter Management**.
   Performance/Fault→Logging/Tracing→ User Filters→admin
2. Click the **Add Filter** link in the **LMM Filter Management** frame. The **Create New Filter** frame appears.



3. Each LMM filter has one destination associated with it either an e-mail destination for logging events, or a web-based logging client to receive those events.

- To specify an e-mail destination, click **Yes** for **Mail Filter?**, and then enter the e-mail header information.
- To specify a web-based logging client destination, click **No** for **Mail Filter?**, and then enter the new **Filter Name**.

4. Click on the Create Filter button to create the filter with default trace and discriminant attributes.
5. The filter now appears in the Existing Filters list.

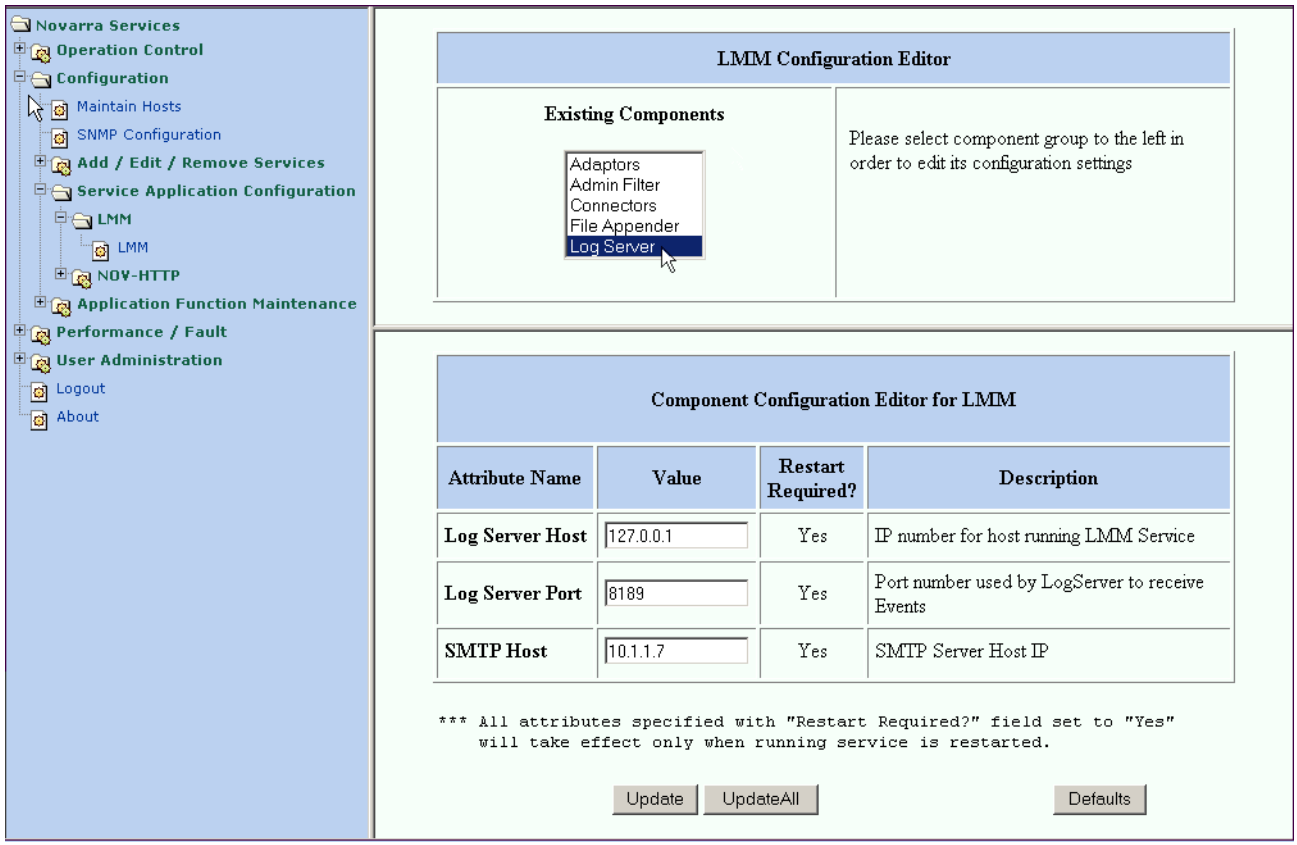
Note:

By default, a filter is off until connected to by a user.

B.1.2.2 Enter the SMTP Server

If you specified an e-mail destination, then you must enter the SMTP server where your LMM e-mail will be sent:

1. Navigate to **Configuration→Service Application Configuration→ LMM→LMM**
2. Select the **LOGSERVER** group in the **Existing Components** box.



3. Enter the SMTP server to use to send your LMM e-mail in the **SmtpHost** attribute. Click the Update button.

Note:

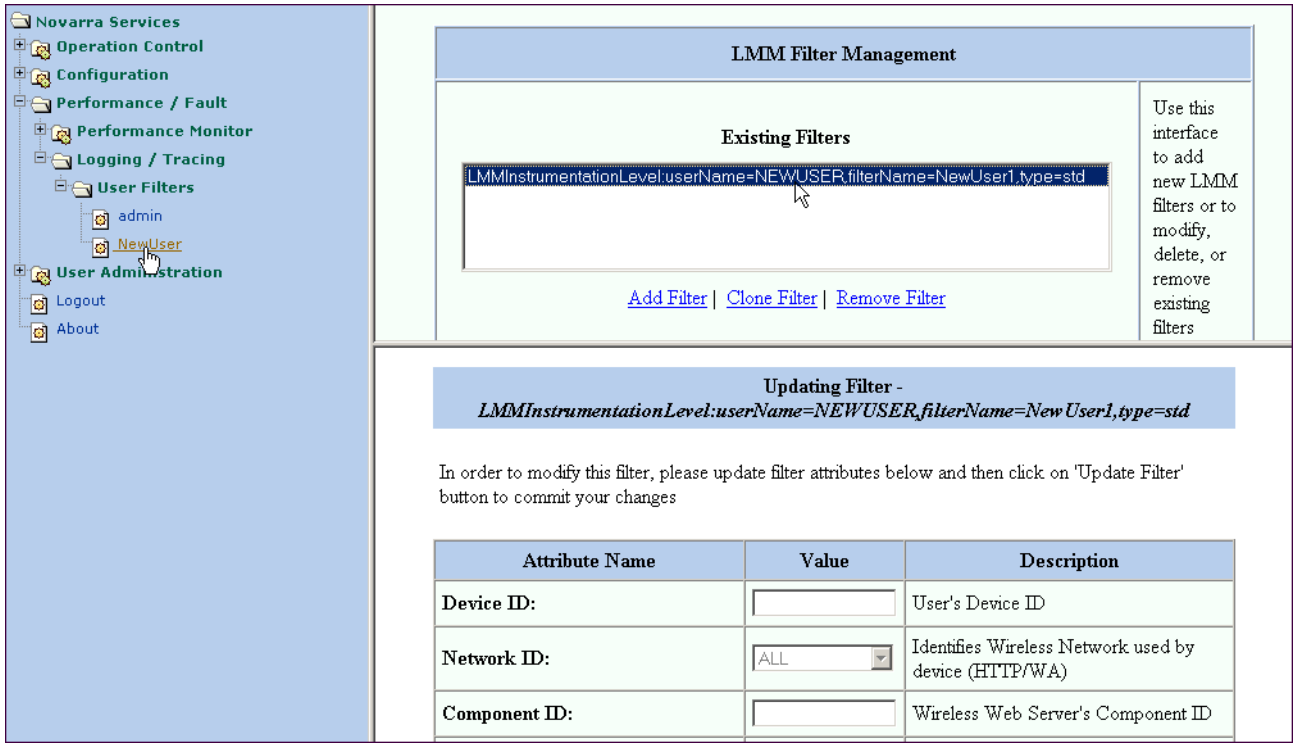
All attributes specified with "Restart Required?" field set to "Yes" will take effect only when running service is restarted.

4. Restart the LMM service

B.1.2.3 Clone A Filter

To clone a filter owned by another LMM user:

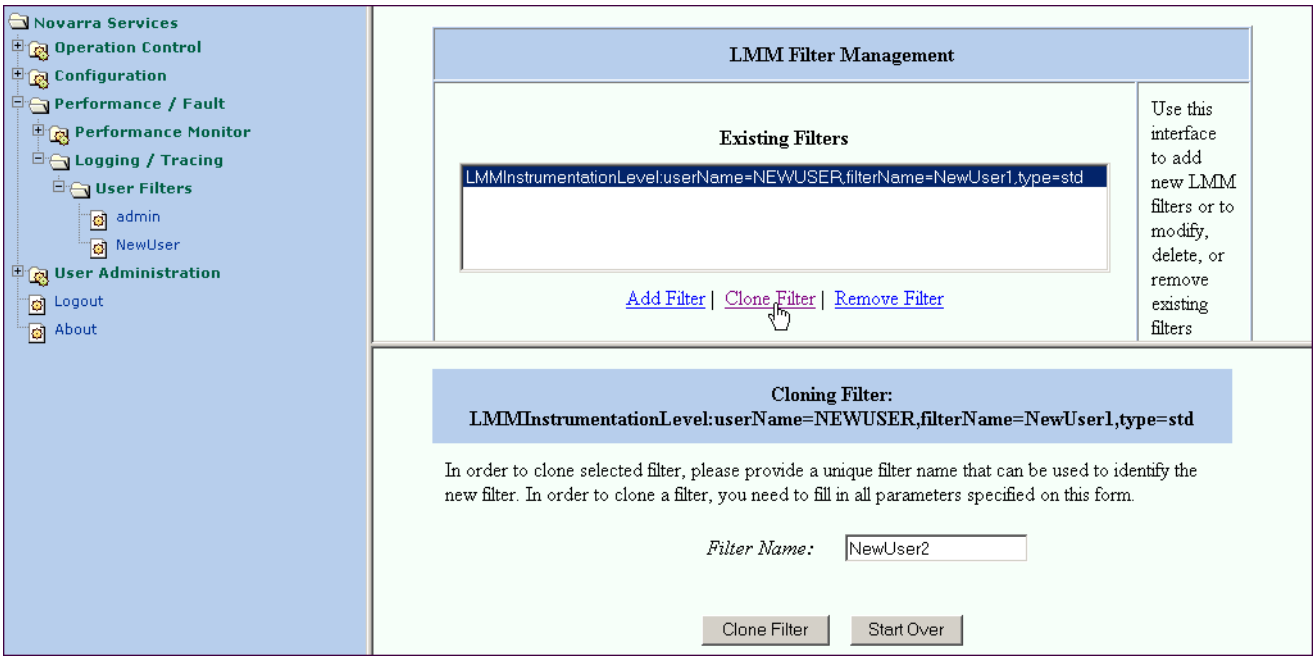
1. Navigate to the **LMM Filter Management**.
   Performance/Fault→Logging/Tracing→ User Filters→ <User's Name>
2. In the **Existing Filters** box, select the filter you want to clone. In the **Updating Filter** frame, you can review the attributes of this filter



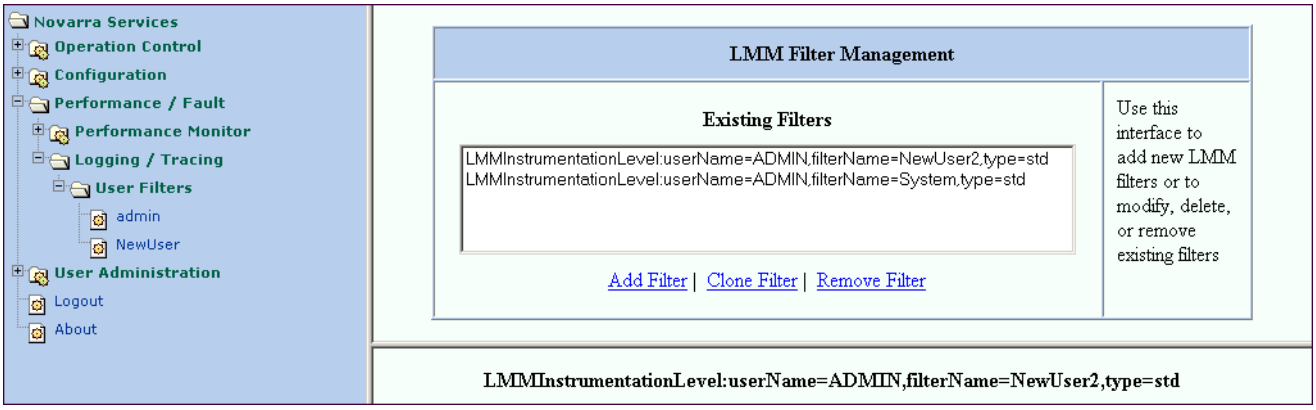
Note:

The Update button in the **Updating Filter** frame is not active (you are just viewing another LMM user's filter).

3. Click on **Clone Filter** link. The **Cloning Filter:** frame appears.



4. Enter the filter name.
5. Click the Clone Filter button. The **LMM Filter Management** frame displays the cloned filter in the current LMM user's **Existing Filters** box.



6. To change the attributes of the cloned filter, click on the filter's name in the **Existing Filters** box.
7. Make your changes and click the Update button.

Note:

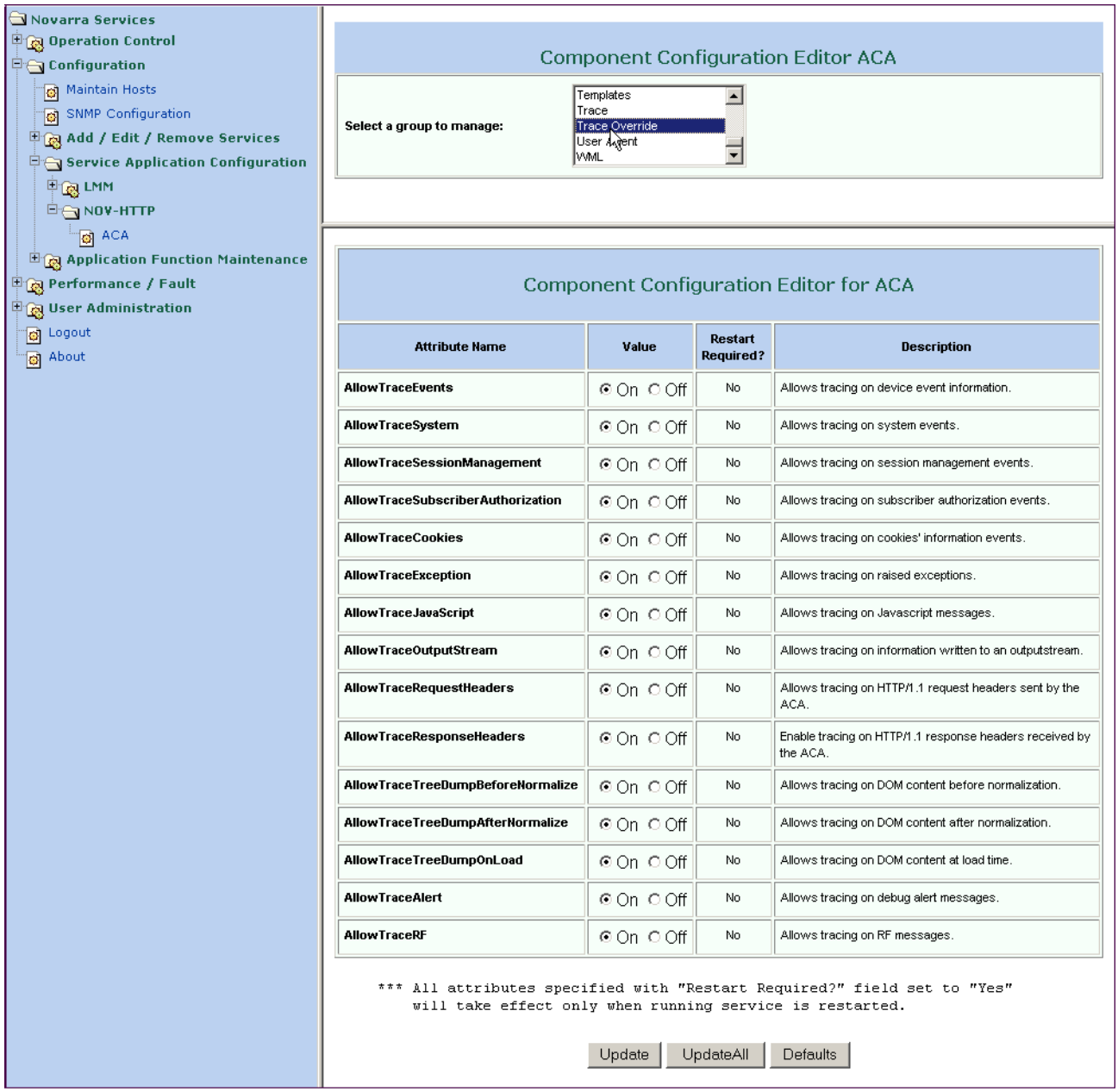
By default, a filter is off until connected to by a user.

B.1.2.4 Filter Overrides

The Novarra Management Console administrator account can override certain trace attributes at the ACA so that events of certain types are never generated by the ACA. This might be done for ACA performance reasons.

To override trace attributes when logged in as **`admin`**:

1. Navigate to the **Component Configuration Editor for ACA** for any of the services. (Example: HTTP):
   Configuration→Service Application Configuration→NOV-HTTP→ACA
2. Select **Trace Overrides** in the **Select a group to manage:** box. The **Component Configuration Editor for ACA** frame appears.

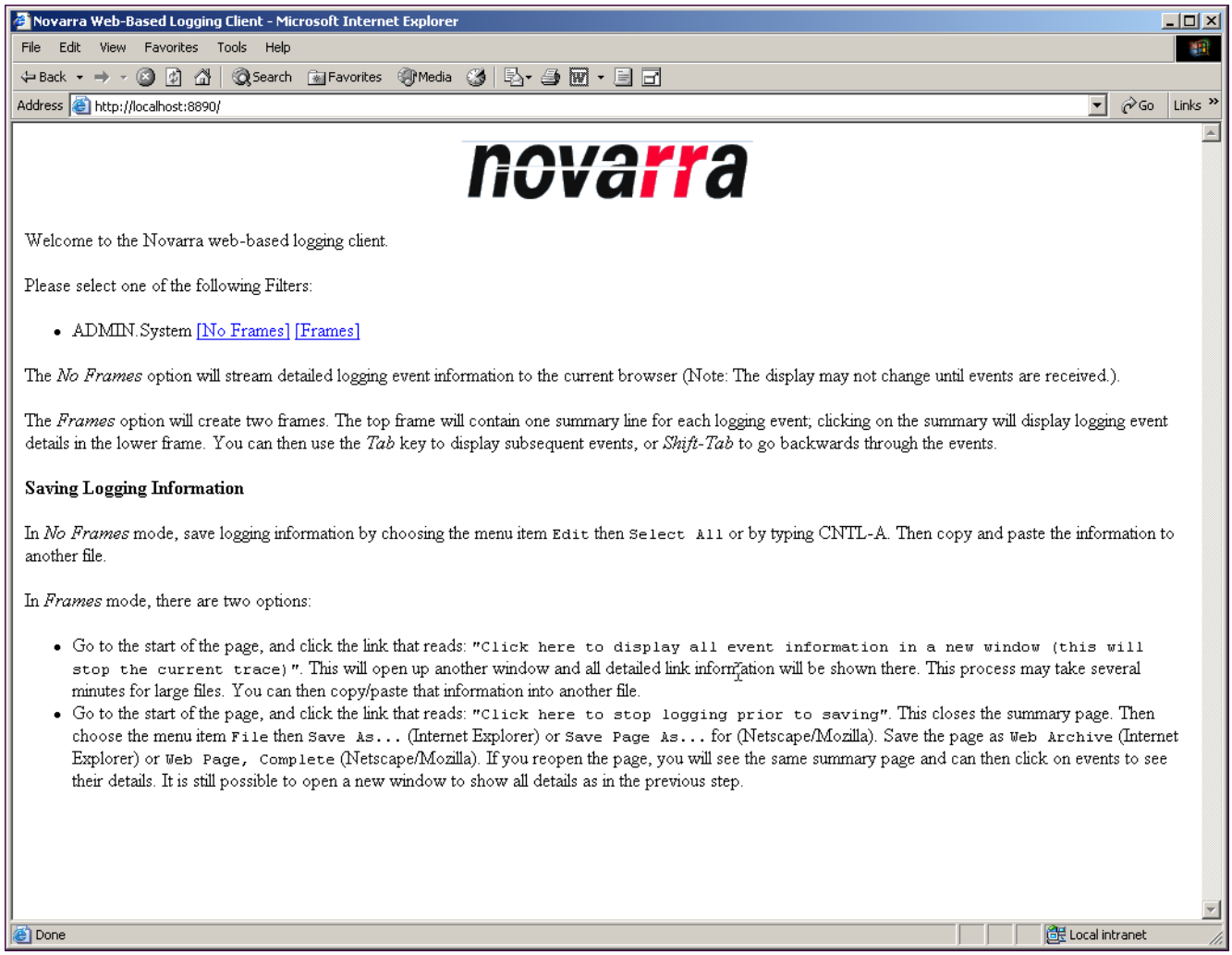


3. Select which trace attributes should never be logged by the ACA by clicking Off for that attribute.
4. Click the Update button to override the specified trace attributes at the ACA.

B.1.3 Using the LMM Log Client

Novarra provides a web-based client for viewing log messages. To access:

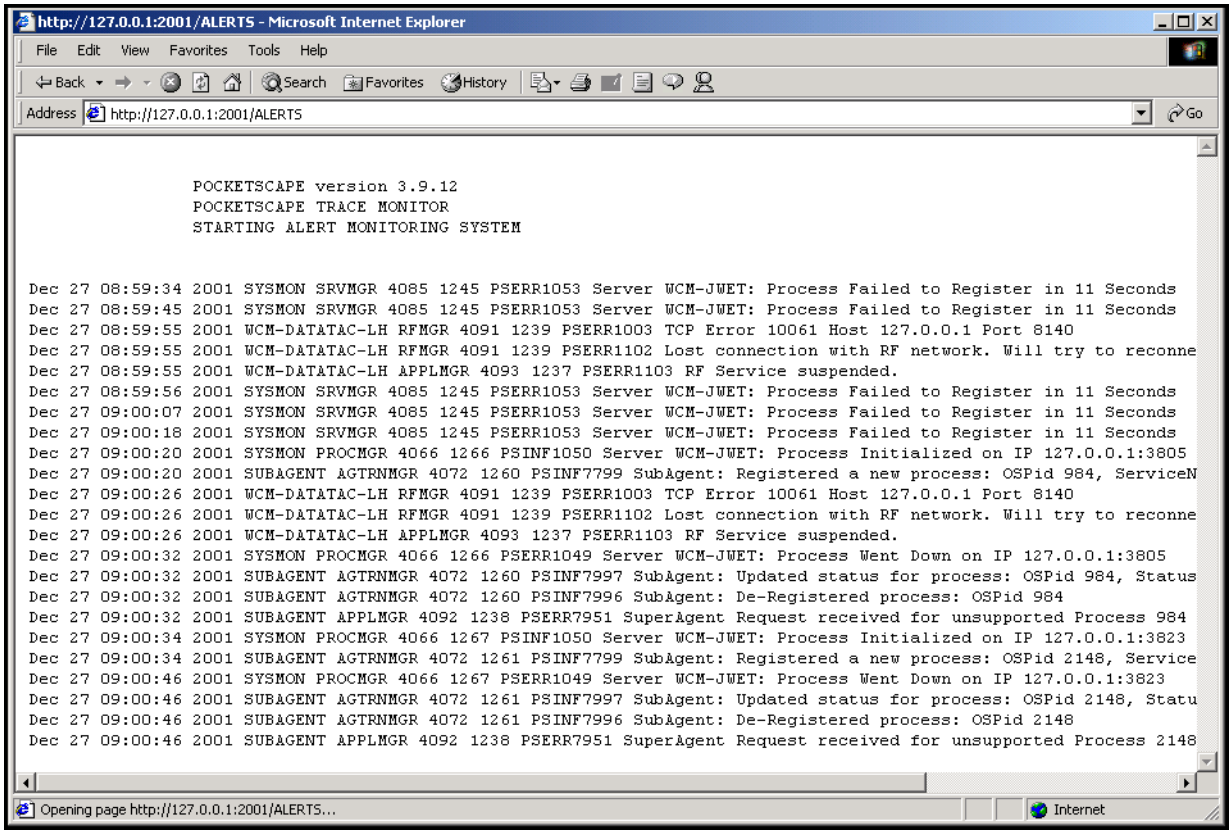
1. Point your browser to port 8890 on the Novarra Management server. An example URL is:
   `http://managementhost:8890`
   Where "managementhost" is the name (or IP Address) of the server hosting the Novarra Management console.
2. The initial browser screen appears. The initial page displays the logging filters that have been previously defined. Refer to "Logging/ Tracing" on page 3-40 for creating, updating and cloning filters.



3. Review the information on this screen and choose either the No Frames or Frames link for the filter you want to view.

B.2 Monitoring Alerts

To view host-wide WirelessWeb Server alerts, point a web browser to http://xxx.xxx.xxx.xxx:2001/ALERTS. Replace xxx.xxx.xxx.xxx with the IP address of the machine on which WirelessWeb Server is running. The port number must be 2001. Below is what the ALERTS screen should look like:



B.2.1 Certificates Expired or Never Installed

The following alert appears when attempting to load a page through Secure Sockets Layer (SSL):

```
HTTP response has no headers. URL was <URL>.
```

Meaning

SSL support has been enabled on the server, but the appropriate certificates have expired or have not been installed in the folder <WirelessWeb location>\config\trustedcerts.

This error also causes the following message to be displayed on WirelessWeb microBrowser:

```
We're sorry...HTTP response has no header. URL was <URL>.
```

Solution

Install the proper certificates as .cer files into the correct folder and restart Novarra WirelessWeb Server.

B.2.2 Certificates Never Installed

The following alert appears when attempting to load a page through Secure Sockets Layer (SSL):

```
Content server- could not find any trusted certificates at path:
'trustedcerts' relative to my working directory.  Disabling SSL.
```

Meaning

The certificates directory does not contain any certificate files.

This error also causes the following message to be displayed on WirelessWeb microBrowser:

```
We're sorry...unsupported protocol: https.  The only supported protocol is
http.
```

Solution

Install certificate files in <WirelessWeb Location>\config\trustedcerts and restart WirelessWeb Server.

B.2.3 Proxy Server Is Not Running

```
Content server <device id>: error.  Connection refused:  no further
information
```

Meaning

The proxy server is not operational or the IP address or port number specified for it in <WirelessWeb Location>\config\mm.conf is wrong. This is applicable only if you are using a proxy server.

This error also causes the following message to be displayed on WirelessWeb microBrowser:

```
We're sorry...could not connect to server. Please try again.
```

Solution

Verify that the proxy server is running and listening on the proper IP and port. The proxy server is configured as specified in section 4.3.1, “Proxy Server,” on page 4-14.

Another workaround is to reconfigure WirelessWeb Server so it does not go through the proxy server.

B.3 Monitoring RF Traces

In the event of problems, you can read the RF traces of the Device Manager and Line Handler to help troubleshoot the source. The output of the Line Handler (connection to the RF network) and the Device Manager (connection between the Adaptive Content Accelerator and the Line Handler) is visible through a browser.

To view the RF traces on another system, enter the correct URL in a Web browser, as described below:

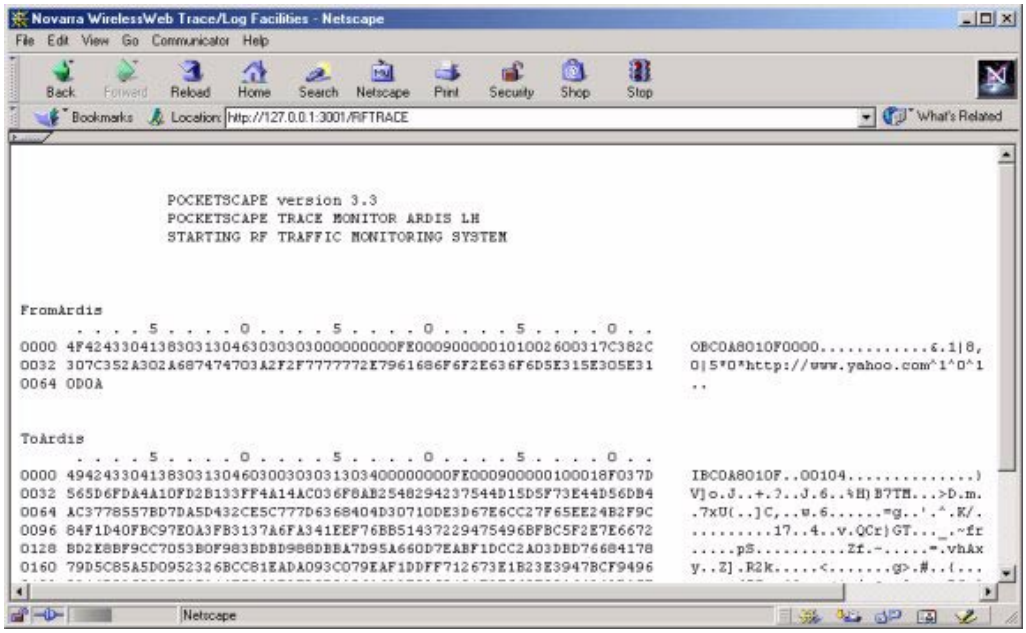
```
Image Server:                    http://xxx.xxx.xxx.xxx:3010/RFTRACE
HTTP Server:                     http://xxx.xxx.xxx.xxx:3011/RFTRACE
```

Note:

The actual IP address of WirelessWeb Server must be used in place of xxx.xxx.xxx.xxx to view RF traces.

The Device Manager RF trace contains the XML-based markup that is sent to the wireless network and then eventually on to the subscriber unit. The information in this trace contains the transformed content from the Adaptive Content Accelerator in a state that can be easily read.

The Line Handler RF trace also contains XML-based markup, which it receives from the Device Manager. However, through the Line Handler RF traces, the XML is compressed and cannot be easily read. This trace is used mainly to verify that content is being sent to the wireless network.



B.4 Troubleshooting WirelessWeb Server Installation

Chapter 2, "Installing Novarra WirelessWeb Enterprise Suite" detailed how to install the Novarra WirelessWeb Server and the Novarra Management Console for the WirelessWeb Server. Once these installations are complete, start both the WirelessWeb Server (on all installed hosts) and start the Tomcat JSP Engine (on the server machine which is hosting the Management Console installation).

To start the WirelessWeb Server, you must start two services on each host.

1. Start Novarra WirelessWeb:
   Start→Programs→Novarra WirelessWeb→Start Novarra WirelessWeb
2. Start Novarra Agent:
   Start→Programs→Novarra WirelessWeb→Start Novarra Agent

The Novarra WirelessWeb service is the core of the WirelessWeb Server installation and consists of a program called "SysMon" (for System Monitor). **`SysMon.exe`** is installed and runs as a Win32 service, and it is the executable that initiates all other WirelessWeb processes/components when so instructed by the operator of the Novarra Management Console. **`Sysmon.exe`** monitors these processes/components continually and ensures that they are always running (when the operator directs that they be run via the Management Console). The service name for **`SysMon.exe`** is **`NovarraSysMon`**.

The Novarra Agent service mediates requests between SysMon and the Management Console application. It consists of a program called **`Novarra_agent.exe`**, and its Win32 service name is **`NovarraStandaloneAgent`**.

To run the Management Console on the one server machine hosting it, you must start the JSP engine and then log into the console:

1. Start Tomcat JSP Engine:
   Start→Programs→Novarra Management Console→Start Tomcat JSP Engine
2. Login to Novarra Management Console:
   Start→Programs→Novarra Management Console→Management Console Login

The following sections give troubleshooting tips for installation problems associated with the Novarra Management Console, the Novarra Agent, and the Novarra SysMon service (which is called "WirelessWeb Server" in the start menus).

B.4.1 Troubleshooting Novarra Management Console Installation

If your Tomcat JSP engine installation is correct, then you will be able to successfully login to the Novarra Management Console. You can then proceed to the next step (see section B.4.2, “Troubleshooting Novarra Agent Installation” on page B-20).

B.4.1.1 Check Installation of Tomcat JSP Engine

If you receive an HTTP 404 error while attempting to log in, you will need to check the installation of the Tomcat JSP Engine on the server hosting it.

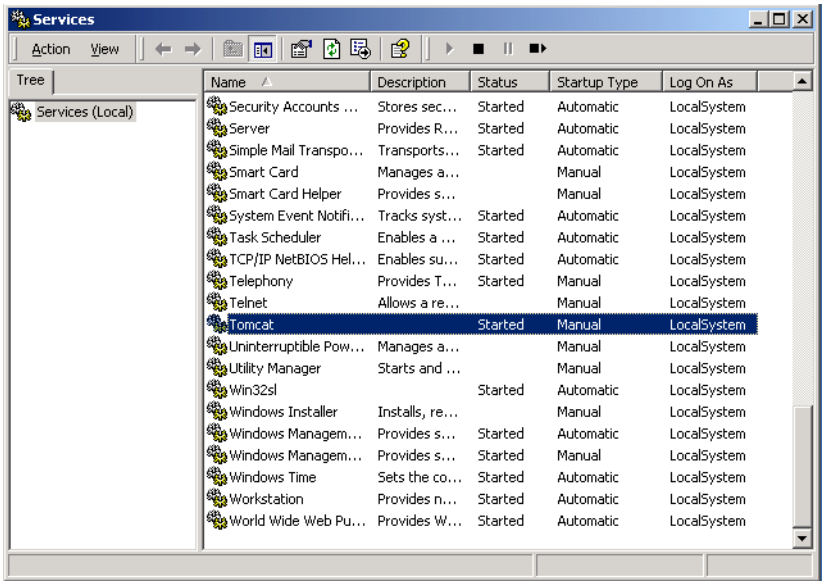
1. Go to that host and make sure that Tomcat is properly configured in the Service Control Manager (SCM) for that host.

   - To open the SCM on Windows 2000:

   Start→Settings→Control Panel→Administrative Tools→Services

   - To open the SCM on Windows NT 4.0:

   Start→Settings→Control Panel→Services
2. Scroll down the list of services and search for **Tomcat**.



- If **Tomcat** appears in the Service Control Manager, see section B.4.1.1.1, “Tomcat Appears in the Service Control Manager” on page B-15.
- If **Tomcat** does not appear in the Service Control Manager, see section B.4.1.1.2, “Tomcat Does Not Appear in the Service Control Manager” on page B-15.

B.4.1.1.1 Tomcat Appears in the Service Control Manager

If Tomcat appears in the SCM, it should show up as "Manual" and "Started". If it does not show up as "Started", then start it by with either of the following methods:

- Start→Programs→Novarra Management Console→Start Tomcat JSP Engine
- Right-click on **Tomcat** in the SCM and select **Start** in the pull down.

B.4.1.1.1.1 Tomcat Appears to Start

If Tomcat appears to have started, try logging in again.

B.4.1.1.1.2 Tomcat Fails to Start

If the Tomcat service fails to start by either of these means, then the two most probable causes are:

- Incorrect pre-existing installation of Tomcat.

Note:

It is beyond the scope of this document to verify a pre-existing installation of Tomcat (if Tomcat was not installed by the Novarra Management Console installation). Refer to http://jakarta.apache.org/site/faqs.html for installation/debugging tips.

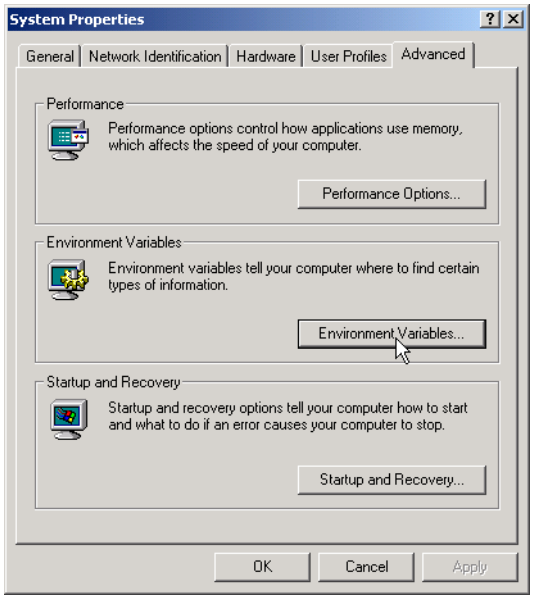
- Improper registry settings. Follow the steps in "Checking the Registry Setting for Tomcat" on page B-19.

B.4.1.1.2 Tomcat Does Not Appear in the Service Control Manager

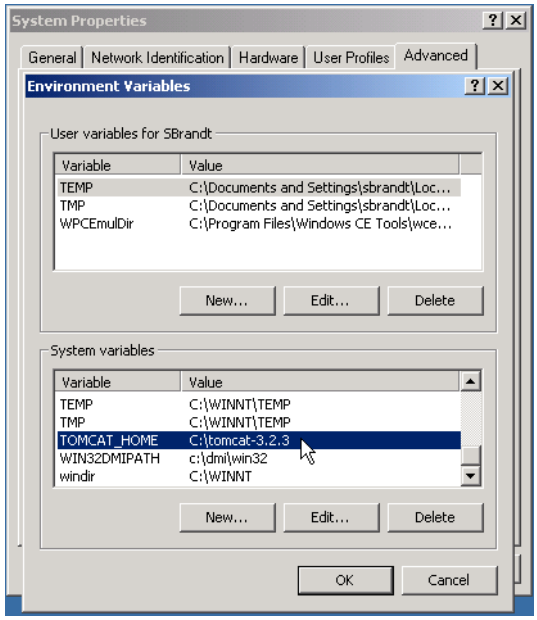
If Tomcat does not appear in the SCM, then the installation of Tomcat should be checked.

1. Open the System Properties panel:
   Start→Settings→Control Panel→System
2. Click the Advanced tab.

3. Click on Environment Variables…



4. In System variables, look for **TOMCAT_HOME**.



B.4.1.1.2.1 TOMCAT_HOME Does Not Appear in the System Variable List

If **TOMCAT_HOME** does not appear in the System variables list, then Tomcat is improperly installed.

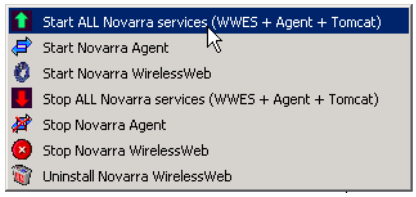
Note:

It is beyond the scope of this document to verify a pre-existing installation of Tomcat (if Tomcat was not installed by the Novarra Management Console installation). Refer to http://jakarta.apache.org/site/faqs.html for installation/debugging tips.

If you did not have Tomcat previously installed, then the original Management Console installation may not have been allowed to complete the Tomcat installation. To check this possibility, uninstall your current installation of the Novarra Management Console and reinstall it.

B.4.1.1.2.1.1 Uninstall and Reinstall Management Console

1. Perform the uninstallation procedures for Management Console (see section C.2, “Uninstalling Novarra Management Console” on page C-4).
2. Perform the unistallation procedures for Tomcat (see section C.3, “Uninstalling Tomcat 3.2.3” on page C-6).
3. Perform the installation procedures for Management Console (see section 2.2.2, “Installing Novarra Management Console” on page 2-4).
4. Start WirelessWeb:
   Start→Programs→Novarra WirelessWeb→Start ALL Novarra services (WWES + Agent + Tomcat)



5. Login to Novarra Management Console:
   Start→Programs→Novarra Management Console→Management Console Login

Note:

If Tomcat still fails to be successfully installed, contact Novarra Technical Support.

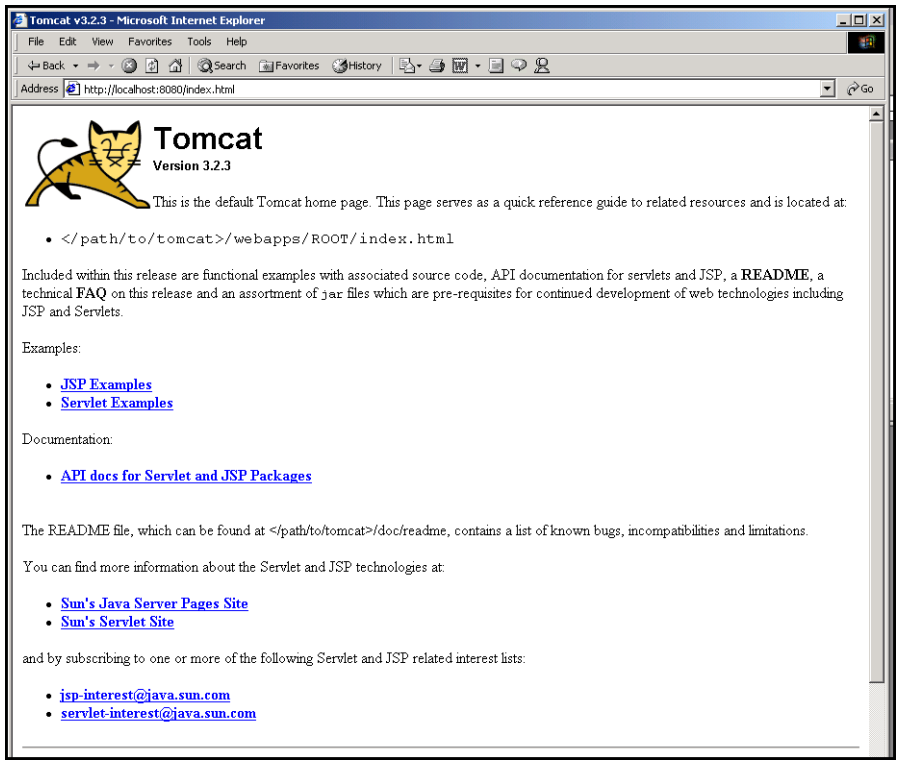
B.4.1.1.2.2 TOMCAT_HOME Does Appear in the System Variable List

1. Record the value of the **TOMCAT_HOME** environment variable as seen in step 4 of section B.4.1.1.2. (e.g. `c:\tomcat-3.2.3`)
2. Using Windows Explorer, go to the `conf` folder under the `c:\tomcat-3.2.3` folder (or whatever the **TOMCAT_HOME** value is).
3. Using a text editor to view the file `server.xml`, search for the following text:

   ```
   <Connector className="org.apache.tomcat.service.
   PoolTcpConnector">
   <Parameter name="handler" value="org.apache.tomcat.
   service.http.HttpConnectionHandler"/>
   <Parameter name="port" value="8080"/>
   ```

4. Note the value of Tomcat's http port (the default is 8080). Call this the <`tomcat_port`>.
5. Point your browser to:

   `http://<management_console_host>:<tomcat_port>`
6. If you see the Tomcat welcome page, then tomcat is up and running.



7. If you don't see the tomcat welcome page, then try to start tomcat; if you still can't see the welcome page, then Tomcat is improperly installed and you will want to either verify your installation of it or rerun Novarra's installation of it (see section B.4.1.1.2.1.1, “Uninstall and Reinstall Management Console” on page B-17).

If you verify your Tomcat installation per above, but you are still unable to log into the Novarra Management Console, then you should check that the Novarra

Management Console's web application file (**NovarraOAMP.war**) is correctly located in the Tomcat directory.

1. Start Tomcat JSP Engine:
   Start→Programs→Novarra Management Console→Start Tomcat JSP Engine
2. Go to c:\tomcat-3.2.3\webapps (or whatever the <**TOMCAT_HOME** value is>\webapps).
3. There, you should see the **NovarraOAMP.war** file, and you should see a subdirectory called **NovarraOAMP**. If you fail to see either of these, then you should uninstall and reinstall Novarra Management Console (see section B.4.1.1.2.1.1, "Uninstall and Reinstall Management Console" on page B-17). Make a note of any problems during the installation, and contact Novarra Technical Support if you still can't login to the Management Console.

B.4.1.1.3 Checking the Registry Setting for Tomcat

To check the registry settings for Tomcat service, run the Windows Registry Editor.

1. From the Windows Start menu, select Run and type
   regedit
2. Click OK.
3. Navigate to the following key:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tomcat\Parameters
4. Verify that the following registry key values appear:

Name	Type	Data
(Default)	REG_SZ	(value not set)
JVM Library	REG_SZ	C:\PROGRA~1\Novarra\JRE\1.3\bin\hotspot\jvm.dll
JVM Option Count	REG_DWORD	0x00000002 (2)
JVM Option Numb...	REG_SZ	-Djava.class.path=C:\TOMCAT~1.3\lib\webserver.jar;C:\TOMCAT~...
JVM Option Numb...	REG_SZ	-Dtomcat.home=C:\TOMCAT~1.3
Start Class	REG_SZ	org.apache.tomcat.startup.Tomcat
Start Method	REG_SZ	main
Start Param Count	REG_DWORD	0x00000002 (2)
Start Param Num...	REG_SZ	-config
Start Param Num...	REG_SZ	C:\TOMCAT~1.3\conf\server.xml
Stop Class	REG_SZ	org.apache.tomcat.startup.Tomcat
Stop Method	REG_SZ	main
Stop Param Count	REG_DWORD	0x00000003 (3)
Stop Param Numb...	REG_SZ	-stop
Stop Param Numb...	REG_SZ	-config
Stop Param Numb...	REG_SZ	C:\TOMCAT~1.3\conf\server.xml
System.err File	REG_SZ	C:\PROGRA~1\Novarra\MANAGE~1\logs\tomcat_stderr.log
System.out File	REG_SZ	C:\PROGRA~1\Novarra\MANAGE~1\logs\tomcat_stdout.log

Note:

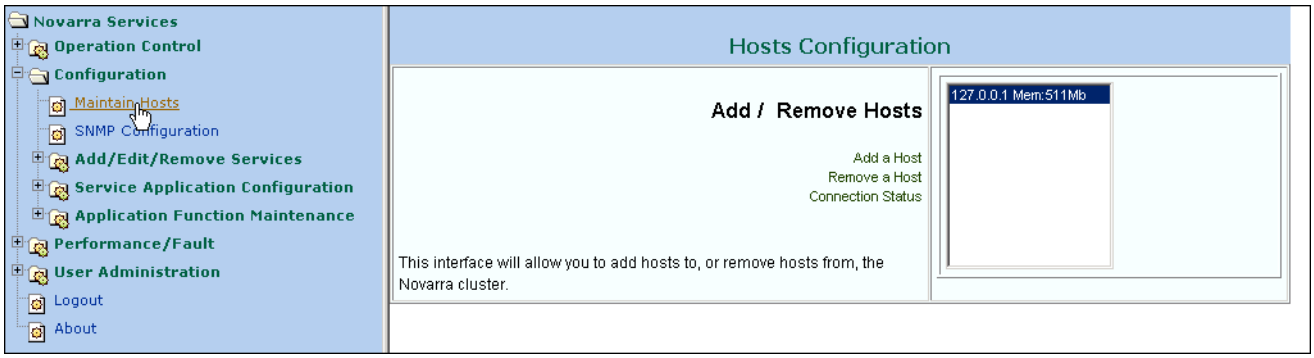
The values above will vary based on the location of your JRE and Tomcat (**TOMCAT_HOME**) installations.

5. If any of the values appear to be incorrect, then re-install the Novarra Management Console. Follow the steps in "Uninstall and Reinstall Management Console" on page B-17.

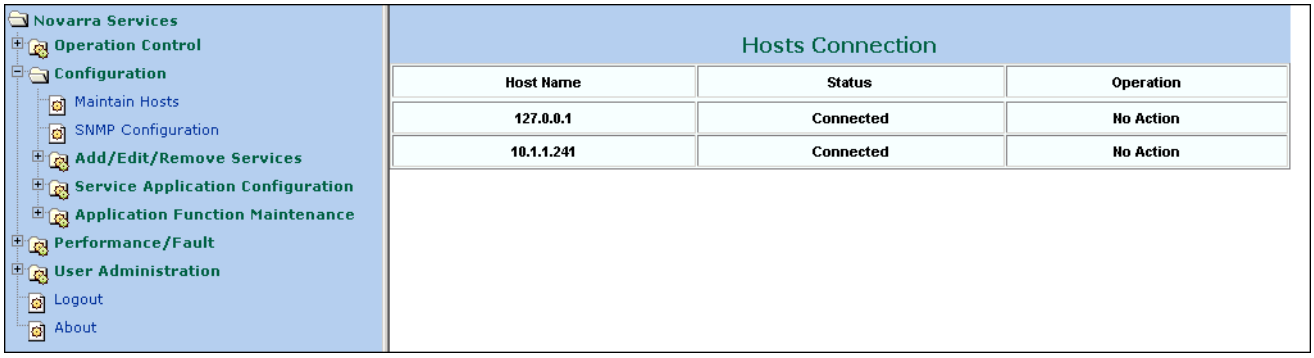
B.4.2 Troubleshooting Novarra Agent Installation

B.4.2.1 Check Host Connection Status

1. After successfully logging in to the Management Console, navigate to: **Configuration→Maintain Hosts**



2. In the Add/Remove Hosts box, you should see listed the local host's IP address (127.0.0.1). This is the host on which the Tomcat JSP engine is running. Highlight this host IP address and then click on **Connection Status**.
3. The host's status should be "Connected". This indicates a connection between the Novarra Management application and the Novarra Agent on the local host.



Also, for each additional host that you've run the WirelessWeb Server installation on, you'll want to add it (and then status the connection to it) by using this interface.

If any host can not be connected to, then the installation of the Novarra Agent should be checked for that host.

1. Go to that host and make sure that **NovarraStandaloneAgent** is properly configured in the Service Control Manager (SCM) for that host.

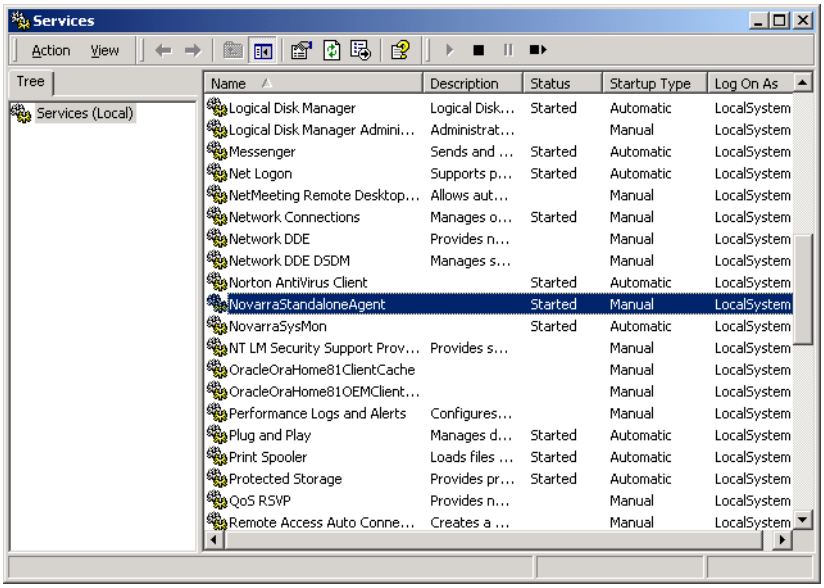
- To open the SCM on Windows 2000:

Start→Settings→Control Panel→Administrative Tools→Services

- To open the SCM on Windows NT 4.0:

Start→Settings→Control Panel→Services

2. Scroll down the list of services and search for **NovarraStandaloneAgent**.



- If **NovarraStandaloneAgent** appears in the Service Control Manager, see B.4.2.1.1, "NovarraStandaloneAgent Appears in the SCM," below.
- If **NovarraStandaloneAgent** does not appear in the Service Control Manager, see section B.4.2.1.2, "NovarraStandaloneAgent Does Not Appear in the SCM" on page B-23.

B.4.2.1.1 NovarraStandaloneAgent Appears in the SCM

If **NovarraStandaloneAgent** appears in the SCM, it should show up as "Manual" and "Started". If it does not show up as "Started", then start it by with either of the following methods:

- Start→Programs→Novarra Management Console→Start Novarra Agent
- Right-click on **NovarraStandaloneAgent** in the SCM and select **Start** in the pull down.

B.4.2.1.1.1 Novarra Agent Appears to Start

If Novarra Agent appears to have started, try logging in again and verifying the host connection status (see section B.4.2.1, "Check Host Connection Status" on page B-20).

B.4.2.1.1.2 Novarra Agent Fails to Start

If the **NovarraStandaloneAgent** service fails to start by either of these means, then the most probable cause is improper registry settings. Check the registry settings by running the Windows Registry Editor.

1. From the Windows Start menu, select Run and type
   `regedit`
2. Navigate to the following key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NovarraStandaloneAgent\Parameters`
3. Verify that the following registry key values appear:

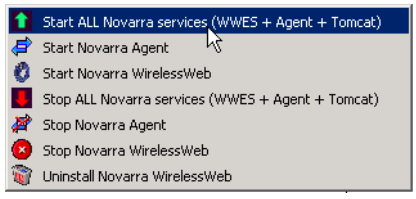
Name	Type	Data
(Default)	REG_SZ	(value not set)
JVM Library	REG_SZ	C:\PROGRA~1\Novarra\JRE\1.3\bin\hotspot\jvm.dll
JVM Option Count	REG_DWORD	0x00000002 (2)
JVM Option Numb...	REG_SZ	-Djava.class.path=C:\PROGRA~1\Novarra\WIRELE~1\lib\novarra.j...
JVM Option Numb...	REG_SZ	-Djava.library.path=C:\PROGRA~1\Novarra\WIRELE~1\lib
Start Class	REG_SZ	com.novarra.oamp.agent.StandaloneAgent
Start Method	REG_SZ	main
Start Param Count	REG_DWORD	0x00000001 (1)
Start Param Num...	REG_SZ	C:\PROGRA~1\Novarra\WIRELE~1\logs\StandaloneAgent.log
System.err File	REG_SZ	C:\PROGRA~1\Novarra\WIRELE~1\logs\StandaloneAgent.err
System.out File	REG_SZ	C:\PROGRA~1\Novarra\WIRELE~1\logs\StandaloneAgent.out

Note:

The values above may vary based on the locations of your JRE and Novarra WirelessWeb Server installations.

If any of the values appear to be incorrect, then uninstall your current installation of the Novarra WirelessWeb:

1. Perform the uninstallation procedures for Management Console (see section C.1, “Uninstalling Novarra WirelessWeb Server” on page C-2).
2. Perform the installation procedures for Management Console (see section 2.2.1, “Installing WirelessWeb Server” on page 2-2).
3. Start WirelessWeb:
   Start→Programs→Novarra WirelessWeb→Start ALL Novarra services (WWES + Agent + Tomcat)

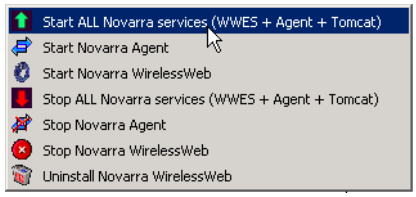


4. Login to Novarra Management Console:
   Start→Programs→Novarra Management Console→Management Console Login
5. Verify the connection status for all WirelessWeb Server hosts (see section B.4.2.1, “Check Host Connection Status” on page B-20).

B.4.2.1.2 NovarraStandaloneAgent Does Not Appear in the SCM

If **NovarraStandaloneAgent** does not appear in the SCM, use Windows Explorer to check if WirelessWeb was installed in the folder you specified during the installation. If not, then the installation may not have been allowed to complete.

1. Perform the installation procedures for Management Console (see section 2.2.1, “Installing WirelessWeb Server” on page 2-2).
2. Start WirelessWeb:
   Start→Programs→Novarra WirelessWeb→Start ALL Novarra services (WWES + Agent + Tomcat)



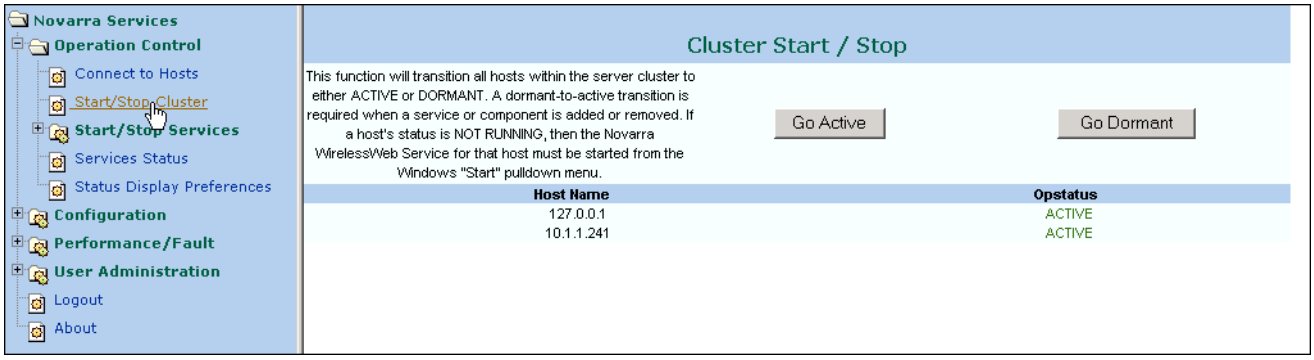
3. Login to Novarra Management Console:
   Start→Programs→Novarra Management Console→Management Console Login
4. Verify the connection status for all WirelessWeb Server hosts (see section B.4.2.1, “Check Host Connection Status” on page B-20).

B.4.3 Troubleshooting NovarraSysmon Installation

After successfully logging into the Novarra Management Console and verifying that all hosts are properly connected to (see section B.4.2.1, “Check Host Connection Status” on page B-20), verify that the NovarraSysMon service is installed and running for all hosts.

B.4.3.1 Check Host Opstatus

1. Navigate to:
   Configuration→Operation Control→Start/Stop Cluster



2. All hosts should show up in the **Cluster Start/Stop** frame with an Opstatus of either **ACTIVE** or **DORMANT**.

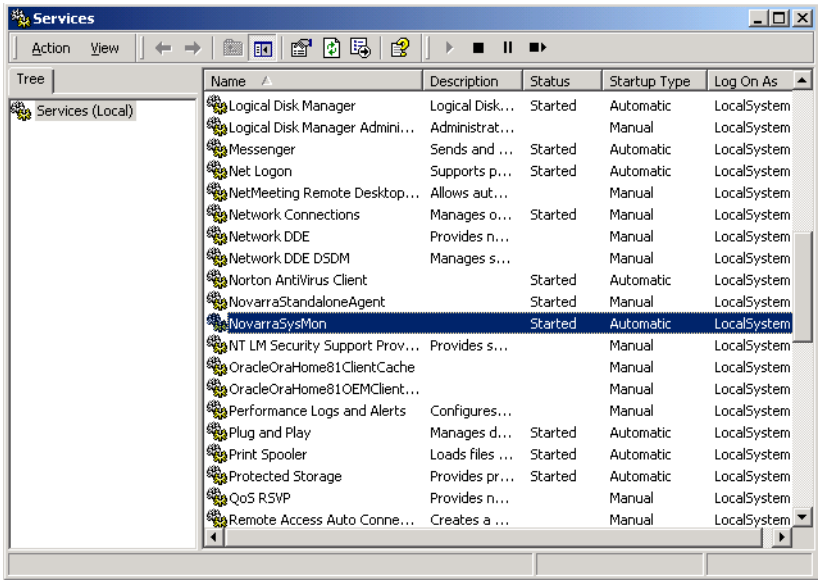
If any host shows up with a status of **Undetermined**, and the NovarraAgent is properly installed and running for that host (as verified in the previous section), then that means that the NovarraSysMon service is somehow improperly installed and should be checked for that host.

1. Go to that host and make sure that **NovarraSysMon** is properly configured in the Service Control Manager (SCM) for that host.

   • To open the SCM on Windows 2000:
   Start→Settings→Control Panel→Administrative Tools→Services

   • To open the SCM on Windows NT 4.0:
   Start→Settings→Control Panel→Services

2. Scroll down the list of services and search for **NovarraSysMon**.



B.4.3.1.1 NovarraSysMon Appears in the SCM

If **NovarraSysMon** appears in the SCM, it should show up as "Automatic" and "Started". If it does not show up as "Started", then start it by with either of the following methods:

- Start→Programs→Novarra Management Console→Start Novarra Agent
- Right-click on **NovarraSysMon** in the SCM and select **Start** in the pull down.

B.4.3.1.1.1 NovarraSysMon Appears to Start

If **NovarraSysMon** appears to have started, try logging in again.

B.4.3.1.1.2 NovarraSysMon Fails to Start

If the **NovarraSysMon** service fails to start by either of these means, then the most probable cause is improper registry settings. Check the registry settings by running the Windows Registry Editor.

1. From the Windows Start menu, select Run and type
   `regedit`
2. Navigate to the following key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NovarraSysMon`
3. Verify that the following registry key values appear:

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	NovarraSysMon
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\Program Files\Novarra\WirelessWeb\tools\SRVANY.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

4. Also, navigate to the following key:
   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NovarraSysMon\Parameters`
5. Verify that the following registry key values appear:

Name	Type	Data
(Default)	REG_SZ	(value not set)
AppDirectory	REG_SZ	C:\PROGRA~1\Novarra\WIRELE~1\Config
Application	REG_SZ	C:\PROGRA~1\Novarra\WIRELE~1\bin\SysMon.exe

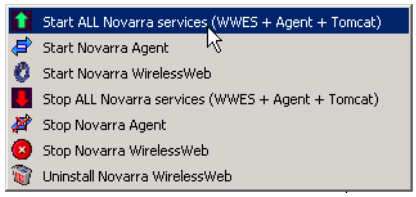
Note:

The values in the above two displays may vary based on the location of your Novarra WirelessWeb Server installation.

If any of the values appear to be incorrect, then uninstall your current installation of the Novarra WirelessWeb:

1. Perform the uninstallation procedures for Management Console (see section C.1, “Uninstalling Novarra WirelessWeb Server” on page C-2).
2. Perform the installation procedures for Management Console (see section 2.2.1, “Installing WirelessWeb Server” on page 2-2).
3. Start WirelessWeb:

   Start→Programs→Novarra WirelessWeb→Start ALL Novarra services (WWES + Agent + Tomcat)



4. Login to Novarra Management Console:

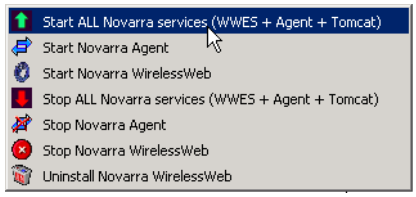
   Start→Programs→Novarra Management Console→Management Console Login
5. Verify the connection status for all WirelessWeb Server hosts (see section B.4.2.1, “Check Host Connection Status” on page B-20).
6. Verify the Opstatus for all cluster elements (see section B.4.3.1, “Check Host Opstatus” on page B-24).

B.4.3.1.2 NovarraSysMon Does Not Appear in the SCM

If **NovarraSysMon** does not appear in the SCM, use Windows Explorer to check if WirelessWeb was installed in the folder you specified during the installation. If not, then the installation may not have been allowed to complete.

1. Perform the installation procedures for Management Console (see section 2.2.1, “Installing WirelessWeb Server” on page 2-2).
2. Start WirelessWeb:

   Start→Programs→Novarra WirelessWeb→Start ALL Novarra services (WWES + Agent + Tomcat)



3. Login to Novarra Management Console:

   Start→Programs→Novarra Management Console→Management Console Login
4. Verify the connection status for all WirelessWeb Server hosts (see section B.4.2.1, “Check Host Connection Status” on page B-20).

B.4.4 Component Won't Start

If a component (**ACA**, **WCM-DATATAC-LH**, **WCM-MOBITEX-DM**, etc.) won't come up (i.e., its status remains **DOWN-OP** or **DOWN-ADMIN** for more than one minute after starting the cluster), then check the following (this example assumes the component is named ACA1):

1. Go to <WWES_install_dir>/logs and review the files `ACA1_stdout.log` and `ACA1_stderr.log` for any problems that ACA1 may have logged while attempting to initialize.
2. If `ACA1_stdout.log` or `ACA1_stderr.log` don't exist, then check the Heap settings for ACA1:
   Configuration→Add/Edit/Remove Services→[service-name]→ACA1
3. Check the Java VM Heap Size -- if it's greater than 64Mb, then change it to 64Mb, stop the cluster, and then start the cluster again.

B.4.5 Statuses Show Undetermined

If the management console shows a status of **Undetermined** for something (e.g., the cluster, the WWES software version in the "About" screen, etc.), then check to make sure the management console is connected to the affected host:

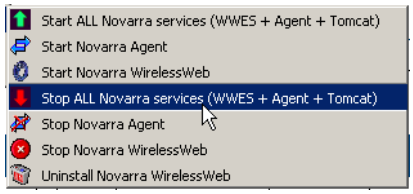
1. Navigate to:
   Configuration→ Maintain Hosts
2. Click on **Connection Status**
3. Ensure that all hosts are marked as **Connected.** If not, attempt to connect to the host using the available form button.
4. If a host cannot be connected to, go to the console of that host and ensure that the Novarra Agent is running by stopping and then starting the agent:
   Start→Programs→Novarra WirelessWeb→Stop Novarra Agent
   Start→Programs→Novarra WirelessWeb→Start Novarra Agent
5. If the host still cannot be connected to, review the `StandaloneAgent.out` and `StandaloneAgent.err` files in the <WWES_install_dir>/logs directory and check for any problems that may have been logged.

B.4.6 Cluster Status is NOT_RUNNING

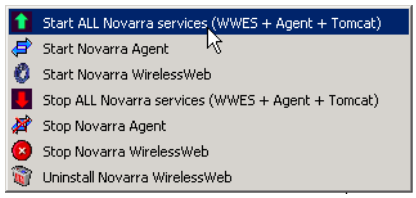
If the Cluster status (**Configuration→Operation Control→Start/Stop Cluster**) is **NOT_RUNNING**, then Sysmon (the monitoring daemon of the WirelessWeb Server) may not be running on that host.

1. First, attempt to restart Sysmon for that host:
   Start→Programs→Novarra WirelessWeb→Stop Wireless Web
   Start→Programs→Novarra WirelessWeb→Start Wireless Web

2. If the Cluster status is still **NOT_RUNNING**, then attempt to restart all WWES components:
   Start→Programs→Novarra WirelessWeb→Stop ALL Novarra services (WWES + Agent + Tomcat)



   Start→Programs→Novarra WirelessWeb→Start ALL Novarra services (WWES + Agent + Tomcat)



3. If none of these procedures work, you may have an incorrect installation (see section B.4, “Troubleshooting WirelessWeb Server Installation” on page B-13.)

Uninstalling Novarra WirelessWeb Enterprise Suite

C

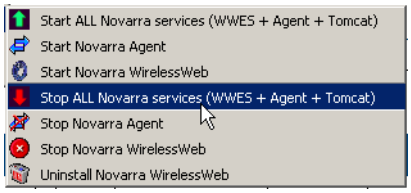
If you are updating or reinstalling WirelessWeb Enterprise Suite, it is not necessary to uninstall it. WirelessWeb Enterprise Suite can be updated or reinstalled and the configuration files from the previous installation saved. But if you need to remove it, the following sections will show you how:

Warning:

Novarra WirelessWeb, Novarra Agent and Tomcat JSP Engine must be stopped before uninstalling:

Navigate to and click the "Stop ALL Novarra services (WWES + Agent + Tomcat)" shortcut:

Start→Programs→Novarra WirelessWeb→Stop ALL Novarra services (WWES + Agent + Tomcat)

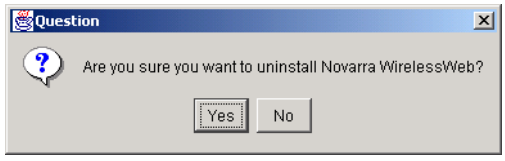


C.1 Uninstalling Novarra WirelessWeb Server

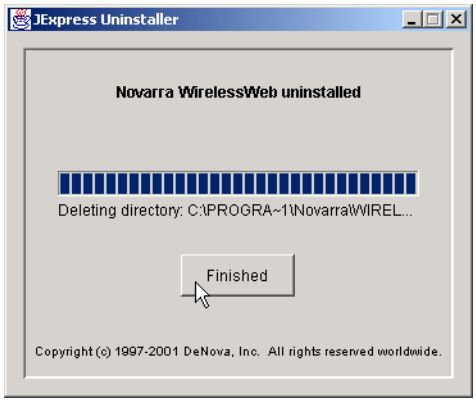
There are two ways to uninstall Novarra WirelessWeb:

C.1.1 Uninstall Novarra WirelessWeb From the Start Menu

1. Navigate to and click the "Uninstall Novarra WirelessWeb" shortcut:
   Start→Programs→Novarra WirelessWeb→Uninstall Novarra WirelessWeb
2. An alert appears asking if you want to uninstall WirelessWeb. Click the Yes button.



3. WirelessWeb is uninstalled and the JExpress Uninstaller panel appears. Click the Finished button.

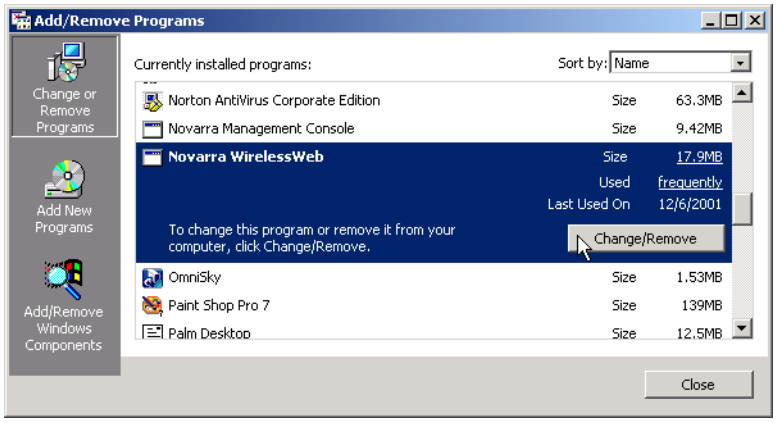


C.1.2 Uninstall Novarra WirelessWeb From the Control Panel

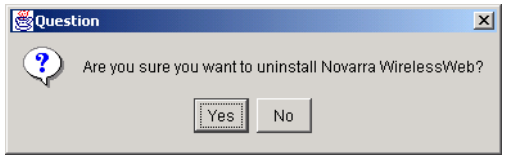
Follow these steps to uninstall Novarra WirelessWeb from the Add/Remove Programs window in the Control Panel:

1. Open Add/Remove Programs window:
   Start→Settings→Control Panel→Add/Remove Programs

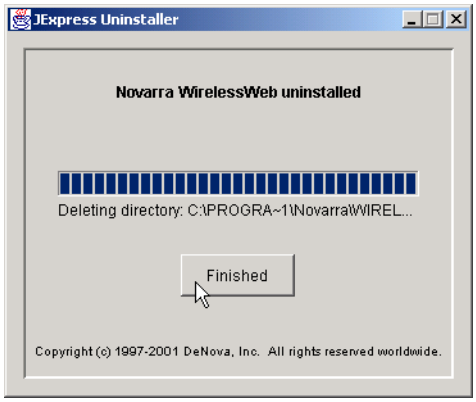
2. Select Novarra WirelessWeb and click the Change/Remove button.



3. An alert appears asking if you want to uninstall WirelessWeb. Click the Yes button.



4. WirelessWeb is uninstalled and the JExpress Uninstaller panel appears. Click the Finished button.



5. Click on Close in the Add/Remove Programs window.

C.2 Uninstalling Novarra Management Console

There are two ways to uninstall Management Console:

- "Uninstall Novarra Management Console From the Start Menu" on page C-4
- "Uninstall Novarra Management Console From the Control Panel" on page C-5

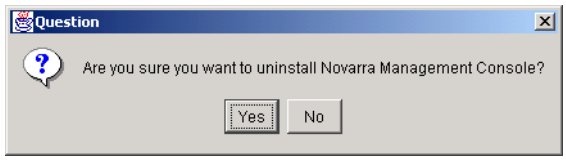
Note:

Tomcat 3.2.3 is not uninstalled with this procedure. See "Uninstalling Tomcat 3.2.3" on page C-6.

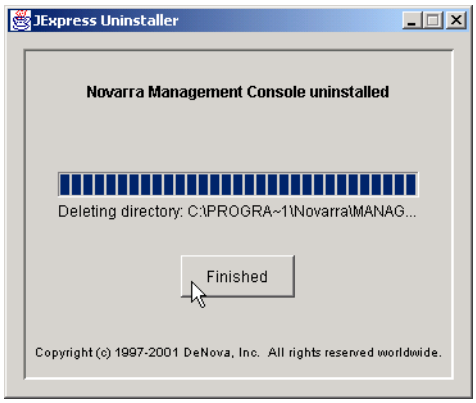
C.2.1 Uninstall Novarra Management Console From the Start Menu

1. Navigate to and click the "Uninstall Novarra Management Console" shortcut:

   Start→Programs→Novarra Management Console→Uninstall Novarra Management Console
2. An alert appears asking if you want to uninstall Management Console. Click the Yes button.



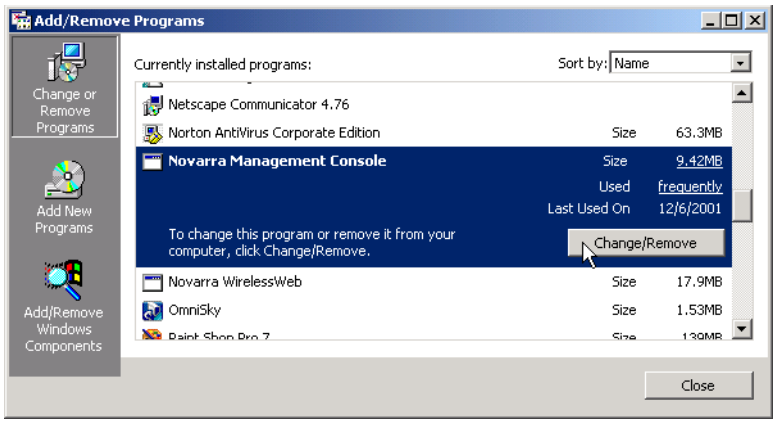
3. Management Console is uninstalled and the JExpress Uninstaller panel appears. Click the Finished button.



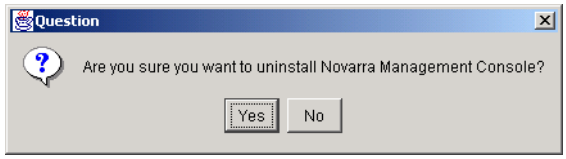
C.2.2 Uninstall Novarra Management Console From the Control Panel

Follow these steps to uninstall Novarra Management Console from the Add/Remove Programs window in the Control Panel:

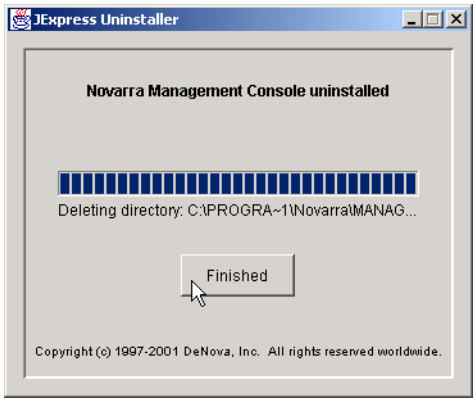
1. Open Add/Remove Programs window:
   Start→Settings→Control Panel→Add/Remove Programs
2. Select Novarra Management Console and click the Change/Remove button.



3. An alert appears asking if you want to uninstall Management Console. Click the Yes button.



4. WirelessWeb is uninstalled and the JExpress Uninstaller panel appears. Click the Finished button.



5. Click on Close in the Add/Remove Programs window.

C.3 Uninstalling Tomcat 3.2.3

If you are updating or reinstalling Management Console, it is not necessary to uninstall Tomcat. But if you should need to remove Tomcat, perform the following procedures:

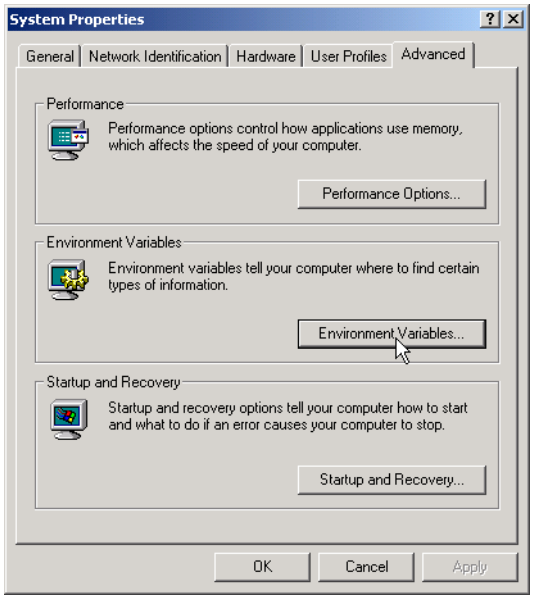
Note:

Do not remove Tomcat JSP Engine if you have other applications that use it. If you are unsure, it is best not to uninstall it.

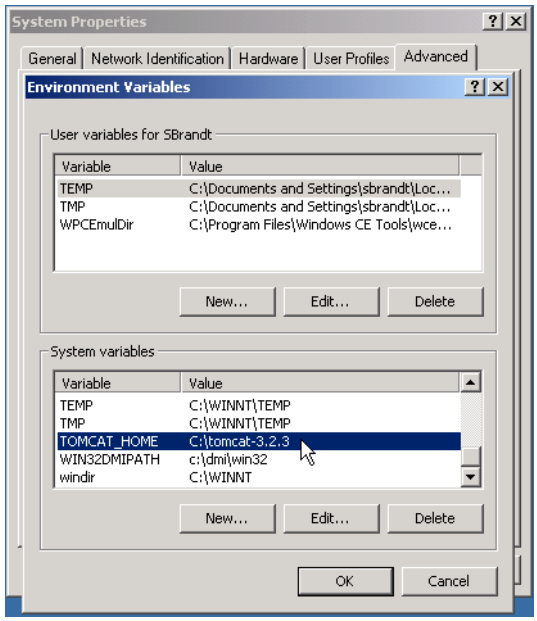
Warning:

Tomcat JSP Engine must be stopped before uninstalling:
Start→Programs→Novarra Management Console→Stop Tomcat JSP Engine

1. Open the System Properties panel:
   Start→Settings→Control Panel→System
2. Click the Advanced tab.
3. Click on Environment Variables…



4. In System variables, click on TOMCAT_HOME and click the Delete button. Click the OK button in the Environment Variables window.



5. Click the OK button to close the System Properties panel.
6. Delete the C:\tomcat-3.2.3 directory and all its content.