Element Manager System Reference - Administration
Avaya Communication Server 1000

Release 7.6
NN43001-632
Issue 06.01
March 2013

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Note to Service Provider

The Product may use Third Party Components that have Third Party Terms that do not allow hosting and may need to be independently licensed for such purpose.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third

parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release

The following sections detail what is new in *Avaya Element Manager System Reference — Administration, NN43001-632* for Avaya Communication Server 1000 Release 7.6.

Features

See the following sections for information about changes that are feature-related for Avaya Communication Server 1000 (Avaya CS 1000) Release 7.6.

Voice mail soft keys enable and disable

Communication Server 1000 Release 7.6 introduces the ability to enable voice mail soft keys on IP Deskphones and M3900 Series digital telephones if using CallPilot as the messaging system. This functionality can be enabled or disabled in the Features web page section of Phones in Element Manager.

See Features web page on page 236.

Shared Bandwidth Management

The Shared Bandwidth Management (SBWM) feature allows bandwidth to be shared dynamically between multiple bandwidth consumers in a single location; you can configure and manage SBWM using Element Manager. New configuration options have been added to the following screens:

- Element Manager > Routes and Trunks > Routes and Trunks
- Element Manager > System > IP Network > Zones
- Element Manager > System > IP Network > IP Telephony Nodes

For more information, see Zones on page 171, Zone Diagnostics on page 106. *Features and Services Fundamentals — Book 6 of 6 (S to Z), NN43001–106*, and *Converging the Data Network with VoIP Fundamentals, NN43001–260*.

Other changes

There are no other changes for this release.

Revision history

March 2013	Standard 06.01. This document is up-issued to support Avaya Communication Server 1000 Release 7.6.
December 2011	Standard 05.14. This document is up-issued for changes in technical content. The List number ranges for procedures Adding a Speed Call List and Adding a Group Hunt List have been revised.
November 2011	Standard 05.13. This document is up-issued for changes in technical content. The System Date and Time and Current system Date and Time sections have been updated.
October 2011	Standard 05.12. This document is up-issued for changes in technical content. The Element Manager Local login section has been updated.
September 2011	Standard 05.11. This document is up-issued for changes in technical content. The System Date and Time and Current system Date and Time sections have been updated.
September 2011	Standard 05.10. This document is up-issued to support the removal of content for outdated features, hardware, and system types.
July 2011	Standard 05.09. This document is up-issued for changes in technical content.
June 2011	Standard 05.08. This document is up-issued for changes in technical content.
May 2011	Standard 05.07. This document is up-issued for changes in technical content. Information has been added to the IP Telephony Nodes section.
March 2011	Standard 05.06. This document is published to support Avaya Communication Server 1000 Release 7.5.
February 2011	Standard 05.05. This document is up-issued for changes in technical content. Java Runtime Environment versions compatible with a Virtual Terminal Emulator are listed in Virtual Terminals on page 37.
November 2010	Standard 05.04. This document is published to support Avaya Communication Server 1000 Release 7.5. This document includes

	information about how to restore IP Telephony Nodes from a prior-Release Call Server.
November 2010	Standard 05.01 to 05.03. These documents are issued to support Avaya Communication Server 1000 Release 7.5.
November 2011	Standard 04.08. This document is up-issued for changes in technical content. The Element Manager Local login section has been updated.
June 2011	Standard 04.07. This document is up-issued to update content for Communication Server 1000 Release 7.0.
May 2011	Standard 04.06. This document is up-issued to update content for Communication Server 1000 Release 7.0. Information has been added to the IP Telephony Nodes section.
March 2011	Standard 04.05. This document is up-issued for changes in technical content.
February 2011	Standard 04.04. This document is up-issued to update content for Communication Server 1000 Release 7.0.
December 2010	Standard 04.03. This document is up-issued to update content for Communication Server 1000 Release 7.0.
June 2010	Standard 04.02. This document is up-issued to update content for Avaya Communication Server 1000 Release 7.0.
June 2010	Standard 04.01. This document is up-issued to support Communication Server 1000 Release 7.0.
October 2009	Standard 03.19. This document is up-issued to support MG XPEC.
June 2009	Standard 03.18. This document is up-issued to provide information concerning deploying more that one Element Manager to manage a single Call Server and the effects on the EM Phone provisioning application and to provide a procedure for removing control M characters from TM configuration files.
June 2009	Standard 03.17. This document is up-issued to support Communication Server 1000 Release 6.0. This document may contain information on or refer to products and naming conventions that are not supported in this release. This information is included for legacy purposes and convenience only. This includes but is not limited to items, such as: SSC; ISP 1100; ITG Pentium cards; and Media Cards running certain IP Line applications.
May 2009	Standard 03.16. This document is up-issued to support Communication Server 1000 Release 6.0. This document may contain information on or refer to products and naming conventions that are not supported in this release. This information is included for legacy purposes and convenience only. This includes but is not limited to items, such as: SSC; ISP 1100; ITG Pentium cards; and Media Cards running certain IP Line applications.

July 2008	Standard 02.15. This document is up-issued to update the Station Fast Sync feature section.
April 2008	Standard 02.14. This document is up-issued to add patching information.
March 2008	Standard 02.12. This document is up-issued to add information about Zone 0 and CR Q01834961.
February 2008	Standard 02.11. This document is up-issued to reflect changes in technical content.
January 2007	Standard 02.10. This document is up-issued to reflect changes in technical content.
December 2007	Standard 02.09. This document is up-issued to support Communication Server 1000 Release 5.5.
August 2007	Standard 01.05. This document is up-issued to support Microsoft Exchange Server 2007 Unified Messaging.
June 2007	Standard 01.03. This document is up-issued for: (1) to specify that PDT access is required to access the Element Manager patching feature. (2) to indicate that the rows in the Excel spreadsheet must be completed sequentially. (3) to correct the graphic Digit Conversion Tree Configuration Web page. (4) to provide more information about QoS threshold values. (5) to correct the graphic Clock Controller Basic Properties Web page.
May 2007	Standard 01.01. This document is up-issued to support Communication Server 1000 Release 5.0. This document contains information previously contained in the following legacy document, now retired: Element Manager System Administration (553-3001-332).
August 2005	Standard 3.00. This document is up-issued to support Communication Server 1000 Release 4.5.
September 2004	Standard 2.00. This document is up-issued for Communication Server 1000 Release 4.0.
October 2003	Standard 1.00. This document is new for Succession 3.0. It was created to support a restructuring of the Documentation Library. This document contains information previously contained in the following legacy document, now retired: Element Management (553-3023-222). Some content from Element Management (553-3023-222) also appears in Succession 1000 Element Manager: Installation and Configuration (553-3001-232).

Chapter 2: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Navigation

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, go to www.avaya.com/support. From this Web site, locate the Training link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 3: Introduction

This document is a global document. Contact your system supplier or your Avaya representative to verify that the hardware and software described are supported in your area.

Subject

This document describes the Element Manager interface.

Applicable Systems

This document applies to the following Avaya Communication Server 1000 (Avaya CS 1000) systems:

- Communication Server 1000M Single Group (CS 1000M SG)
- Communication Server 1000M Multi Group (CS 1000M MG)
- Communication Server 1000E (CS 1000E)

Intended Audience

This document is intended for individuals responsible for administering CS 1000 and Meridian 1 systems.

Conventions

Terminology

In this document, the following systems are referred to generically as system:

- Communication Server 1000E (CS 1000E)
- Communication Server 1000M (CS 1000M)
- Meridian 1

Related information

This section lists information sources that relate to this document.

Technical Documentation

The following technical documents are referenced in this document:

- *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*
- *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*
- *Avaya Network Routing Service Fundamentals, NN43001-130*
- *Avaya SIP Line Fundamentals, NN43001-508*
- *Avaya Co-resident Call Server and Signaling Server Fundamentals, NN43001-509*
- *Avaya Subscriber Manager Fundamentals, NN43001-120*
- *Avaya Transmission Parameters Reference, NN43001-282*
- *Avaya Dialing Plans Reference, NN43001-283*
- *Avaya Security Management Fundamentals, NN43001-604*
- *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*
- *Avaya System Management Reference, NN43001-600*
- *Avaya Communication Server 1000 Fault Management - SNMP, NN43001-719*

- *Avaya Software Input Output Reference — Maintenance, NN43001-711*
- *Avaya Branch Office Installation and Commissioning, NN43001-314*
- *Avaya System Redundancy Fundamentals, NN43001-507*
- *Avaya Software Input Output Administration, NN43001-611*

Chapter 4: Overview

Contents

This chapter contains information about the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Element Manager overview

Element Manager is a Web-based user interface used to configure and maintain Avaya CS 1000 components.

Element Manager is deployed with the Avaya Unified Communications Management solution on a Linux based operating system. UCM provides logon and security features for Element Manager.

For more information about UCM, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116.*

For more information about installing the Linux operating system, see *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

With Subscriber Manager, an administrator can create an account, publish/display phone attributes, and add and configure phone services for subscribers with available Templates in Element Manager. A template contains attributes common to a CS 1000 phone type. Once a template is created, you can use it to apply these common attributes to a group of phones, without having to repetitively define the same value for each phone. In general, using a template is a more efficient method of adding large numbers of phones than maintaining each phone individually.

Note:

It is possible to deploy more than one EM pointing to a Call Server using Deployment Manager, but the EM Phone provisioning application (Phones) does not support this. See, Limitations of deploying multiple Element Managers to manage a single Call Server on page 292.

Element Manager is a simple and user-friendly Web-based interface that supports a broad range of system management tasks, including:

- configuration and maintenance of IP Peer and IP Telephony features
- configuration and maintenance of traditional routes and trunks
- configuration and maintenance of numbering plans
- configuration of Call Server data blocks
- maintenance commands, system status inquiries, backup and restore functions
- patch upload, patch activation, firmware download

Element Manager has many features to help administrators manage systems with greater efficiency. Examples are as follows:

- Web pages provide a single point-of-access to parameters that were traditionally available through multiple overlays.
- Parameters are presented in logical groups to increase ease-of-use and speed-of-access.
- The hide or show information option enables administrators to see information that relates directly to the task at hand.
- Full-text descriptions of parameters help administrators reduce configuration errors.
- To simplify response selection, configuration screens offer preselected defaults, lists, checkboxes, and range values.
- To simplify the importing of phones to the database a Comma Separated Value (CSV) file can be used.

Note:

All screen captures in this chapter are applicable to CS 1000E and CS 1000M systems. Where there is no indicator, the screen and commands are available on both.

Note:

Option 81C and 61C must be upgraded to a CS 1000 M (SG or MG) in order to deploy it with UCM.

Key features

The following functional areas can be accessed using Element Manager:

- Links — Provides access to Virtual Terminal sessions.
- IP Network — Helps the user access all functions related to managing IP Networks. These functions include data and physical structure configuration, high-profile operational activities, and administrative/maintenance functions.
- System — Provides access to system-wide configuration and basic hardware/software management, including supported maintenance overlays and configuration.
- Customers — Allows the user to view and edit customer properties.
- Routes and Trunks — Provides access to all functions required to create and manage trunks.
- Dialing and Numbering Plans — Provides a way to configure all Electronic Switched Network (ESN) data blocks for the Call Server. Network Routing Service cannot be launched from inside EM from CS 1000 Release 6.0 onwards. To access configuration for the Network Routing Service (NRS), you must log on through UCM.
- Phones— Enables users to import and configure phones for the Call Server.
- Tools — Provides general administrative tools, features and functions, and allows the user to find and access task-related pages, including Reports.
- Security — Allows the user to perform Security functions, including IP Security.

Signaling Server

Element Manager enables administrators to perform the following activities on the Signaling Server:

- reset
- access the maintenance window
- download new IP Phone firmware
- upgrade IP Phone firmware
- view report log
- view Operational Measurements (OM) data
- Telnet
- patching

- increase Virtual Trunk capacity and perform configuration tasks on Virtual Trunks
- configure and manage the Web-based services for Personal Directory, Redial List, and Callers List
- add, delete, view, and edit Signaling Server information

Call Server and Media Gateway

For Call Server and Media Gateway, Element Manager enables administrators to configure and manage the following data:

- Configuration Record
- Customer Data Block
- Route Data Blocks
- Trunks
- ESN Data Block
- Patching

To learn more about parameters that can be configured and managed in Element Manager, see *Avaya System Management Reference, NN43001-600* .

IP Line and Voice Gateway

Element Manager enables administrators to perform the following activities on the IP Line and Voice Gateway Media Cards:

- View and configure Simple Network Management Protocol (SNMP) parameters and add IP addresses for forwarding SNMP traps.
- View and configure Voice Gateway profile data.
- View and edit Quality of Service (QoS) parameters.
- Use Local Area Network (LAN) configuration to configure the Management LAN (ELAN) subnet, Telephony LAN (TLAN) subnet, and Routes.
- View and edit Simple Network Time Protocol (SNTP) Server and Client information.
- View and configure file server access for downloading firmware for IP Phones.

- View and select the Loss and Level Plan for the country. For more information about selecting the Loss and Level Plan for the country, see *Avaya Transmission Parameters Reference, NN43001-282* .
- Add, remove, view, and edit card properties of Voice Gateway Media Cards.

To learn more about IP Line and Voice Gateway Media Card parameters that can be configured and managed in Element Manager, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

The following maintenance activities are supported when using Element Manager for IP Line and Voice Gateway Media Card:

- reset Voice Gateway Media Card
- enable/disable Voice Gateway Media Card
- access the maintenance window to the Voice Gateway Media Card
- download new loadware/firmware for upgrades
- run Syslog reports
- obtain Operational Measurement (OM) data
- Telnet to the card
- patching

To learn more about the IP Line and Voice Gateway maintenance activities that are supported by Element Manager, see IP Network on page 123.

Chapter 5: How to use Element Manager

Contents

This chapter contains information about the following topics:

Launching Element Manager

You can launch the Element Manager from the UCM or using local login method. Element Manager is installed with the Avaya Unified Communications Management (UCM) solution on a CP PM server or on one of the Commercial off the shelf (COTS) servers.

Start Element Manager from the UCM solution. This solution supports Single Sign-on so that you can access multiple systems. Users access UCM Common Services through Microsoft Internet Explorer 6.02600 or later. For information about how to log on to UCM Common Services, configure the UCM Common Services, and log on to Element Manager, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Element Manager Local logon

Local log in to Element Manager typically occurs when you perform an initial system set up, or when connectivity is lost and you cannot perform a network log in to Element Manager. When you log in to Element Manager locally, you must provide a Call server IP address.

Note:

To access the local login page, type the url in the Web browser Address bar and press **Enter**. You must enter the url in one of the following formats:

- https://<FQDN of the server where the EM application is installed>/emWebLocal/
- https://<IP address of the server where the EM application is installed>/emWebLocal/

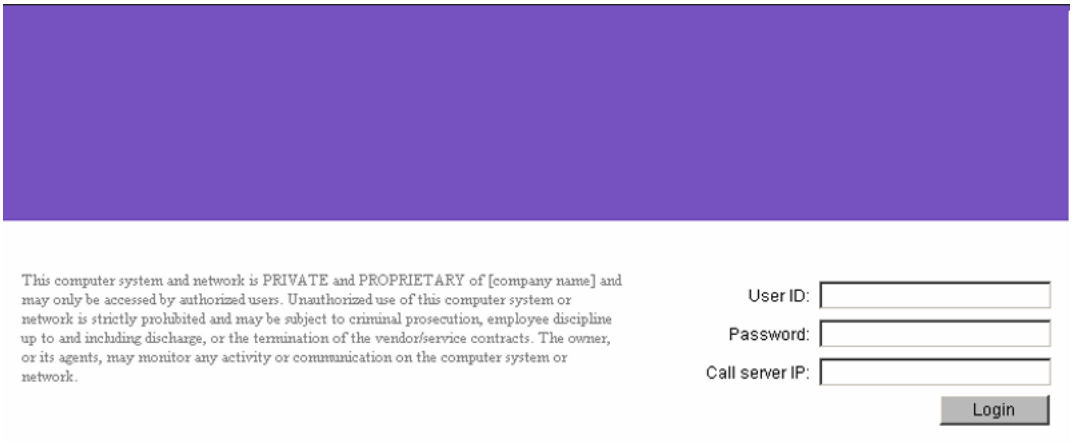


Figure 1: Element Manager Login page

When you access Element Manager locally, you cannot access the following links.

- Nodes: Servers, Media Cards
- Maintenance and Reports
- Call Server PEP
- File Upload
- IP Phone Firmware
- Voice Gateway Media Card
- Media Cards PEPS
- Date and time
- Phones

Timeout after a period of inactivity

Element Manager times out after a period of inactivity. Sessions end without warning, from all Element Manager Web pages, with one exception—the Edit Web pages. When you work on this Web page, a message appears that warns of the impending timeout action. Click **OK** (on the warning message) within the remaining timeout period (5 minutes) to reset the timer. If no response occurs within the five-minute warning period, the session ends, and you must log in again. Data modifications made on screen, but not submitted to the system, are lost.

File uploads using Internet Explorer

To upload files in Internet Explorer you must provide the full local file path. In Internet Explorer, navigate to **Tools** > **Internet Options** > **Security** > **Custom level...**. In the Security settings dialog box enable **Include local directory path when uploading files to a server**.

ActiveX configuration in Internet Explorer

Element Manager uses ActiveX controls in several of the Internet Explorer pages. You must make the following required IE settings for Element Manager to work properly.

- Change or configure the Security settings.
- Go to **Tools > Internet Options > Security > Custom Level**. Add the Element Manager site to the Trusted Site Zone. In the **Security Settings** dialog box for the appropriate zone, select **Enable** or **Prompt** for the Initialize and script ActiveX controls not marked as safe.

  If **Disable** is selected, then you receive the following error:

  ```
  Automation server can not create object.
  ```

Navigation

The Element Manager navigator is on the left side of the Web page as shown in Figure 2: Element Manager navigator on page 34.

Figure 2: Element Manager navigator

Links in the Element Manager navigator are structured as follows:

- **Home**
- **Links**
  - Virtual Terminals
- **System**
  - Alarms
  - Maintenance
  - Core Equipment

- Peripheral Equipment
- IP Network
- Interfaces
- Engineered Values
- Emergency Services
- Geographic Redundancy
- Software

• **Customers**

• **Routes and Trunks**

- Routes and Trunks
- D-Channels
- Digital Trunk Interface

• **Dialing and Numbering Plans**

- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Conversion

• **Phones**

- Templates
- Reports
- Views
- Lists
- Properties
- Migration

• **Tools**

- Backup and Restore
- Call Server Initialization
- Date and Time
- Logs and Reports

• **Security**

- Passwords
- Policies
- Login Options

During periods of high call volume, Element Manager Web pages load slowly.

Configuring data

In many cases, you can edit data using configuration Web pages. At the bottom of the configuration Web pages, the following four buttons appear:

- **Submit** — Transmits changes to the Call Server.
- **Refresh**— Refreshes data from the Call Server. Refresh overwrites any changes not yet submitted.
- **Delete** — Deletes the item being edited or configured.
- **Cancel** — Discards the changes and returns to the appropriate configuration page.

Logging off

To log off Element Manager and UCM, click the **Logout** link in the top right corner of the Web page.

Chapter 6: Links

Contents

This chapter contains information about the following topics:

Introduction

The features available under the **Links** branch of the Element Manager navigator enable Element Manager to be the single point of management access to Web pages and character-based interfaces.

Use the Virtual Terminal feature to access any IP-based elements on the network. On the Call Server, you can access context-sensitive online help, which provides detailed information about system prompts and error messages.

Virtual Terminals

Click the **Virtual Terminals** link to open the Virtual Terminal Sessions Web page as shown in Figure 3: Virtual Terminal Sessions Web page on page 38.

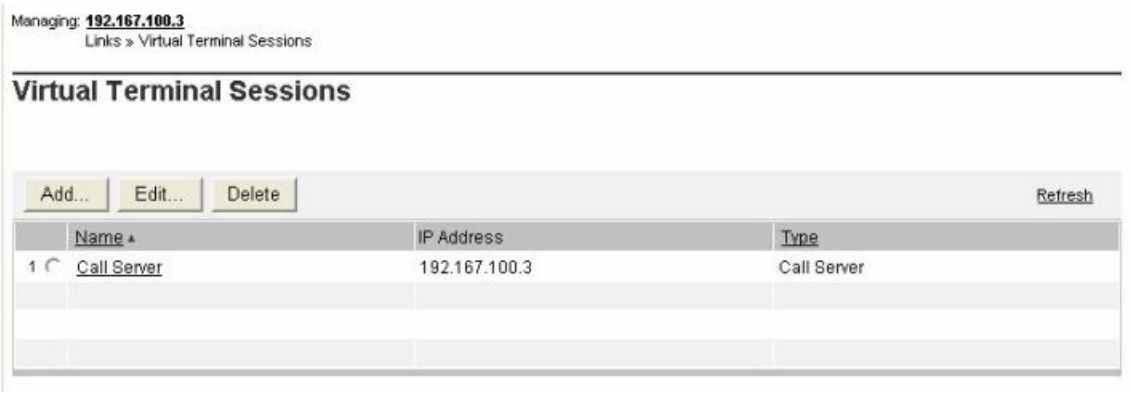


Figure 3: Virtual Terminal Sessions Web page

The Virtual Terminal Sessions Web page enables users to bookmark the connection details to any IP-based element on the network. Virtual Terminal can be used to connect to an element which supports Telnet, Rlogin or SSH2.

Virtual Terminal (VT) sessions are secured using SSL and SSH. If the element doesn't support SSH then normal TCP fallback is also provided (either to the Telnet or Rlogin server) to connect to the elements.

Important:

Java Runtime Environment (JRE) version 1.5 or higher must be installed for the Virtual Terminal Emulator to run properly.

Follow the steps in Adding a Virtual Terminal session on page 38 to add a Virtual Terminal Session .

Adding a Virtual Terminal session

1. On the Virtual Terminal Sessions Web page, click **Add**.

   The Add Virtual Terminal Session Web page appears, as shown in Figure 4: Add Virtual Terminal Session Web page on page 38.

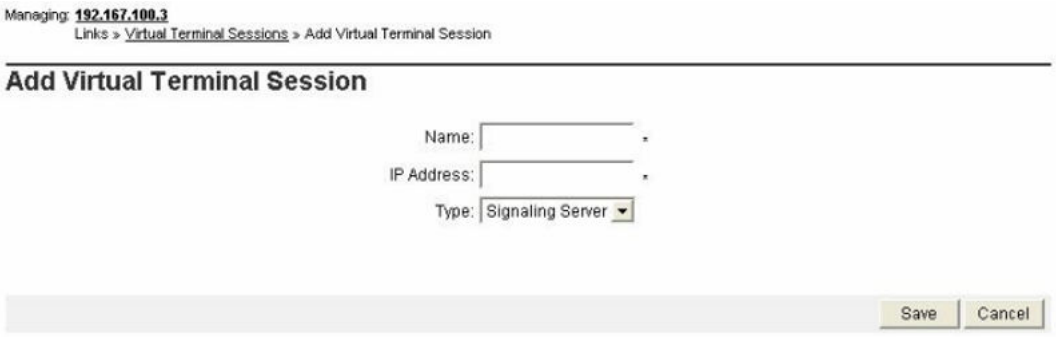


Figure 4: Add Virtual Terminal Session Web page

2. Type the **Name** and **IP Address** for the session.

3. From the list, select the **Type**.
4. Click **Save** to save.

   OR

   To cancel the session, click **Cancel**.

To access a Virtual Terminal Session that is already created, click the name of the Virtual Terminal Session on the Virtual Terminal Sessions Web page. A Virtual Terminal window appears in a separate browser window.

Note:

Virtual terminal prompts for pdt2 password, but you can press Enter and give the admin1 or admin2 password to get connected, and pdt2 password is not mandatory if you start Virtual Terminal through UCM.

Note:

Upon initial launch of Virtual terminal, the user is prompted for the PDT2 level password. Entering this password will navigate user to the PDT2 shell of the Call Server. The user can also carriage return past the PDT2 password prompt. This action will prompt the user for a new username for other accounts on the Call Server. The user can provide admin1 or admin2 login credentials allowing overlay access to the Call Server.

Note:

For security reasons, each Virtual Terminal session is forced to time out in 20 minutes.

The Virtual Terminal window provides a menu with the following items:

- Current Overlay
- Current Prompt
- Search M1 Help Files
- About Terminal Client

When the user enters an overlay, the Current Overlay and Current Prompt menu items are enabled.

Click the **Help -> Current Overlay** link to open a Help window containing help for that particular overlay.

Click the **Help -> Current Prompt** link to open a Help window explaining the definition of the prompt, along with acceptable responses.

Follow the steps in Editing an existing Virtual Terminal session on page 39 to edit an existing Virtual Terminal session.

Editing an existing Virtual Terminal session

1. Select the radio button beside the appropriate Virtual Terminal name on the Virtual Terminal Sessions Web page.
2. Click **Edit**.

The information about the Virtual Terminal Session selected is displayed in the fields.

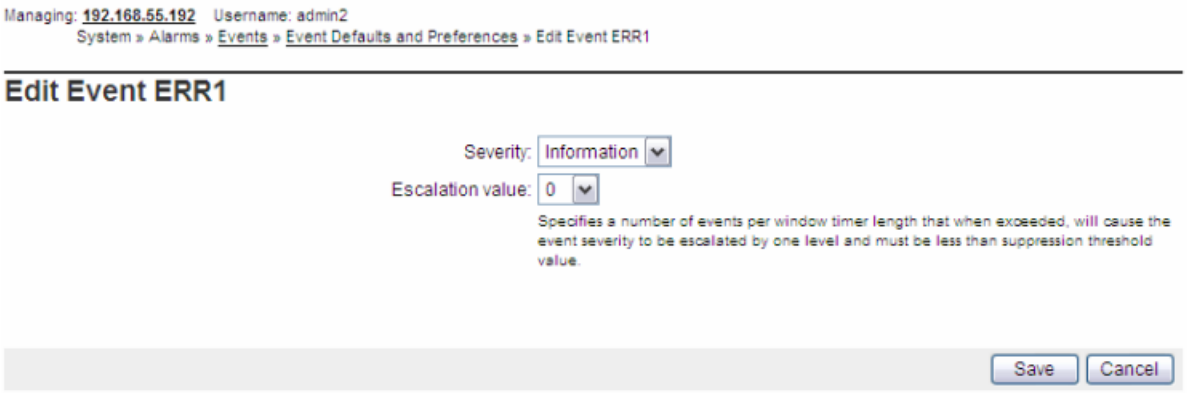
3. Edit the **Name** and **IP Address** values as necessary.
4. To change this session so that it logs into a Call Server, select the **Call Server** check box.
5. Click **Save** to save the changes.
6. Click **Cancel** to undo any changes made.

Deleting an existing Virtual Terminal Session

1. Select the radio button beside the appropriate Virtual Terminal name on the Virtual Terminal Sessions Web page.
2. Click **Delete** to remove the Virtual Terminal Session information completely.

Edit Event ERR1

This Edit Event ERR1 Web page contains site-specific preferences for event severities as well as criteria for severity escalation.



This page contains two fields as follows:

- **Severity**: User can change the severity of the event by changing the value of this field. It has the following options:

  - Default
  - Information
  - Minor
  - Major
  - Critical

- **Escalation value**: The escalation threshold specifies a number of events per window timer length that, when exceeded, causes the event severity to be escalated up one level. The window timer length is set to 0 minute by default. Escalation occurs only for minor or

major alarms. Escalation value must be less than the universal suppression threshold value. This field can have values from 0 to 14.

Chapter 7: System

Contents

This chapter contains information about the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Introduction

The **System** branch of the Element Manager navigator provides access to diagnostic tools that enable users to issue a variety of commands to the components of the CS 1000 system.

The following buttons appear on some or all of the System Web pages:

- **Submit** — Transmits changes to the Call Server.
- **Refresh** — Refreshes data from the Call Server. Refresh overwrites any changes not yet submitted.
- **Cancel** — Discards the changes and returns to the appropriate configuration Web page.

Events

To configure or edit Events information, click the **Alarms > Events** link in the **System** branch of the Element Manager navigator. The Events Web page appears as shown in Figure 5: Events Web page on page 45.

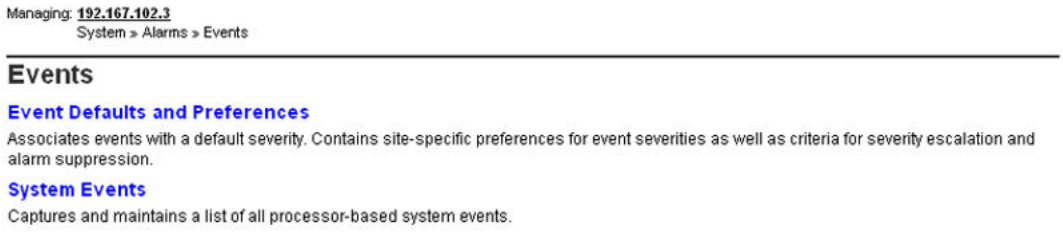


Figure 5: Events Web page

To display event default severity, event thresholds and site-specific event preferences, click the **Event Defaults and Preferences** link to open the Event Defaults and Preferences Web page as shown in Figure 6: Event Defaults and Preferences Web page on page 46.

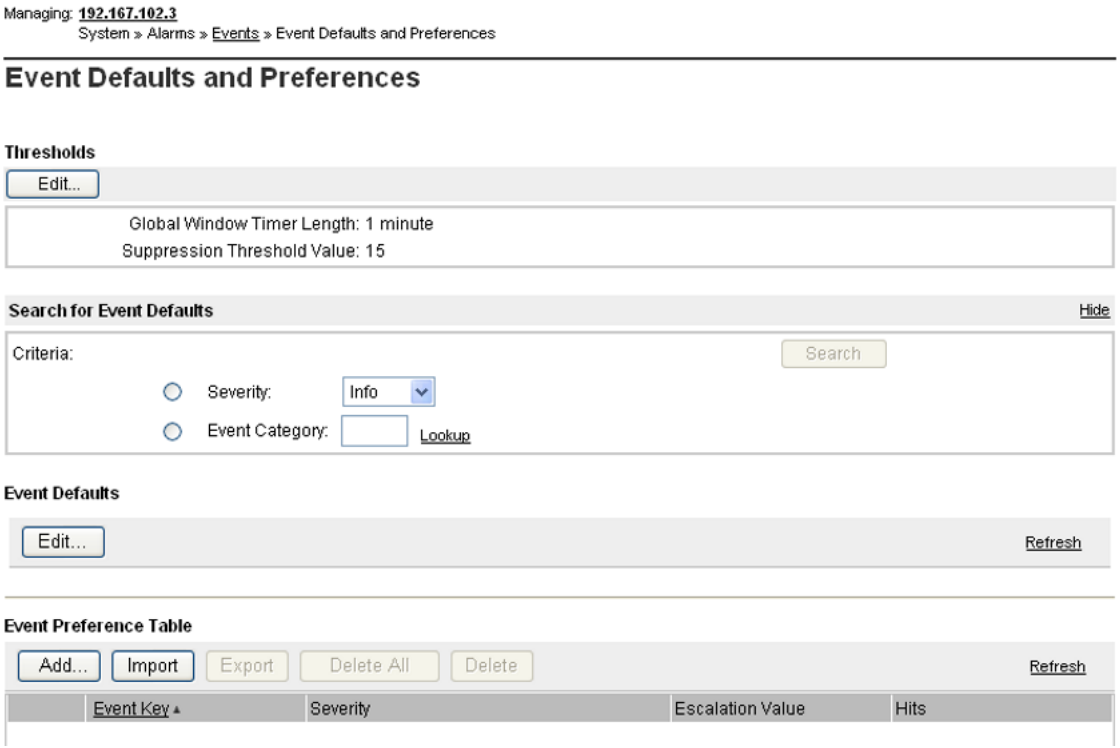


Figure 6: Event Defaults and Preferences Web page

To edit the **Suppression Threshold Value** and **Global Window Timer Length** that are common to all events, in the **Thresholds** section click **Edit**. The Edit Thresholds Web page appears as shown in Figure 7: Edit Thresholds Web page on page 46.

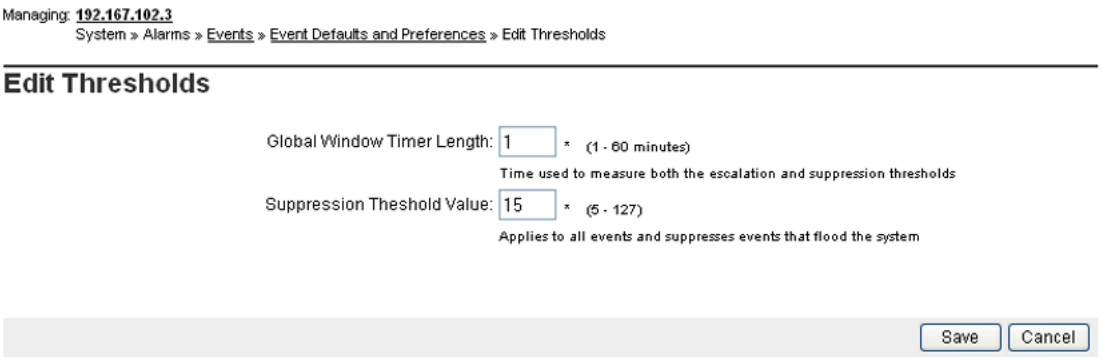


Figure 7: Edit Thresholds Web page

Enter the desired changes and click **Save**.

Search for event defaults by clicking either the **Severity** or **Event Category** radio buttons. Type the search criteria and click **Search**. The results appear in the **Event Defaults** section.

To maintain a list of system events, from the Events Web page click the **System Events** link. The System Events Web page appears as shown in Figure 8: System Events Web page on page 47.

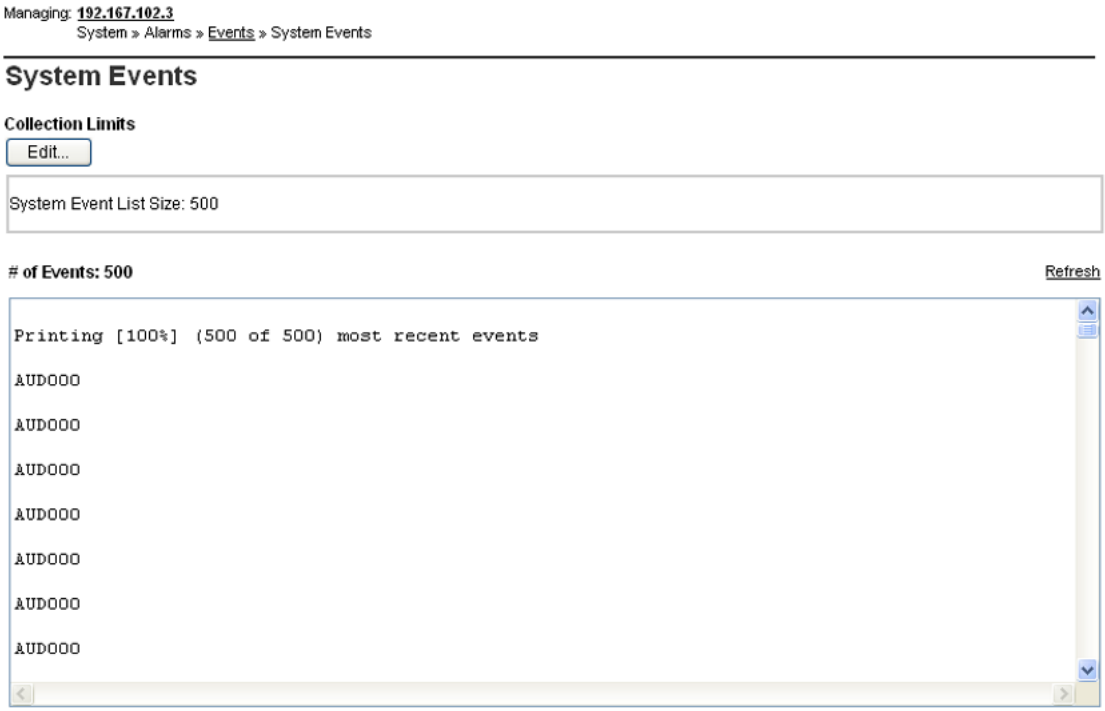


Figure 8: System Events Web page

The **System Event List Size** value in the **Collection Limit** section is the upper limit to the number of events collected in the System Event List. To edit this limit, click **Edit**.

All events collected in the system event list are displayed in the text area at the bottom of the page.

Use this page to import an Event Preference Table from a user specified location to the switch.

Import Event Preference Table (EPT)

Use this page to import an Event Preference Table from a user specified location to the switch.

To display this page, choose **System > Alarms > Events > Event Defaults and Preferences**. In the **Event Preference Table** section, click **Import**.

The Event Preference Table page appears.

Note:

The user must change the Security settings in Microsoft Internet Explorer while importing the EPT. This file resides at the user PC which uses ActiveX FileSystemObject for validation. This provides access to the local file system of the PC using even JavaScript code. Microsoft IE has a field called "Initialize and script ActiveX controls not marked as safe" under **IE -> Tools -> Security -> Custom Level**. This field must be configured either to "Prompt" or "Enable". When this field is disabled, IE cannot create ActiveX objects, which causes an error called "Automation server can not create object" and validation for the file fails. If the IE Security level setting is High, ActiveX controls are not allowed. Therefore, configure the IE security level to Medium, with the specified field configured to either "Prompt" or "Enable".

Import Event Preference Table

1. Click **Browse**, to browse for the Event Preference Table.
2. Click **Import & Activate** to import the Event Preference Table to the switch.
3. Click **Cancel** to return to the Event Defaults and Preferences page, without importing a Event Preference Table to the switch.

SNMP

The SNMP Profile Manager provides a common interface for configuring SNMP parameters on all CS 1000 Network Elements. You can use SNMP Profile Manager which is part of the UCM solution, to add, modify and delete SNMP profiles. Profiles can be configured and assigned to the following types of UCM managed elements:

- Element Manager
- Call Server (configuration settings are migrated to the SS, VGMC, and MGC)
- NRSM (configuration settings are migrated to NRS)

Fault management is implemented in Element Manager.

To configure or edit SNMP information, click the **Alarms > SNMP** link in the System branch of the Element Manager navigator. The SNMP Configuration Web page appears as shown in Figure 9: SNMP Configuration Web page on page 49.

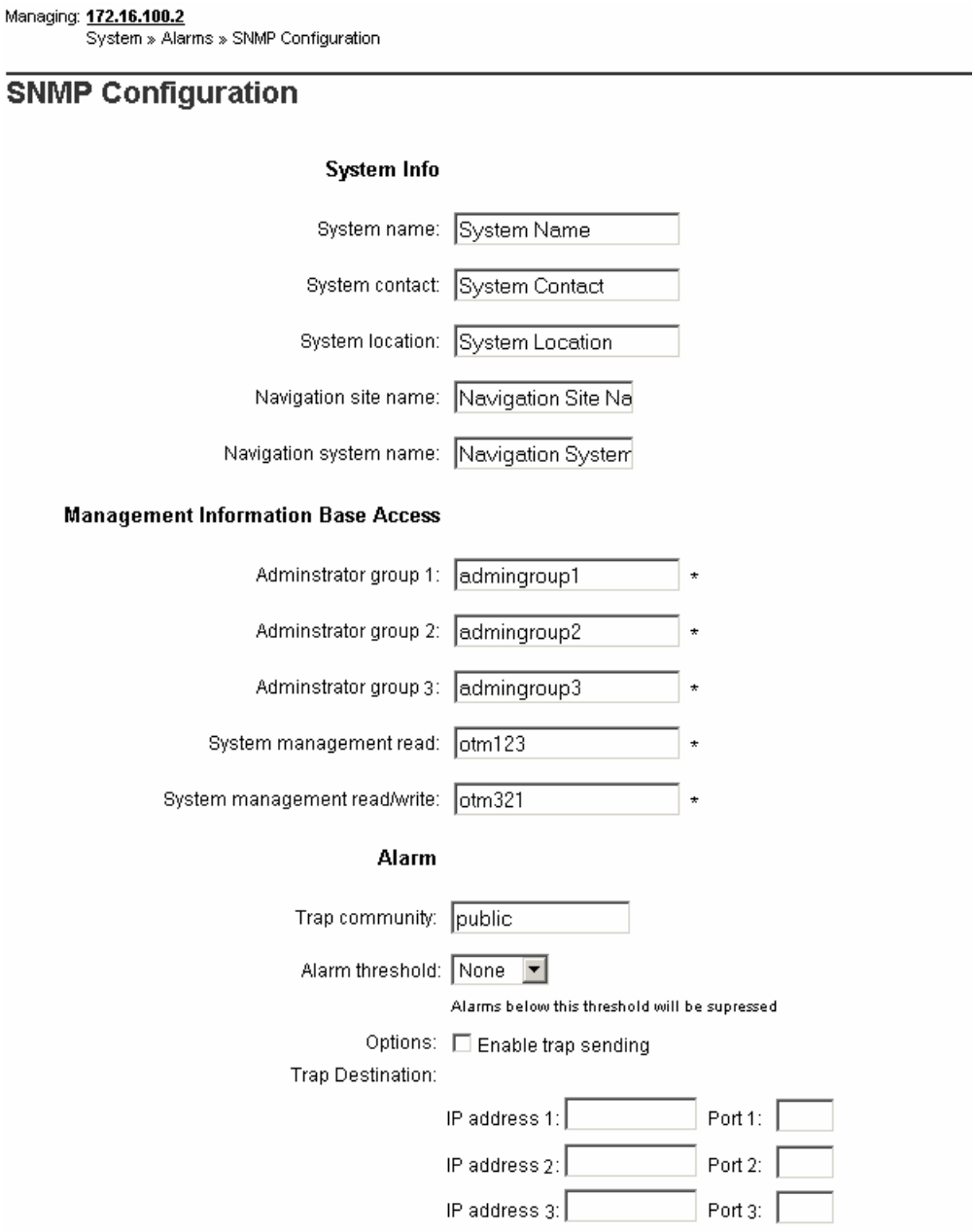


Figure 9: SNMP Configuration Web page

The information entered on this Web page corresponds to the SNMP data traditionally configured using LD 117 - Ethernet and Alarm Management.

The SNMP parameters are grouped in three logical groups in the SNMP Configuration Web page:

- System Info
- Management Information Base Access
- Alarm

Configuration of SNMP by Element Manager at the system level propagates upward to the SNMP Profile Manager. Changes made in Element Manager apply to all CS 1000 elements.

For detailed information about SNMP, see *Avaya Communication Server 1000 Fault Management - SNMP, NN43001-719*.

Maintenance

When the user clicks the **Maintenance** link in the **System** branch of the Element Manager navigator, the Maintenance Web page appears. The user can choose how the options appear. If the user chooses **Select by Functionality**, the diagnostic tool options appear according functionality as shown in Figure 10: Maintenance diagnostic tools presented by functionality on page 51.

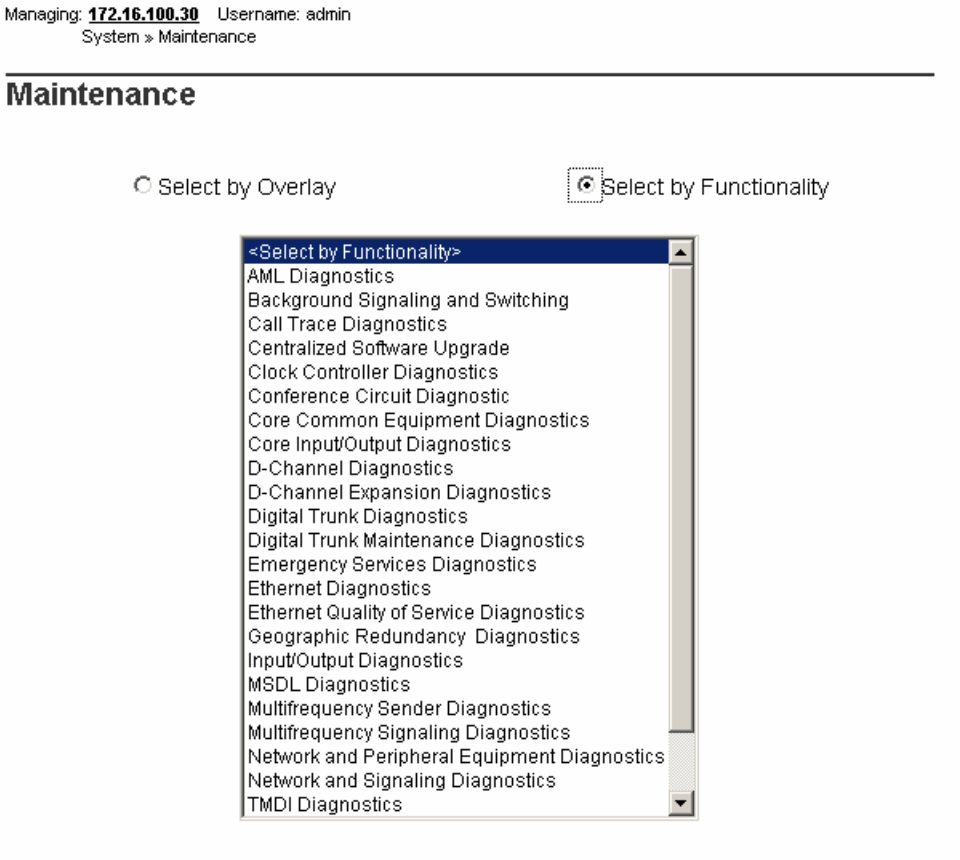


Figure 10: Maintenance diagnostic tools presented by functionality

The following tool options are available from this Web page:

- AML Diagnostics
- Background Signaling and Switching
- Call Trace Diagnostics
- Centralized Software Upgrade
- Clock Controller Diagnostics
- Conference Circuit Diagnostic
- Core Common Equipment Diagnostics
- Core Input/Output Diagnostics
- D-Channel Diagnostics
- D-Channel Expansion Diagnostics
- Digital Trunk Diagnostics
- Digital Trunk Maintenance Diagnostics
- Emergency Services Diagnostics
- Ethernet Diagnostics

- Ethernet Quality of Service Diagnostics
- Geographic Redundancy Diagnostics
- Input/Output Diagnostics
- InterGroup Switch & System Clock
- MSDL Diagnostics
- Multifrequency Sender Diagnostics
- Multifrequency Signaling Diagnostics
- Network and Peripheral Equipment Diagnostics
- Network and Signaling Diagnostics
- TMDI Diagnostics
- Tone and Digit Switch Diagnostics
- Trunk Diagnostics
- Zone Diagnostics

Note:

Depending on the type of system being accessed, not all options may be available.

If the user chooses **Select by Overlay**, the following options appear according to LD numbers, as shown in Figure 11: Call Server diagnostic tools presented by overlay on page 53:

- LD 30 - Network and Signaling
- LD 32 - Network and Peripheral Equipment
- LD 34 - Tone and Digit Switch
- LD 36 - Trunk
- LD 37 - Input/Output
- LD 38 – Conference Circuit
- LD 39 - Intergroup Switch and System Clock
- LD 45 - Background Signaling and Switching
- LD 46 - Multifrequency Sender
- LD 48 - Link
- LD 54 - Multifrequency Signaling
- LD 60 - Digital Trunk Interface and Primary Rate Interface
- LD 75 - Digital Trunk
- LD 80 - Call Trace
- LD 96 - D-Channel
- LD 117 - Ethernet and Alarm Management
- LD 135 - Core Common Equipment

- LD 137 - Core Input/Output
- LD 143 - Centralized Software Upgrade

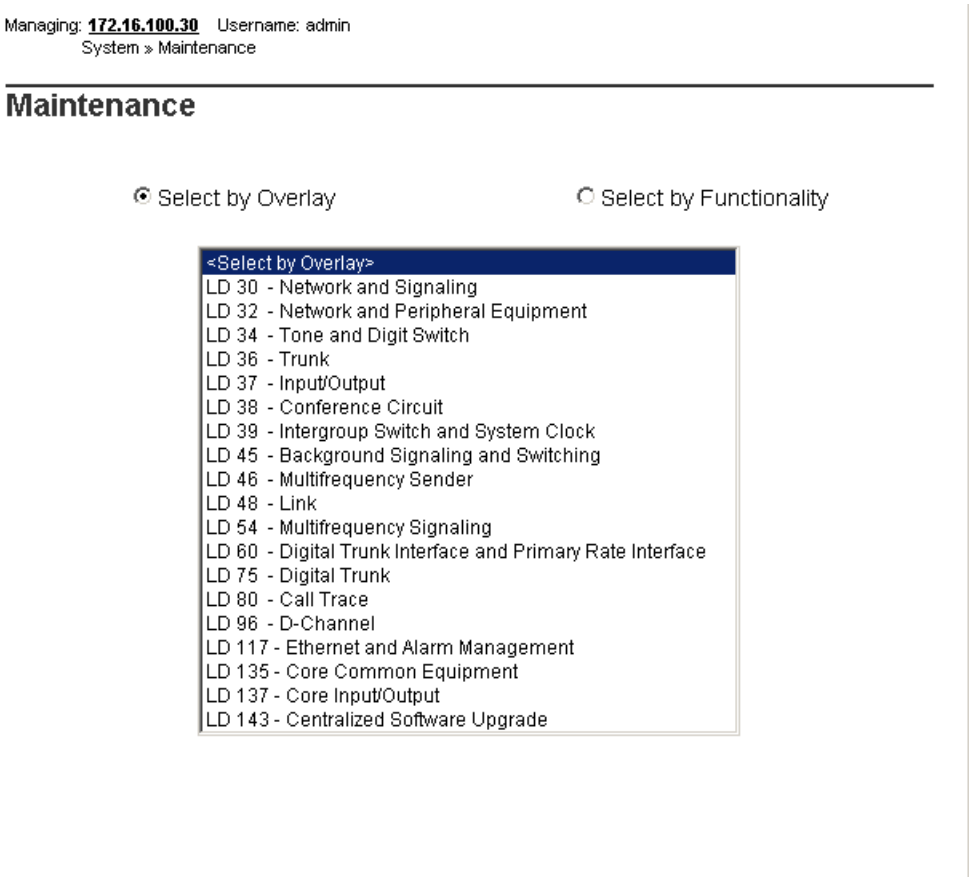


Figure 11: Call Server diagnostic tools presented by overlay

If selecting an overlay that corresponds to more than one functionality, choose the desired functionality in the **Select Group** list, as shown in Figure 12: Select Group list on page 54.

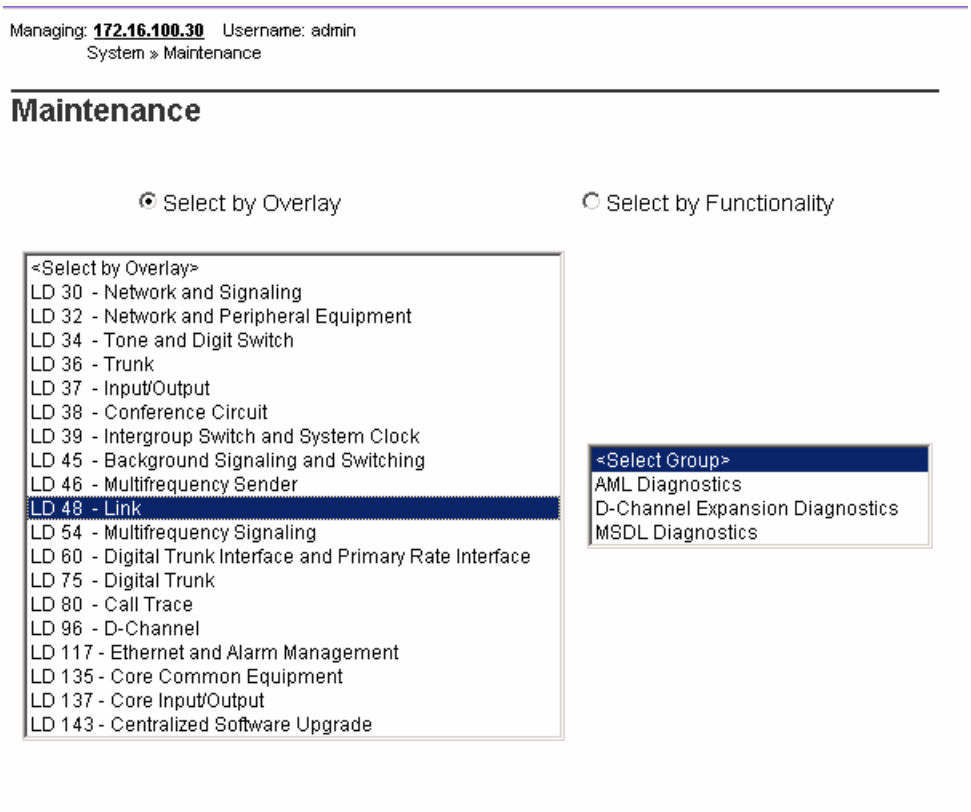


Figure 12: Select Group list

This document presents the options by functionality, with cross-references to the appropriate overlay.

The following sections provide information about each functionality.

Application Module Link Diagnostics

Click the **AML Diagnostics** link in the list of **Maintenance** functions to open the Link: AML Diagnostics Web page as shown in Figure 13: AML Diagnostics Web page on page 55.

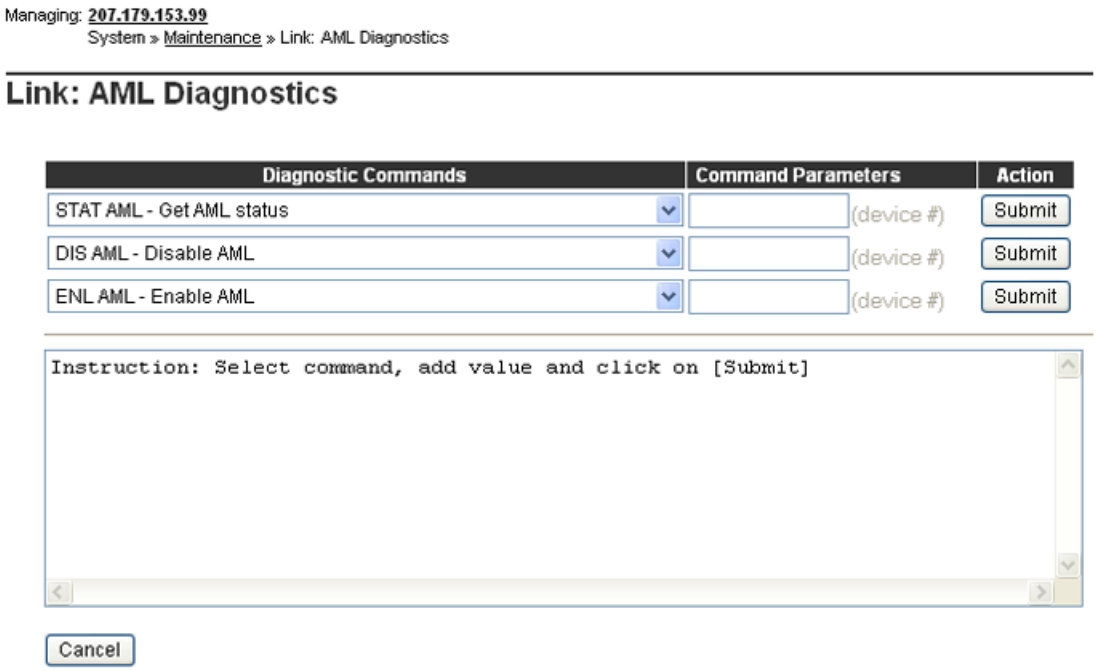


Figure 13: AML Diagnostics Web page

The commands available from this Web page correspond to the AML diagnostics traditionally performed by using LD 48.

To perform AML commands using this Web page, follow the steps in Performing AML commands on page 55.

Performing AML commands

1. Select one of the following commands from the first **Commands** list:
    a. STAT AML - Get AML status
    b. STAT ELAN - Check status of all specified / all configured ELANs
    c. EST AML - Establish layer 2 on AML
    d. MAP AML - Get card information of one or all AMLs
    e. RLS AML - Release layer 2 on AML
    f. SLFT AML - Perform self-test on AML
    g. UPLD AML - Upload parameter table 1 to 4 from AML
2. (Optional) Enter the device number in the **Command Parameters** text box.
3. Click **Submit**.

To disable AML using this Web page, follow the steps in Disabling AML on page 55.

Disabling AML

1. Select one of the following commands from the second **Commands** list:

a. DIS AML - Disable AML
b. DIS AML - Disable AUTO recovery on AML
c. DIS AML - Disable layer 2 on AML
d. DIS AML - Disable layer 7 on AML
e. DIS AML - Disable MDL error reporting on AML
f. DIS ELAN - Disable ELAN (server/client task)

2. (Optional) Enter the device number in the **Command Parameters** text box.
3. Click **Submit**.

To enable AML using this Web page, follow the steps in Enabling AML on page 56.

Enabling AML

1. Select one of the following commands from the third **Commands** list:
   a. ENL AML - Enable AML
   b. ENL AML - Enable Automatic set-up on AML
   c. ENL AML - Enable AUTO recovery on AML
   d. ENL AML - Enable Layer 2 on AML
   e. ENL AML - Enable Layer 7 on AML
   f. ENL AML - Enable MDL error reporting on AML
   g. ENL ELAN- Enable ELAN (server task)
2. (Optional) Enter the device number in the **Command Parameters** text box.
3. Click **Submit**.

Background Signaling and Switching Diagnostics

The Background Signaling and Switching diagnostics Web page is applicable only to Large Systems.

Click the **Background Signaling and Switching** link in the list of **Call Server** functionalities to open the Background Signaling and Switching Diagnostics Web page, as shown in Figure 14: Background Signaling and Switching Diagnostics Web page on page 57.

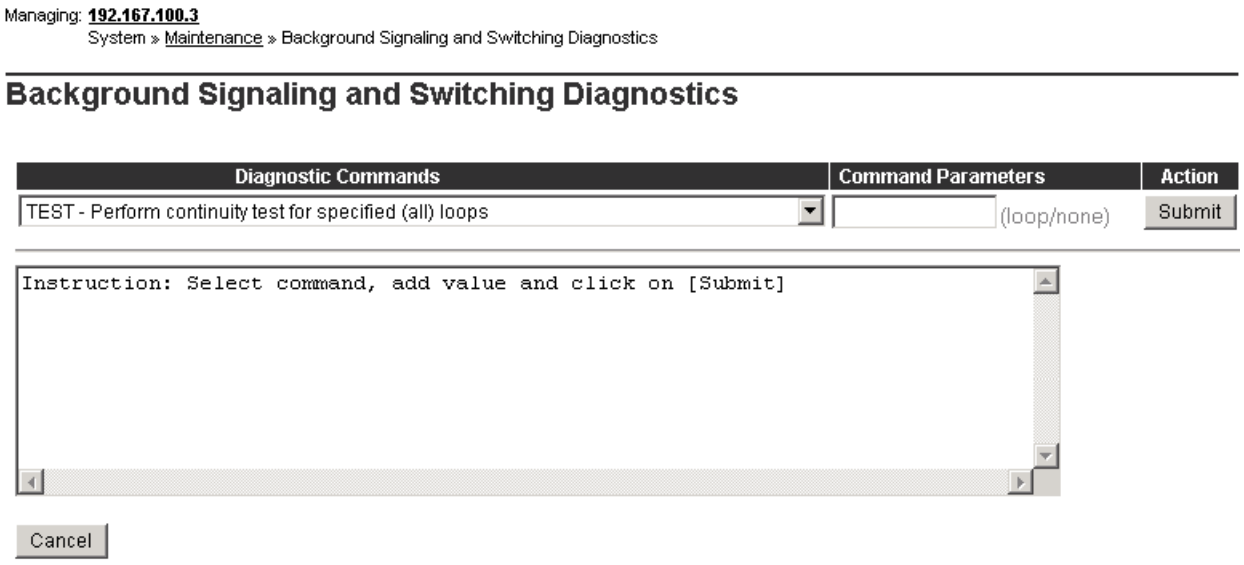


Figure 14: Background Signaling and Switching Diagnostics Web page

The commands available from this Web page correspond to the Background Signaling and Switching command traditionally performed using LD 45 - Background Signaling and Switching Diagnostics.

This Web page is used to perform the TEST command. This command performs a continuity test for specified loops.

Performing the TEST command

1. Select the **Diagnostic Command** from the list.
2. Enter the loop number in the **Command Parameters** box.

   Note:

   To run the TEST command on all loops, leave the **Command Parameters** box empty.
3. Click **Submit**.

Call Trace Diagnostics

Click the **Call Trace Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Call Trace Diagnostics Web page, as shown in Figure 15: Call Trace Diagnostics Web page on page 58.

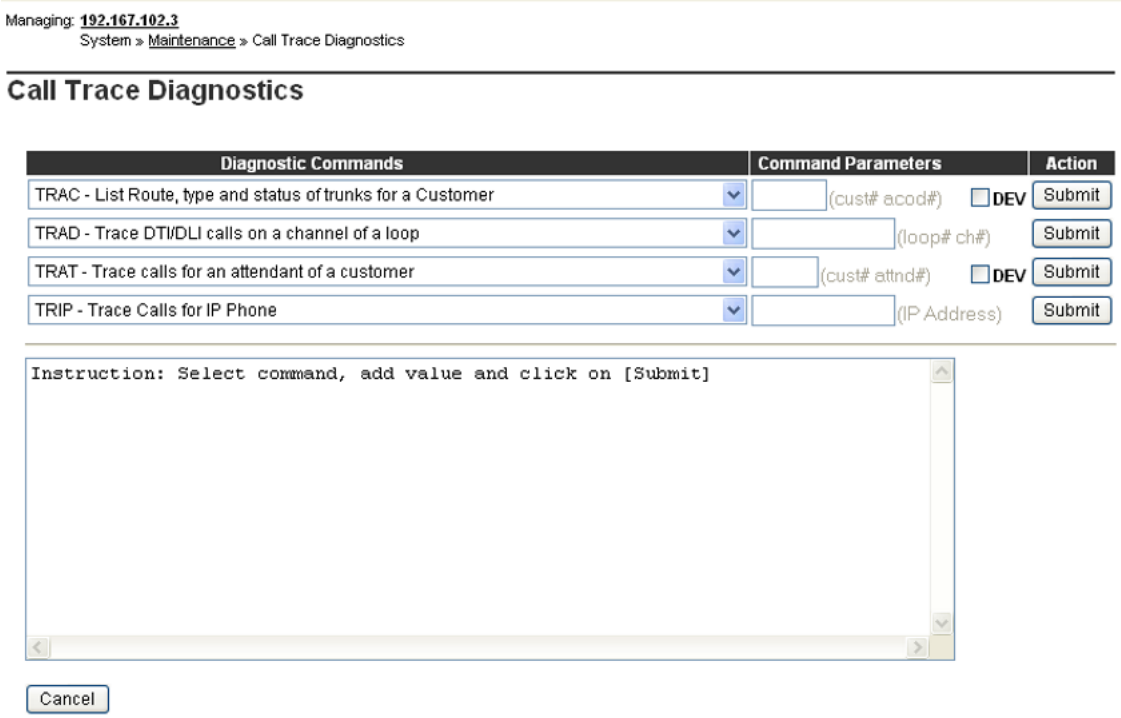


Figure 15: Call Trace Diagnostics Web page

The commands available from this Web page correspond to the Call Trace diagnostics traditionally performed by using LD 80 - Call Trace Diagnostics.

This Web page is used to perform the following Call Trace functions:

- TRAC commands
- TRAD commands
- TRAT commands
- TRIP commands

To perform TRAC commands, follow the steps in Performing TRAC commands on page 58.

Note:

To issue a detailed call trace select the DEV checkbox.

Performing TRAC commands

1. Select one of the following commands from the first Commands list:
    a. TRAC - List Route, type and status of trunks for a Customer
    b. TRAC - Trace calls for specified customer and DN/LSC DN

c. TRAC - Trace calls for specified customer, route and member
d. TRAC - Trace calls on specified Digital Subscriber Loop (0-7)
e. TRAC - Trace calls associated with the specified unit
f. TRAC - Trace calls on specified key for specified unit

2. Enter the customer number and the acod number in the **Command Parameters** text box.
3. Click **Submit**.

To perform TRAD commands, follow the steps in Performing TRAD commands on page 59.

Performing TRAD commands

1. Select the following command from the second **Commands** list:
   - TRAD - Trace DTI/DLI calls on a channel of a loop
2. Enter the loop number and channel number in the **Command Parameters** text box.
3. Click **Submit**.

To perform TRAT commands, follow the steps in Performing TRAT commands on page 59.

Note:
To issue a detailed call trace select the DEV checkbox.

Performing TRAT commands

1. Select one of the following commands from the third **Commands** list:
   a. TRAT - Trace calls for an attendant for a customer
   b. TRAT - Trace calls on a key of an attendant of a customer
   c. TRAT - Trace attendant calls for a unit
   d. TRAT - Trace attendant calls on specified key of a unit
2. Enter the customer number and attendant number in the **Command Parameters** text box.
3. Click **Submit**.

To perform TRIP commands, follow the steps in Performing TRIP commands on page 59.

Performing TRIP commands

1. Select the following command from the fourth **Commands** list:

   TRIP - Trace calls for IP Phone
2. Enter the required parameters in the **Command Parameters** text box.
3. Click **Submit**.

Centralized Software Upgrade

Click the **Centralized Software Upgrade** link in the list of **Maintenance** diagnostic tools to open the Centralized Software Upgrade Web page, as shown in Figure 16: Centralized Software Upgrade Web page on page 60.

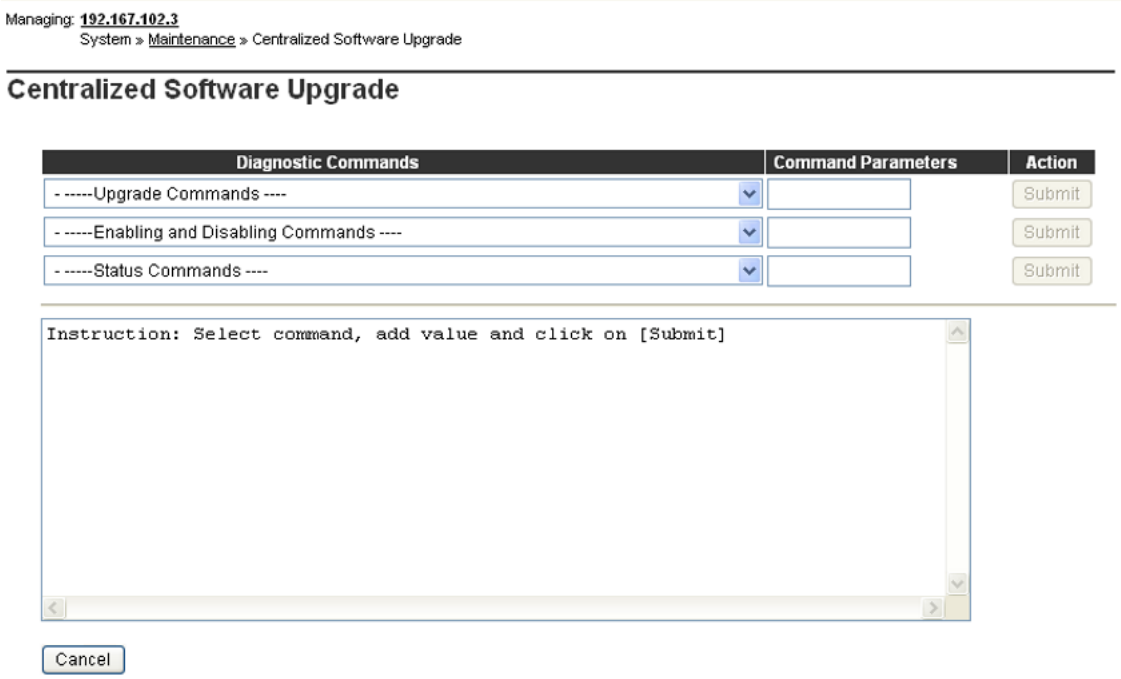


Figure 16: Centralized Software Upgrade Web page

To perform Upgrade commands, follow the steps in Performing Upgrade commands on page 60.

Performing Upgrade commands

1. Select the following commands from the first **Commands** list:
    a. UPGMG - Upgrade IPMG
    b. UPGMG ALL - Upgrade ALL IPMGs
    c. UPGMGCOMMIT - Initiate Reboot of the IPMG after upgrade
    d. UPGMGCOMMI ALL - Initiate Reboot of all the IPMG after upgrade

e. UPGMGBOOT - Upgrade the bootrom of the IPMG

2. Enter the required parameters in the **Command Parameters** text box.
3. Click **Submit**.

To perform Enabling and Disabling commands, follow the steps in Performing Enabling and Disabling commands on page 61.

Performing Enabling and Disabling commands

1. Select the following commands from the second **Commands** list:
    a. ENL AUTOUPGMG - Enable Automatic Software Upgrade
    b. DIS AUTOUPGMG - Disable Automatic Software Upgrade
2. If ENL AUTOUPGMG is used, select either SEQ or SIM from the menu.
3. Click **Submit**.

To perform Status commands, follow the steps in Performing Status commands on page 61.

Performing Status commands

1. Select the following commands from the third **Commands** list:
    a. PRT AUTOUPGMG - Displays settings of Automatic Software Upgrade feature
    b. UPGMG STAT - Provides display details of the specified IPMG upgrade status
    c. UPGMGSETUP - Display the current CSU Setting
    d. UPGMGABORT - Abort and display centralized software upgrades
    e. HELP - Provides a list of all supported commands
2. If UPGMG STAT is used, enter the Superloop # and Shelf # in the **Command Parameters** text box.
3. Click **Submit**.

Clock Controller Diagnostics

Click the **Clock Controller Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Digital Trunk Interface and Primary Rate Interface: Clock Controller Diagnostics Web page as shown in Figure 17: Digital Trunk Interface and Primary Rate Interface: Clock Controller Diagnostics Web page on page 62.

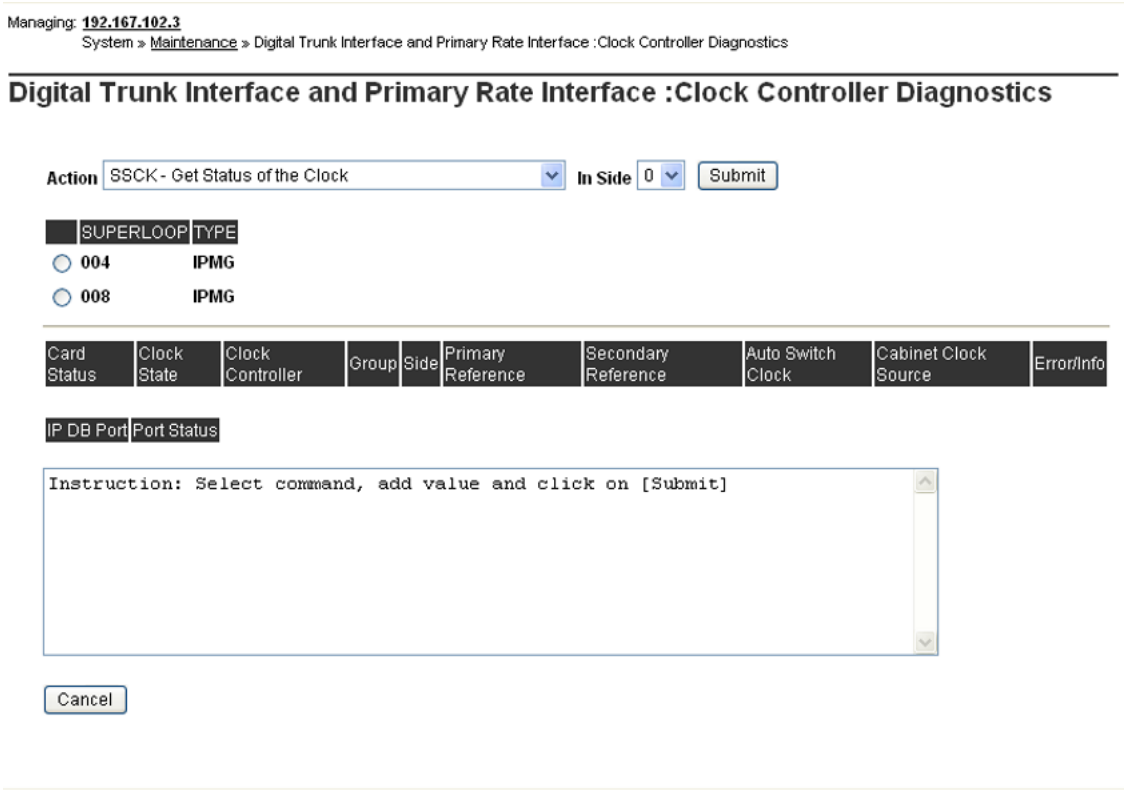


Figure 17: Digital Trunk Interface and Primary Rate Interface: Clock Controller Diagnostics Web page

This Web page is used to maintain the digital trunk interface and the primary rate interface clock controllers.

The commands available from this Web page correspond to the Clock Controller data traditionally maintained by using LD 60 - Digital Trunk Interface and Primary Rate Interface Clock Controller.

This Web page shows the status of the Clock Controller card.

To perform Clock Controller maintenance activities using this Web page follow the steps in Performing Clock Controller maintenance activities on page 62.

Performing Clock Controller maintenance activities

1. Select one of the following commands from the **Action** list:
    a. SSCK - Get Status of the Clock
    b. ENL CC - Enable the Clock
    c. DIS CC - Disable the Clock
    d. TRCK - Set the Clock Controller
    e. DSCK - Disable the clock for loop

f. ENCK - Enable the secondary clock reference for card
g. EREF - Enable auto switchover of reference clocks
h. IDC - Get card ID of Clock Controller Card
i. MREF - Disable switchover of system clocks
j. SEFT CC - Execute self test

2. Select a Cabinet number from the **In Side** list.
3. Select the appropriate sub-parameters.
4. Click**Submit**.

Core Common Equipment Diagnostics

Click the **Core Common Equipment Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Core Common Equipment Diagnostics Web page, as shown in Figure 18: Core Common Equipment Diagnostic Web page on page 63.

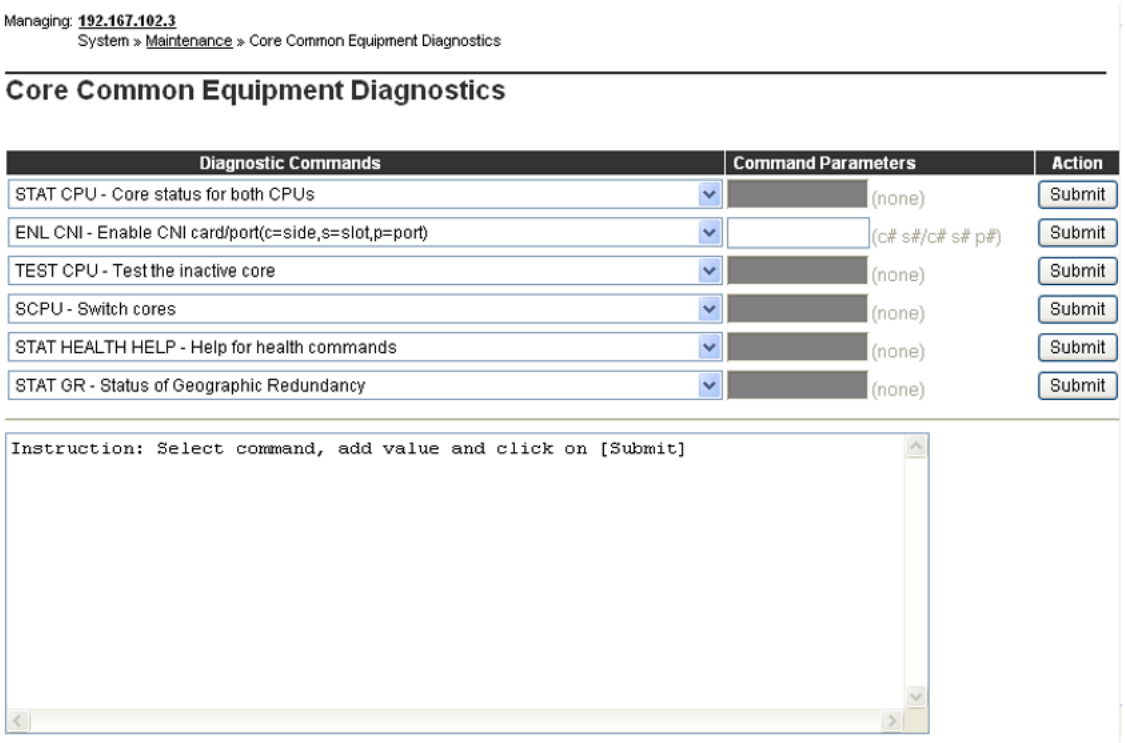


Figure 18: Core Common Equipment Diagnostic Web page

The commands available from this Web page correspond to the Core Common Equipment data traditionally maintained by using LD 135 - Core Common Equipment.

To execute status commands using this Web page, follow the steps in Performing Core Common Equipment Status commands on page 64.

Performing Core Common Equipment Status commands

1. Select one of the following commands from the first **Commands** list:
    a. STAT CPU - Core status for both CPUs
    b. STAT CNI - Status of configured CNI (c=side, s=slot, p=port)
    c. STAT MEM - Status of SIMMs on both CPs
    d. STAT EXT - Status of all Extender pair designations
    e. STAT SUTL - Status of system utility
2. Enter appropriate **Command Parameters** wherever applicable.
3. Click **Submit**.

To execute CNI commands using this Web page, follow the steps in Performing Core Common Equipment CNI commands on page 64.

Performing Core Common Equipment CNI commands

1. Select one of the following commands from the second **Commands** list:
    a. ENL CNI - Enable CNI card/port (c=side, s=side, p=port)
    b. DIS CNI - Disable CNI all, card or port
    c. DSPL - Display active core contents
    d. DSPL ALL - Display active core contents for all
    e. IDC CPU - Print card ID for active core
    f. IDC CNI - Print card ID for CNI on active side
    g. ENL EXT - Enable specified Extender pair
2. Enter the required parameters in the **Commands Parameters** text box.
3. Click **Submit**.

To execute test commands using this Web page, follow the steps in Performing Core Common Equipment test commands on page 64.

Performing Core Common Equipment test commands

1. Select one of the following commands from the third **Commands** list:
    a. TEST CPU - Test the inactive core
    b. TEST CNI - Test CNI card/port (c=card, s=slot, p=port)
    c. TEST IPB - Test backplane on Secondary Interprocessor Bus
    d. TEST LCD - Test the LCD display on the active CP card
    e. TEST LED - Test LEDs

f. TEST SUTL - Test system utility

2. Enter appropriate **Command Parameters** wherever applicable.
3. Click **Submit**.

To execute miscellaneous commands using this Web page, follow the steps in Performing Core Common Equipment miscellaneous commands on page 65.

Performing Core Common Equipment miscellaneous commands

1. Select one of the following commands from the fourth **Commands** list:
    a. SCPU - Switch cores
    b. SPLIT - Put a redundant system into single mode
    c. CDSP - Clear maintenance displays
    d. CMAJ - Clear major alarm and reset power fail transfer
    e. CMIN - Clear the minor alarm for all customers
    f. CUTOVR - Transfer call processing from active to standby cores
    g. JOIN - Synchronize the memory and drives
2. Click **Submit**.

To execute status health commands using this Web page, follow the steps in Performing Core Common Equipment status health commands on page 65.

Performing Core Common Equipment status health commands

1. Select one of the following commands from the fifth **Commands** list:
    a. STAT HEALTH HELP - Help for health commands
    b. STAT HEALTH - Overall health status
    c. STAT HEALTH AML - AML health status
    d. STAT HEALTH DSPDB - DSP Daughterboard health status (applicable only to systems with Media Gateway Controllers containing DSP Daughterboards)
    e. STAT HEALTH IPL - IPL health status
    f. STAT HEALTH ELAN - ELAN health status
    g. STAT HEALTH HW - Hardware health status
2. Click **Submit**.

To execute Geographic Redundancy commands using this Web page, do the following:

Performing Core Common Equipment Geographic Redundancy commands

1. Select one of the following commands from the sixth **Commands** list:
    a. STAT GR - Status of Geographic Redundancy
    b. TEST GR - Test Geographic Redundancy

c. CLR GR - Clear operation for the secondary CS

2. Enter appropriate **Command Parameters** wherever applicable.
3. Click **Submit**.

Core Input/Output Diagnostics

Click the **Core Input/Output Diagnostics** link in the list of **Maintenance** tools to open the Core Input/Output Diagnostics Web page as shown in Figure 19: Core Input/Output Diagnostics Web page on page 66.

This Web page is used to obtain the status of PPP and Ethernet links. The commands available from this Web page correspond to the tools traditionally maintained using LD 137 - Core Input/Output Diagnostics.

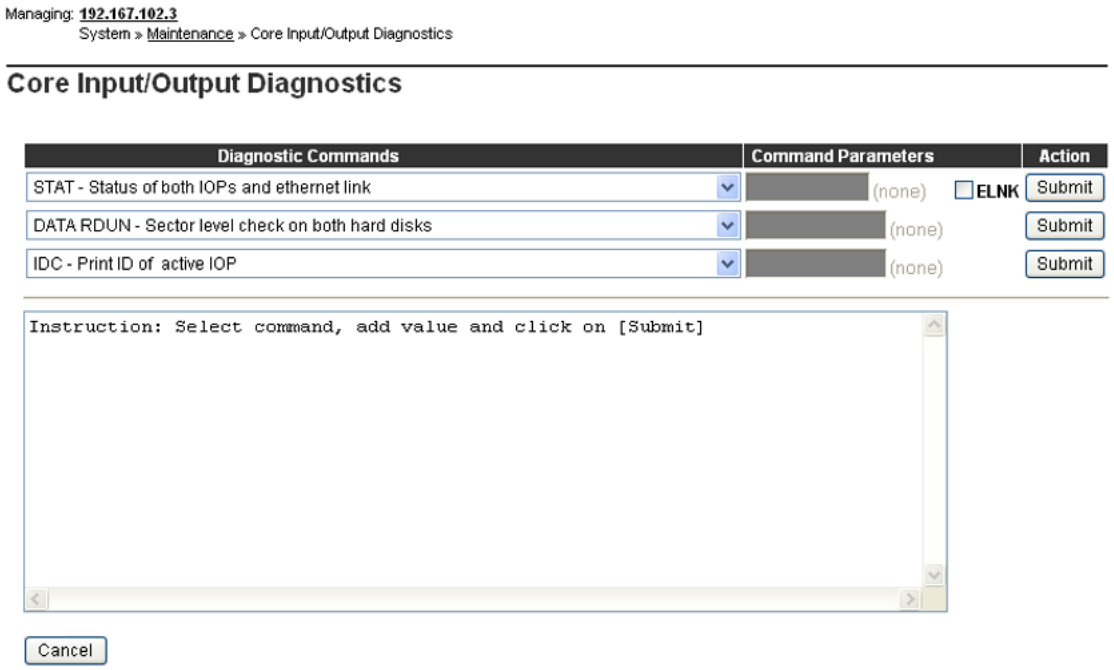


Figure 19: Core Input/Output Diagnostics Web page

To perform diagnostic commands using this Web page, follow the steps in Performing Core Input/Output diagnostic commands on page 66.

Performing Core Input/Output diagnostic commands

1. Use the first **Commands** list to perform the following diagnostic activities:

   a. STAT - Status of both IOPs and CMDUs and ethernet link

b. STAT RDUN - Status of both disks
c. STAT FMD - Status of active Fixed Media Devices
d. STAT RMD - Status of active Removable Media Devices

2. Click **Submit**.
3. Use the second **Commands** list to perform the following diagnostic activities:
    a. DATA RDUN - Sector level check on both hard disks
    b. TEST RDUN - Test file level check on both hard disks
4. Click **Submit**.
5. Use the third **Commands** list to perform the following diagnostic activities:
    a. IDC - Print IDs of both CMDUs and active IOP
    b. SDID - Display security device information
6. Click **Submit**.

Network and Conference Circuit Diagnostic

Click the **Conference Circuit** link in the list of **Maintenance** diagnostic tools to open the **Conference Circuit** Web page as shown in the following figure.

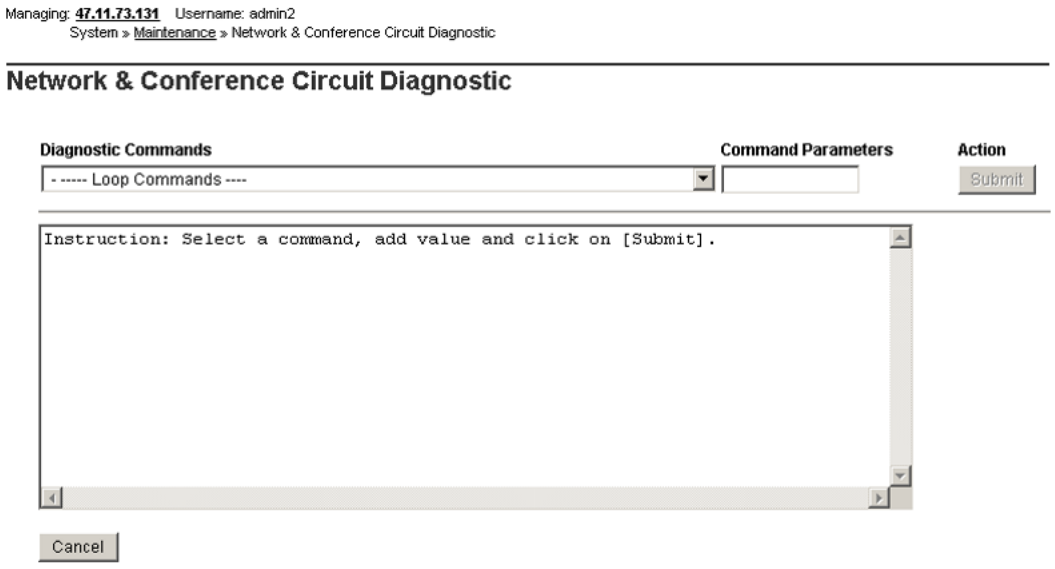


Figure 20: Network and Conference Circuit Diagnostic Web page

1. Use the **Diagnostic Commands** list to perform the following commands:
    a. ENLL - Enable Conference Loops

b. DISL - Disable Conference Loops

c. STAT - Status of Conference Loops

2. Add a value in the **Command Parameter**s field.
3. Click **Submit**.

D-channel Diagnostics

Click the **D-channel Diagnostics** link in the list of **Maintenance** diagnostic tools to open the **D-Channel Diagnostics** Web page as shown in Figure 21: D-channel Diagnostics Web page on page 68.

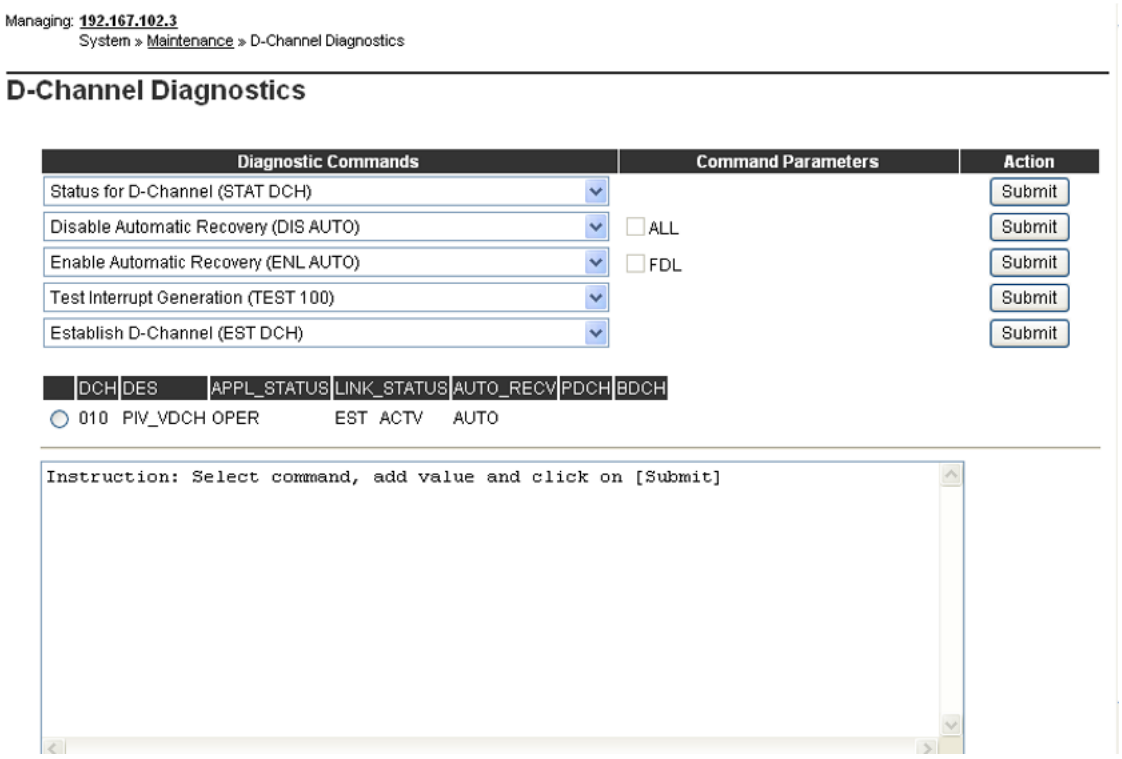


Figure 21: D-channel Diagnostics Web page

This Web page is used to test and maintain D-channel links and D-channel Interface (DCHI) cards. The commands available from this Web page correspond to the D-channel data traditionally maintained using the following overlays:

- LD 37 - Input/Output Diagnostic
- LD 48 - Link Diagnostic
- LD 96 - D-channel Diagnostic

To execute status commands using this Web page, follow the steps in Performing D-channel status commands on page 69.

Performing D-channel status commands

1. Select one of the following commands from the first **Commands** list:
    a. Status for D-Channel (STAT DCH)
    b. Status for Service Message (STAT SERV)
2. Click **Submit**.

To execute disable commands using this Web page, follow the steps in Performing D-channel disable commands on page 69.

Performing D-channel disable commands

1. Select one of the following commands from the second **Commands** list:
    a. Disable Automatic Recovery (DIS AUTO)
    b. Disable D-Channel (DIS DCH). Select the ALL check box to disable all D-Channels.
    c. Disable Local Loop Back (DIS LLB)
    d. Disable Remote Loop Back (DIS RLB)
    e. Disable Test Mode (DIS TEST)
2. Click **Submit**.

To execute enable commands using this Web page, follow the steps in Performing D-channel enable commands on page 69.

Performing D-channel enable commands

1. Select one of the following commands from the third **Commands** list:
    a. Enable Automatic Recovery (ENL AUTO)
    b. Enable D-Channel (ENL DCH). To force a loadware download at the same time, select the FDL check box.
    c. Enable Local Loop Back (ENL LLB)
    d. Enable Remote Loop Back (ENL RLB)
    e. Enable Test Mode (ENL TEST)
2. Click **Submit**.

To execute test commands using this Web page, follow the steps in Performing D-channel test commands on page 69.

Performing D-channel test commands

1. Select one of the following commands from the fourth **Commands** list:
    a. Test interrupt Generation (TEST 100)

b. Test Loop Back (Test 101)
c. Test Interrupt Handler (TEST 200)
d. Test Interrupt Handler-to-link (TEST 201)

2. Click **Submit**.

To execute D-Channel commands using this Web page, follow the steps in Performing D-channel commands on page 70.

Performing D-channel commands

1. Select one of the following commands from the fifth **Commands** list:
   a. EEstablish D-Channel (EST DCH)
   b. Get Physical Address and switch settings (MAP DCH)
   c. Reset DCH and Inhibit Signaling (RST DCH)
   d. Release D-Channel (RLS DCH)
   e. Switch to Standby D-Channel (SDCH DCH)
2. Click **Submit**.

D-Channel Expansion Diagnostics

Click the **D-Channel Expansion Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Link: D-Channel Expansion Diagnostics Web page as shown in Figure 22: Link: D-Channel Expansion Diagnostics Web page on page 71.

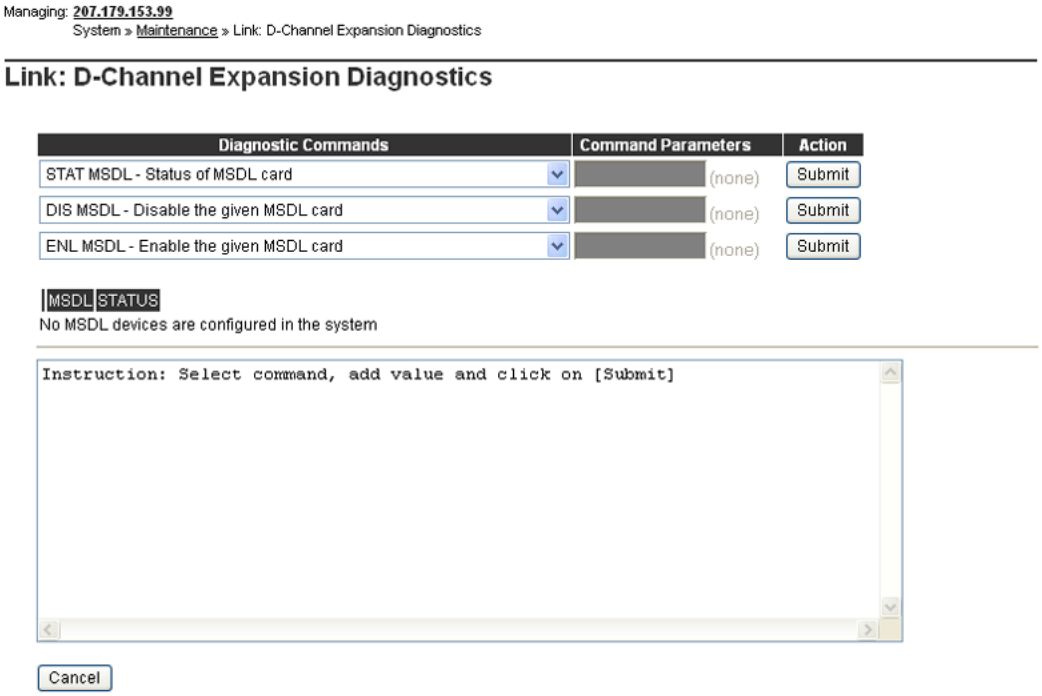


Figure 22: Link: D-Channel Expansion Diagnostics Web page

This Web page is used to test and maintain Multipurpose Serial Data Link (MSDL) cards. The commands available from this Web page correspond to the MSDL data traditionally configured by using LD 48 - Link Diagnostic.

To perform MSDL diagnostic activities using this Web page, follow the steps in Performing D-channel Expansion MSDL diagnostic commands on page 71.

Performing D-channel Expansion MSDL diagnostic commands

1. Select one of the following commands from the first **Commands** list:
    a. STAT MSDL - Status of MSDL card
    b. STAT MSDL full - Status MSDL card and available RAM
    c. SLFT MSDL - Self test on the given MSDL card
    d. RST MSDL - Power-On rest the given MSDL card
2. Click **Submit**.

To execute disable commands using this Web page, follow the steps in Performing D-channel Expansion disable commands on page 71.

Performing D-channel Expansion disable commands

1. Select one of the following commands from the second **Commands** list:
    a. DIS MSDL all - Disable the given MSDL card

b. DIS MSDL ALL - Disable all ports and then the MSDL card
c. DIS MSDL AUDM - Disable MSDL auditing for the MSDL card
d. DIS MSDL DBG - Disable debugger option for the MSDL card

2. Click **Submit**.

To execute enable commands using this Web page, follow the steps in Performing D-channel Expansion enable commands on page 72.

Performing D-channel Expansion enable commands

1. Select one of the following commands from the third **Commands** list:
   a. ENL MSDL - Enable the given MSDL card
   b. ENL MSDL all - Enable all ports and then the MSDL card
   c. ENL MSDL AUDM - Enable MSDL auditing for the MSDL card
   d. ENL MSDL FDL - Force download loadware to the MSDL card
2. Click **Submit**.

Digital Trunk Diagnostics

Click the **Digital Trunk Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Digital Trunk Interface and Primary Rate Interface: Digital Trunk Diagnostics Web page as shown in Figure 23: Digital Trunk Interface and Primary Rate Interface: Digital Trunk Diagnostics Web page on page 73.

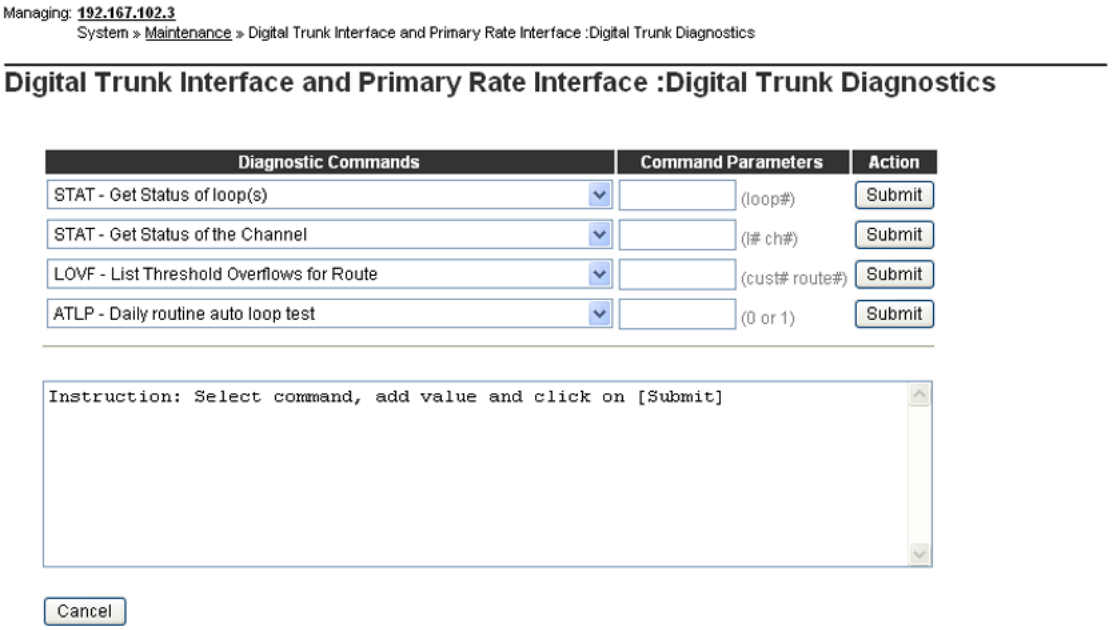


Figure 23: Digital Trunk Interface and Primary Rate Interface: Digital Trunk Diagnostics Web page

This Web page is used to test and maintain Digital Trunk Cards. The commands available from this Web page correspond to the DTI/PRI data traditionally maintained by using LD 60 - Digital Trunk Interface and Primary Rate Interface Diagnostics.

Use this Web page to issue maintenance commands on cards, channels, or routes by using the appropriate command list and parameter text box.

To perform maintenance activities on a Digital Trunk Card using this Web page, follow the steps in Performing maintenance activities on a Digital Trunk Card on page 73.

Performing maintenance activities on a Digital Trunk Card

1. Select one of the following commands from the first **Commands** drop-down list:
    a. STAT - Get Status of loop(s)
    b. DISL - Disable network and DTI/PRI cards of loop
    c. DISI - Disable loop (when all channels are idle
    d. ENCH - Enable all channels on 2.0 Mb/s DTRI/PRI
    e. ENLL - Enable network and DTI/PRI cards of loop
    f. LCNT - List contents of alarm counters on loop(s)
    g. RCNT - Reset alarm counters of all DTI/PRI loops
    h. SLFT - Self Test on the loop)

i. DSYL - Disable yellow alarm processing for loop
j. ENYL - Enable yellow alarm processing for loop
k. DLBK - Disable remote loop back test
l. RLBK - Close loop at carrier interface point for testing
m. RMST - Perform remote loop back test on loop

2. Enter the Loop number in the **Command Parameters** text box.
3. Click **Submit**.

To perform maintenance activities on a Channel belonging to a Digital Trunk Card using this Web page, follow the steps in Performing maintenance activities on a Channel on page 74.

Performing maintenance activities on a Channel

1. Select one of the following commands from the second Commands drop-down list:
   a. STAT - Get Status of the channel
   b. DSCH - Disable the channel
   c. ENCH - Enable the channel
   d. SLFT - Self Test on the channel
   e. DLBK - Disable remote loop back test on channel
   f. RLBK - Close channel at carrier interface point
   g. RMST - Perform far end loop test on Channel
   h. RSET - Reset thresholds for channel on loop
2. Enter the Loop number and the Channel number, separated by a space, in the **Command Parameters** text box.
3. Click **Submit**.

To perform maintenance activities on a Digital Trunk Route using this Web page, follow the steps in Performing maintenance activities on a Digital Trunk Route on page 74.

Performing maintenance activities on a Digital Trunk Route

1. Select one of the following commands from the third **Commands** drop-down list:
   a. LOVF - List Thresholds Overflows for the Route
   b. CMIN - Clear minor alarm indication for customer
2. Enter the Customer number and the Route number, separated by a space, in the **Command Parameters** text box.
3. Click **Submit**.

To perform maintenance activities on a card using this Web page, follow the steps in Performing maintenance activities on a card on page 75.

Performing maintenance activities on a card

1. Select one of the following commands from the fourth **Commands** drop-down list:
    a. ATLP - Daily routine automatic card test
    b. CDSP - Clear maintenance display
2. Enter the 0 or 1 in the **Command Parameters** text box.
3. Click **Submit**.

Digital Trunk Maintenance Diagnostics

Click the **Digital Trunk Maintenance Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Digital Trunk Diagnostics Web page as shown in Figure 24: Digital Trunk Diagnostics Web page on page 75.

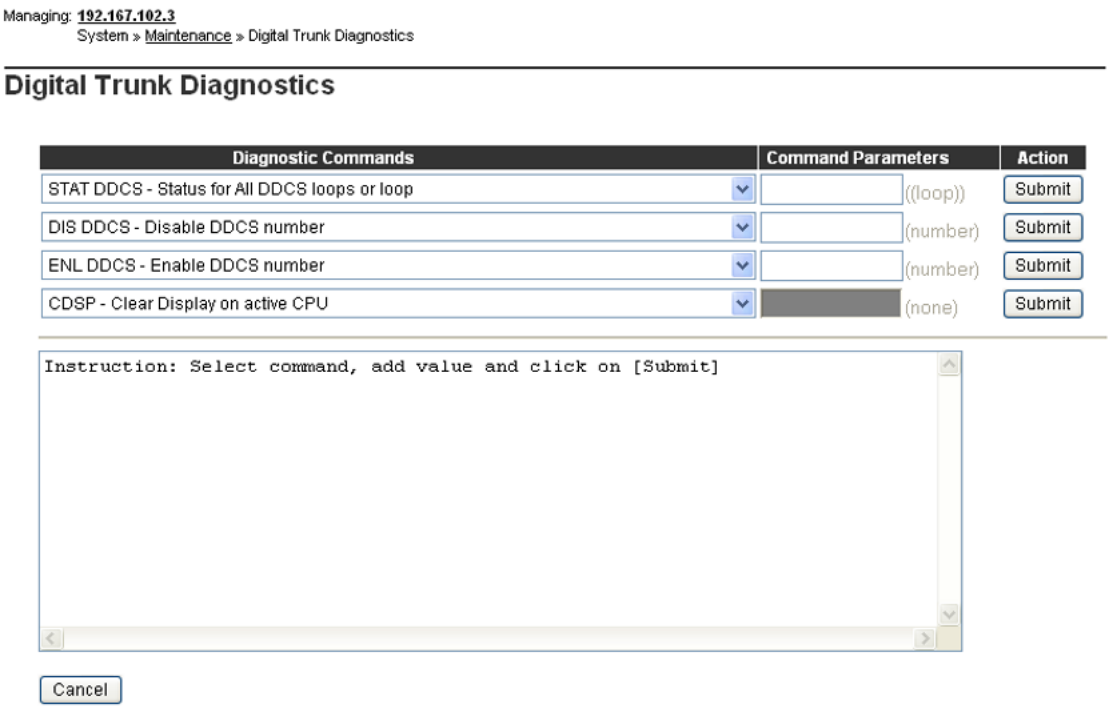


Figure 24: Digital Trunk Diagnostics Web page

The commands available from this Web page correspond to the digital trunk diagnostics traditionally performed by using LD 75 - Digital Trunk Diagnostics.

To get status information about a digital trunk using this Web page, follow the steps in Performing status commands on a digital trunk on page 76.

Performing status commands on a digital trunk

1. Select one of the following status commands from the first **Commands** drop-down list:
    a. STAT DDCS - Status for all DDCS loops or loop
    b. STAT DDSL - Status for all DDSLs or DDSL number
    c. STAT DTCS - Status for all DTCS loops or DTCS loop
    d. STAT DTRC - Status of RDC on loop
    e. STAT DTSL - Status of all DTSLs or DTSL number
    f. STAT DTVC - Status of VDC on loop
    g. STAT LSSL - Status of LSSL number for APNSS
    h. STAT LSRC - Status of RDC on Signaling Link number
    i. STAT LSVC - Status of VDC on Signaling Link number
2. Enter the Loop number in the **Command Parameters** text box.
3. Click **Submit**.

To disable an entity on a digital trunk using this Web page, follow the steps in Performing disable commands on a digital trunk on page 76.

Performing disable commands on a digital trunk

1. Select one of the following disable commands from the second **Commands** drop-down list:
    a. DIS DDSC - Disable DDSC number
    b. DIS DDSL - Disable DDSL number
    c. DIS DTCS - Disable DTCS loop
    d. DIS DTRC - Disable RDC on Loop
    e. DIS DTSL - Disable DTSL number
    f. DIS DTVC - Disable VDC on loop
    g. DIS LSSL - Disable LSSL number for APNSS
    h. DISI DDCS - Disable all Channels on Loop as idle
    i. DISI DTCS - Disable DTCS loop
2. Enter the appropriate number in the **Command Parameters** text box.
3. Click **Submit**.

To enable an entity on a digital trunk using this Web page, follow the steps in Performing enable commands on a digital trunk on page 77.

Performing enable commands on a digital trunk

1. Select one of the following enable commands from the third **Commands** drop-down list:
    a. ENL DDSC - Enable DDSC number
    b. ENL DDSL - Enable DDSL number
    c. ENL DTCS - Enable DTCS loop
    d. ENL DTRC - Enable RDC on Loop
    e. ENL DTSL - Enable DTSL number
    f. ENL DTVC - Enable VDC on loop
    g. ENL LSSL - Enable LSSL number for APNSS
2. Enter the appropriate number in the **Command Parameters** text box.
3. Click **Submit**.

To perform miscellaneous commands on a digital trunk using this Web page, follow the steps in Performing miscellaneous commands on a digital trunk on page 77.

Performing miscellaneous commands on a digital trunk

1. Select one of the following enable commands from the fourth **Commands** drop-down list:
    a. CDSP - Clear display on active CPU
    b. CMIN - Clear minor alarm for all customers
    c. STRT - Start DDSL number
2. Enter the necessary parameters.
3. Click **Submit**.

Emergency Services Diagnostics

Click the **Emergency Services Diagnostics** link in the list of Maintenance diagnostic tools to open the Emergency Services Diagnostics Web page as shown in Figure 25: Emergency Services Diagnostics Web page on page 78.

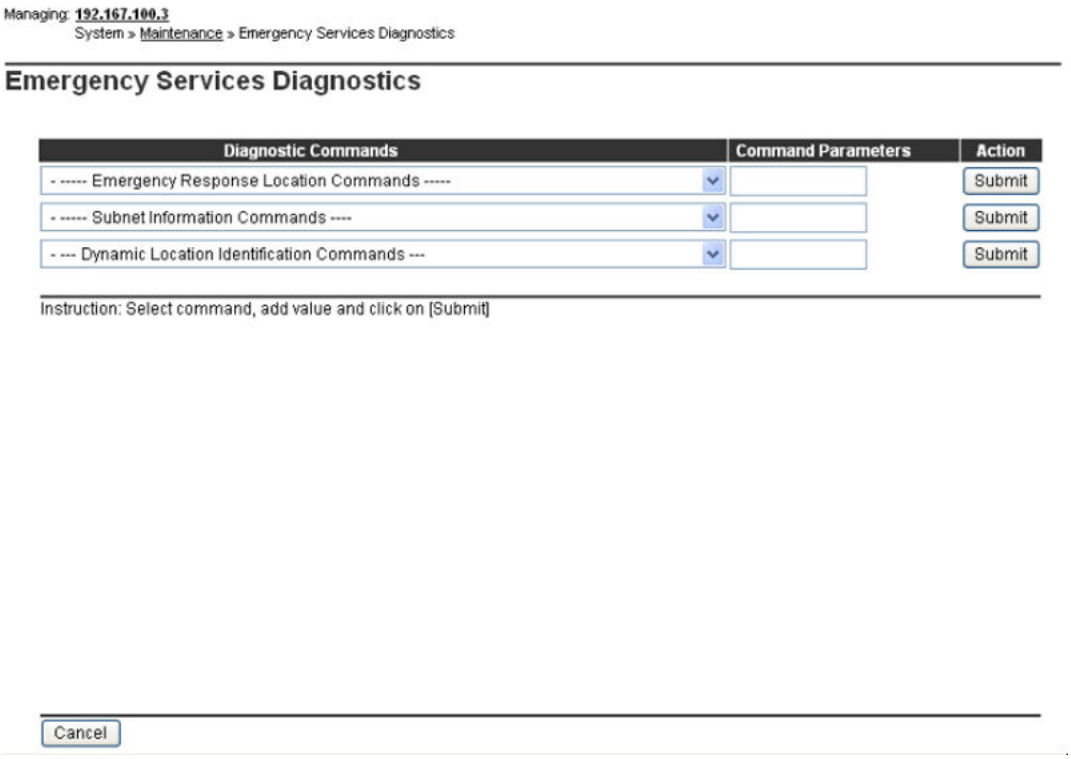


Figure 25: Emergency Services Diagnostics Web page

To perform Emergency Response Location commands using this Web page, follow the steps in Performing Emergency Response Location commands on page 78.

Performing Emergency Response Location commands

1. Select one of the following commands from the first **Commands** list:
    a. PRT ERL - Print Emergency Response Location
    b. ENL ERL - Enable ERL
    c. DIS ERL - Disable ERL
2. Enter the required parameters in the **Command Parameters** text box.
3. Click **Submit**.

To perform Subnet Information commands using this Web page, follow the steps in Performing Subnet Information commands on page 78.

Performing Subnet Information commands

1. Select one of the following commands from the second **Commands** list:
    a. PRT SUBNET - Print Subnet Location
    b. PRT SUBNET NTH - Print Subnet Locations Starting from Index #
    c. PRT SUBNET ERL - Print All Subnet Locations for ERL

d. PRT SUBNET ECL - Print All Subnet Locations for ECL

e. EST SUBNETLIS - Test Subnet Location

2. Enter the required parameters in the **Command Parameters** text box.
3. Click **Submit**.

To perform Dynamic Location Identification commands using this Web page, follow the steps in Performing Dynamic Location Identification commands on page 79.

Performing Dynamic Location Identification commands

1. Select one of the following commands from the third **Commands** list:

   a. PRT ELIN - Print Dynamic ELIN

   b. STAT ELIN - Get Status of Dynamic ELIN

   c. STAT ELIN ACTIVE - Get Status of active Dynamic ELIN
2. Enter the required parameters in the **Command Parameters** text box.
3. Click **Submit**.

Ethernet Diagnostics

Click the **Ethernet Diagnostics** link in the list of Maintenance diagnostic tools to open the Ethernet Diagnostics Web page as shown in Figure 26: Ethernet Diagnostics Web page on page 80.

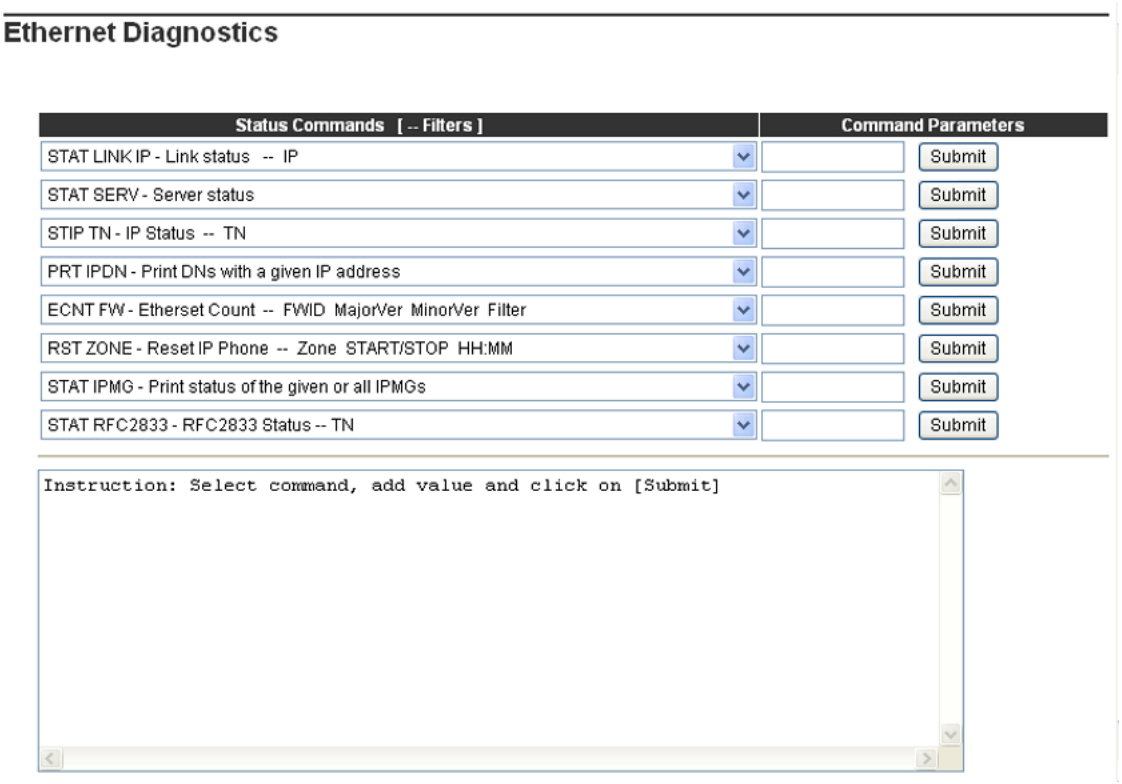


Figure 26: Ethernet Diagnostics Web page

This Web page is used to maintain Ethernet elements. The commands available from this Web page correspond to the data traditionally maintained by using LD 117- Ethernet Quality of Service Diagnostics.

To execute Link status commands, follow the steps in Performing Link status commands on page 80.

Performing Link status commands

1. Select one of the following commands from the first **Commands** drop-down list:
    a. STAT LINK IP - Link Status -- IP
    b. STAT LINK SRV - Link Status -- Server
    c. STAT LINK NAME - Link Status -- Host Name
    d. STAT LINK NODE - Link Status -- Node ID
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute server status commands, follow the steps in Performing server status commands on page 81.

Performing server status commands

1. Select one of the following commands from the second **Commands** drop-down list:
    a. STAT SERV - Server Status
    b. STAT SERV IP - Server Status --IP
    c. STAT SERV TYPE - Server Status -- Type
    d. STAT SERV APP - Server Status -- Application
    e. STAT SERV NAME - Server Status -- Name
    f. STAT SERV NODE - Server Status -- Node ID
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute IP status commands, follow the steps in Performing IP status commands on page 81.

Performing IP status commands

1. Select one of the following commands from the third **Commands** drop-down list:
    a. STIP TN - IP Status -- TN
    b. STIP TYPE - IP Status -- Type
    c. STIP ZONE - IP Status -- Zone
    d. STIP NODE - IP Status -- Node ID
    e. STIP HOSTIP - IP Status -- Host IP
    f. STIP ACF - IP Status -- Active Call Failover
    g. STIP TERMIP - IP Status -- Term IP
    h. STIP FW - IP Status -- FWID MajorVer MinorVer Filter
    i. STIP MODL - IP Status -- ModelName
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute print commands, follow the steps in Performing print commands on page 81.

Performing print commands

1. Select one of the following commands from the fourth Commands drop-down list:
    a. PRT IPDN - Print DNs with a given IP address
    b. PRT DNIP Print IP address(es) with a given DN
    c. PRT IPR - Print information for the given IPMG

d. PRT IPMG - Print information for the given IPMG

2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute Etherset Count commands, follow the steps in Performing Etherset Count commands on page 82.

Performing Etherset Count commands

1. Select one of the following commands from the fifth **Commands** drop-down list:
    a. ECNT FW - Etherset Count -- FWID MajorVer MinorVer Filter
    b. ECNT MODL - Etherset Count -- Model
    c. ECNT PEC - Etherset Count -- PEC
    d. ECNT ZONE - Etherset Count -- Zone Customer #
    e. ECNT CARD - Etherset Count -- Loop Shelf Card Customer#
    f. ECNT NODE - Etherset Count -- Node ID
    g. ECNT SS - Etherset Count -- HostName
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute Reset IP Phone commands, follow the steps in Performing Reset IP Phone commands on page 82.

Performing Reset IP Phone commands

1. Select one of the following commands from the sixth **Commands** drop-down list:
    a. RST ZONE - Reset IP Phone -- Zone START/STOP HH:MM
    b. RST FW - Reset IP Phone -- FWID START/STOP HH:MM
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute IPMG commands, follow the steps in Performing IPMG commands on page 82.

Performing IPMG commands

1. Select one of the following commands from the seventh **Commands** drop-down list:
    a. STAT IPMG - Print status of the given or all IPMGs
    b. STAT IPMG SUMMARY - Print status of all IPMGs
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute RFC2833 commands, follow the steps in Performing RFC2833 commands on page 83.

Performing RFC2833 commands

1. Select one of the following commands from the eighth **Commands** drop-down list:
    a. STAT RFC2833 - RFC2833 Status - TN
    b. ENL RFC2833PRT - Enable the info Message Printing
    c. DIS RFC2833PRT - Disable the info Message Printing
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

Ethernet Quality of Service Diagnostics

Click the **Ethernet Quality of Service Diagnostic** link in the list of **Maintenance**diagnostic tools to open the Ethernet Quality of Service Diagnostics Web page as shown in Figure 27: Ethernet Quality of Service Diagnostics Web page on page 83.

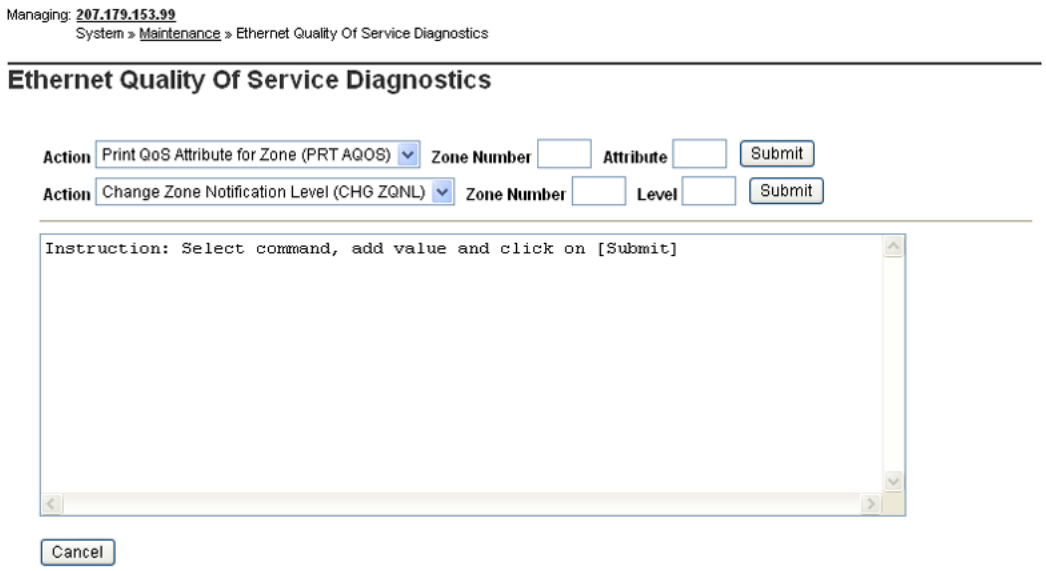


Figure 27: Ethernet Quality of Service Diagnostics Web page

This Web page is used to issue commands on elements by using the appropriate **Action** list and the corresponding Zone Number and Attribute or Level text boxes.

The commands that are available from this Web page correspond to data traditionally maintained by using LD 117 - Zone Configuration and Diagnostic.

To perform maintenance activities for Zone Attributes, follow the steps in Performing maintenance activities for Zone Attributes on page 84.

Performing maintenance activities for Zone Attributes

1. Select one of the following commands from the **Action** list:
    a. Print QoS attribute for Zone (PRT AQOS)
    b. Print Zone IP statistics (PRT ZQOS)
2. Enter the appropriate value in the corresponding **Zone Number** and **Attribute** text box.
3. Click **Submit**.

To perform maintenance activities for Zone Levels, follow the steps in Performing maintenance activities for Zone Levels on page 84.

Performing maintenance activities for Zone Levels

1. Select one of the following commands from the **Action** list:
    a. Change Zone Notification Level (CHG ZQNL)
    b. Print Zone Notification Level (PRT ZQNL)
2. Enter the appropriate value in the corresponding **Zone Number** and **Level** text box.
3. Click **Submit**.

Input/Output Diagnostics

Click the **Input/Output Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Input Output Diagnostics Web page as shown in Figure 28: Input/Output Diagnostics Web page on page 85.

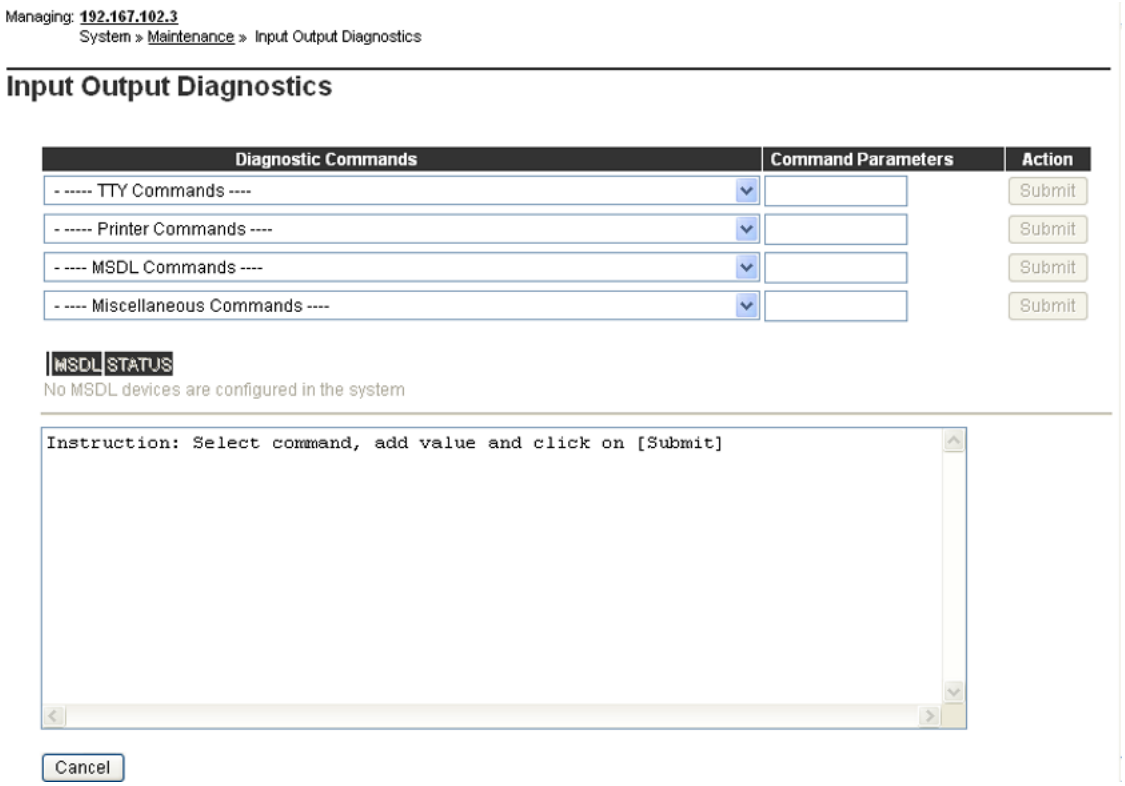


Figure 28: Input/Output Diagnostics Web page

The commands available from this Web page correspond to the Input/Output diagnostics traditionally performed using LD 37 - Input/Output.

To execute TTY commands, follow the steps in Performing Input/Output TTY commands on page 85.

Performing Input/Output TTY commands

1. Select one of the following commands from the first Commands list:
    a. STAT TTY - Get status of TTY device(s)
    b. ENL TTY - Enable TTY
    c. DIS TTY - Disable TTY
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute Printer commands, follow the steps in Performing Input/Output Printer commands on page 85.

Performing Input/Output Printer commands

1. Select one of the following commands from the second **Commands** list:
    a. STAT PRT - Get status of Printer(s)

b. ENL PRT - Enable Printer
c. DIS PRT - Disable Printer

2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To execute MDSL commands, follow the steps in Performing Input/Output MDSL commands on page 86.

Performing Input/Output MDSL commands

1. Select one of the following commands from the third **Commands** list:
   a. STAT MSDL - Get status of MSDL card(s)
   b. ENL MSDL - Enable MSDL device
   c. DIS MSDL - Disable MSDL device
   d. SLFT MSDL - Self test MSDL device
   e. RST MSDL - Reset MSDL device
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the miscellaneous commands, do the following:

1. Select one of the following commands from the fourth **Commands** list:
   a. STAT - Get status of all I/O devices in system
   b. STAT XSM - Get status of the system monitor
   c. STAT LINK - Get status of CDR data Link(s)
   d. CMIN - Clear minor alarm for all customers
   e. CDSP - Clear maintenance display on active CPU
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

Intergroup Switch and System Clock Generator Diagnostics

Click the **Intergroup Switch and System Clock Generator Diagnostics** link in the list of **Call Server** functionalities to open the Intergroup Switch and System Clock Generator Diagnostics Web page as shown in Figure 29: Intergroup Switch and System Clock Generator Diagnostics Web page on page 87.

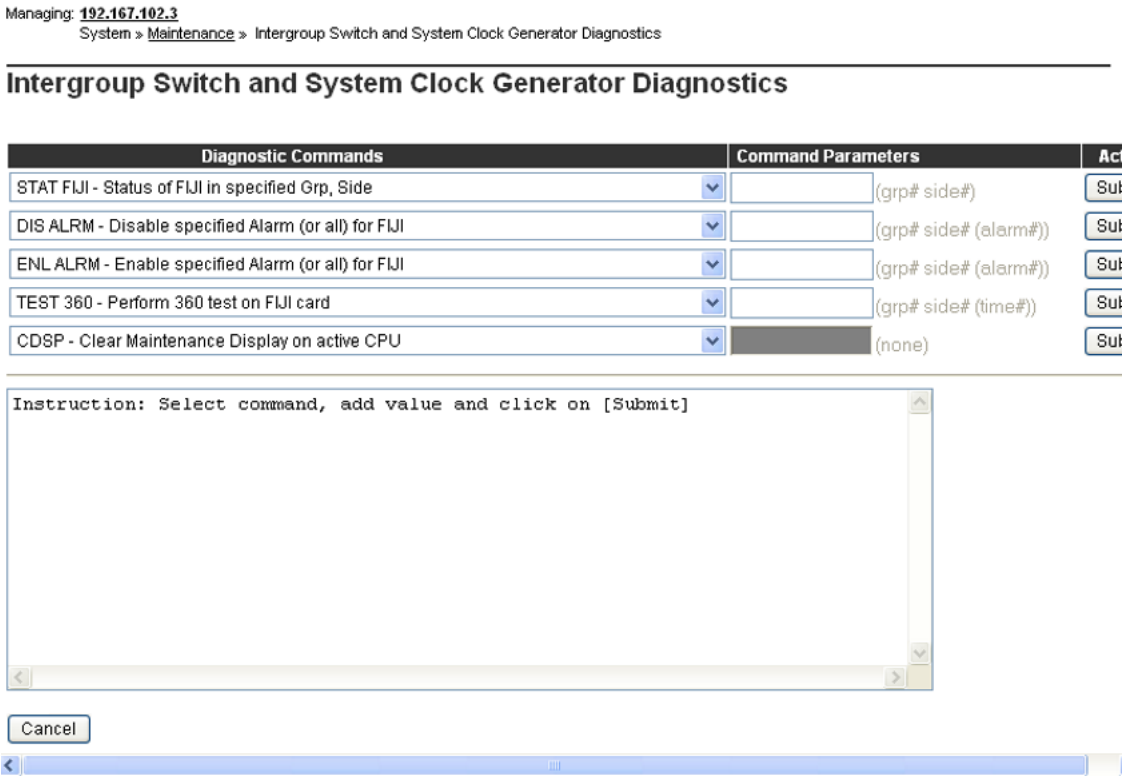


Figure 29: Intergroup Switch and System Clock Generator Diagnostics Web page

The commands available from this Web page correspond to the Intergroup Switch and System Clock Generator diagnostics traditionally performed using LD 39.

To use status commands, follow the steps in Performing Intergroup status commands on page 87.

Performing Intergroup status commands

1. Select one of the following commands from the first **Commands** list:
    a. STAT FIJI - Status of FIJI on specified Grp, Side
    b. STAT PER - Status of specified PS card
    c. STAT SCG - Status of specified SCG card (0 or 1)
    d. STAT RING - Status of all FIJI cards on specified Ring
2. Enter the group number and side number in the **Command Parameters** text box.
3. Click **Submit**.

To use the disable commands, follow the steps in Performing Intergroup disable commands on page 87.

Performing Intergroup disable commands

1. Select one of the following commands from the second **Commands** list:

a. DIS ALRM - Disable specified Alarm (or all) for FIJI
b. DIS FIJI - Disable FIJI in specified Group and Side
c. DSPS - Disable specified PS card
d. DIS SCG - Disable specified SCG card (0 or 1)
e. DIS RING - Disable all FIJI cards on specified Ring
f. DIS RALM - Disable all alarms for all RIJI cards in Ring

2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the enable commands, follow the steps in Performing Intergroup enable commands on page 88.

Performing Intergroup enable commands

1. Select one of the following commands from the third **Commands** list:
   a. ENL ALRM - Enable specified Alarm (or all) for FIJI
   b. ENL FIJI - Enable FIJI in specified Group and Side
   c. ENPS - Enable specified PS card
   d. ENL SCG - Enable specified SCG card (0 or 1)
   e. ENL RING - Enable all FIJI cards on specified Ring
   f. ENL RALM - Enable all alarms for all FIJI cards in Ring
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the test commands, follow the steps in Performing Intergroup test commands on page 88.

Performing Intergroup test commands

1. Select one of the following commands from the fourth **Commands** list:
   a. TEST 360 - Perform 360 test on FIJI card
   b. TEST FIJI - Self Test FIJI Card
   c. TEST BKPL - Test backplane
   d. TEST CMEM - Test connection memory
   e. TEST LINK - Perform Link test to identify hardware faults
   f. TEST ALL - Perform FIJI diagnostic test
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the miscellaneous commands, follow the steps in Performing Intergroup miscellaneous commands on page 89.

Performing Intergroup miscellaneous commands

1. Select one of the following commands from the fifth **Commands** list:
    a. CDSP - Clear Maintenance Display on active CPU
    b. CMIN - Clear minor alarm for all customers
    c. ARCV ON - Set auto-recovery operation for ring
    d. ARCV OFF - Reset auto-recovery operation for ring
    e. ALRD ON - Turn on alarm display for all FIJI cards
    f. ALRD OFF - Turn off alarm display for all FIJI cards
    g. RSET - Reset thresholds for switchover functionality
    h. RSTR - Restore Ring(s)
    i. SCLK - Switchover to the other SCG
    j. SLCK FRCE - Force clock to switch to other SCG
    k. SWRG - Switch Call Processing to specified ring
2. If SWRG is selected, enter appropriate **Command Parameters**.
3. Click **Submit**.

MSDL Diagnostics

Click the **MSDL Diagnostics** link in the list of Maintenance diagnostic tools to open the Multipurpose Serial Data Link (MSDL) Diagnostics Web page as shown in Figure 30: MSDL Diagnostics Web page on page 90.

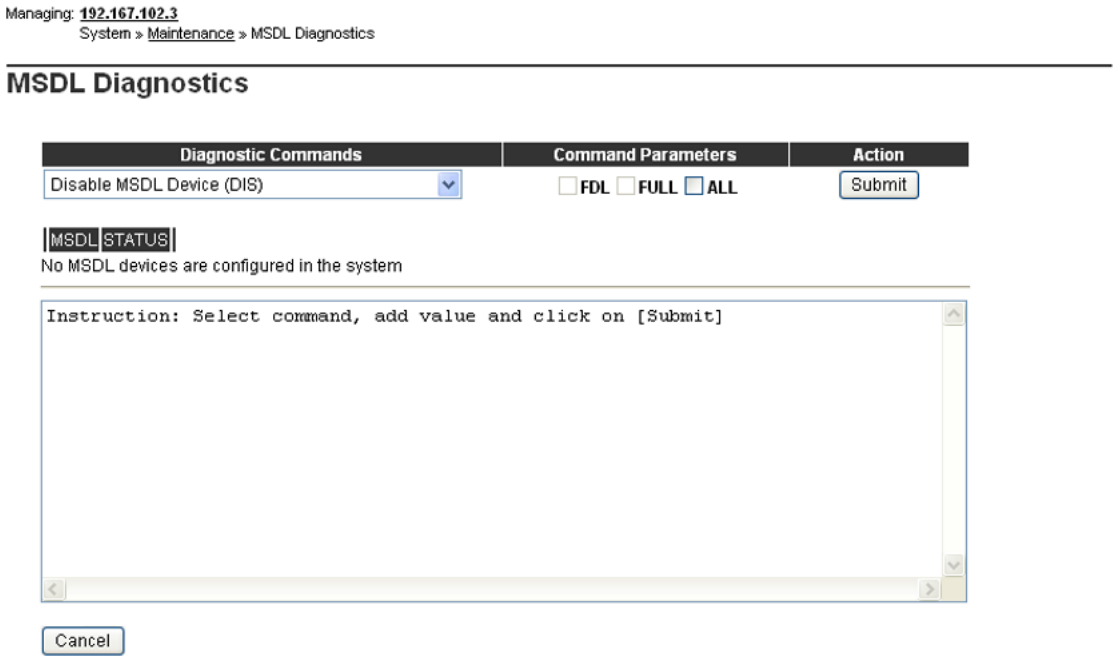


Figure 30: MSDL Diagnostics Web page

The commands available from this Web page correspond to the MSDL diagnostics traditionally performed by using LD 96 - D-channel.

This Web page is used to perform the following MSDL diagnostic functions:

- Disable MSDL Device (DIS)
- Enable MSDL Device (ENL)
- Self Test (SLFT)
- Get Status of MSDL Device (STAT)
- Causes Power-On Reset of MSDL Device (RST)

To perform diagnostic activities using this Web page, follow the steps in Performing MSDL diagnostic activities on page 90.

Performing MSDL diagnostic activities

1. Select the required **Diagnostic Command** from the **Commands** list.
2. To update the loadware, select the **FDL (Force Download)** check box when the Enable MSDL Device command is selected.
3. To check the status of all MDSL devices, select the **Full** check box when the Get Status of MSDL Device command is selected.

4. Enter the required command parameters in the **Command Parameters** text box.
5. Click **Submit**.

Multifrequency Sender Diagnostics

The Multifrequency Sender Diagnostics Web page is available only on Large Systems.

Click the **Multifrequency Sender Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Multifrequency Sender Diagnostics Web page as shown in Figure 31: Multifrequency Sender Diagnostics Web page on page 91.

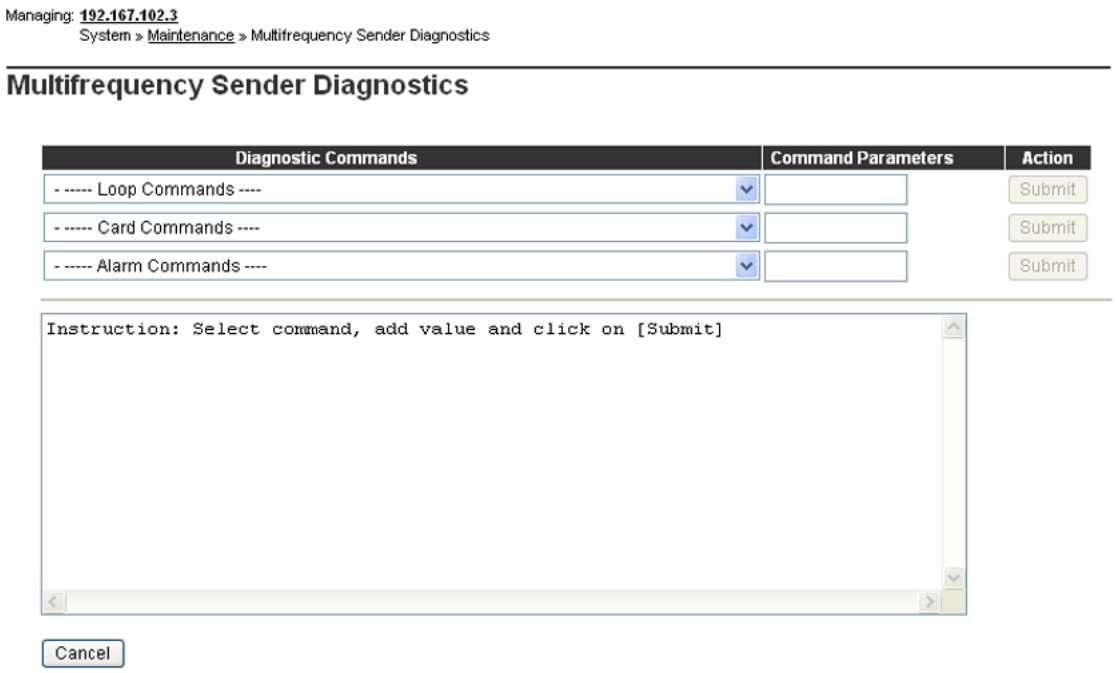


Figure 31: Multifrequency Sender Diagnostics Web page

The commands available from this Web page correspond to the Multifrequency Sender diagnostics traditionally performed by using LD 46.

To use the loop commands, follow the steps in Performing Multifrequency Sender loop commands on page 91.

Performing Multifrequency Sender loop commands

1. Select one of the following commands from the first **Commands** list:
    a. STAT - Get Status of MFS loop

b. ENLL - Enable loop
c. DISL - Disable loop
d. MFS - Test and enable MFS loop

2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the card commands, follow the steps in Performing Multifrequency Sender card commands on page 92.

Performing Multifrequency Sender card commands

1. Select one of the following commands from the second **Commands** list:
   a. ENLX - Enable Conf/TDS/MFS card on loop
   b. DISX - Disable Conf/TDS/MFS card on loop
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit** button.

To use the alarm commands, follow the steps in Performing Multifrequency Sender alarm commands on page 92.

Performing Multifrequency Sender alarm commands

1. Select one of the following commands from the third **Commands** list:
   a. CMAJ - Clear major alarm and reset power fail
   b. CDSP - Clear Maint display on active CPU
   c. CMIN - Clear minor alarm for all customers
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

Multifrequency Signaling Diagnostics

Click the **Multifrequency Signaling Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Multifrequency Signaling Diagnostics Web page as shown in Figure 32: Multifrequency Signaling Diagnostics Web page on page 93.

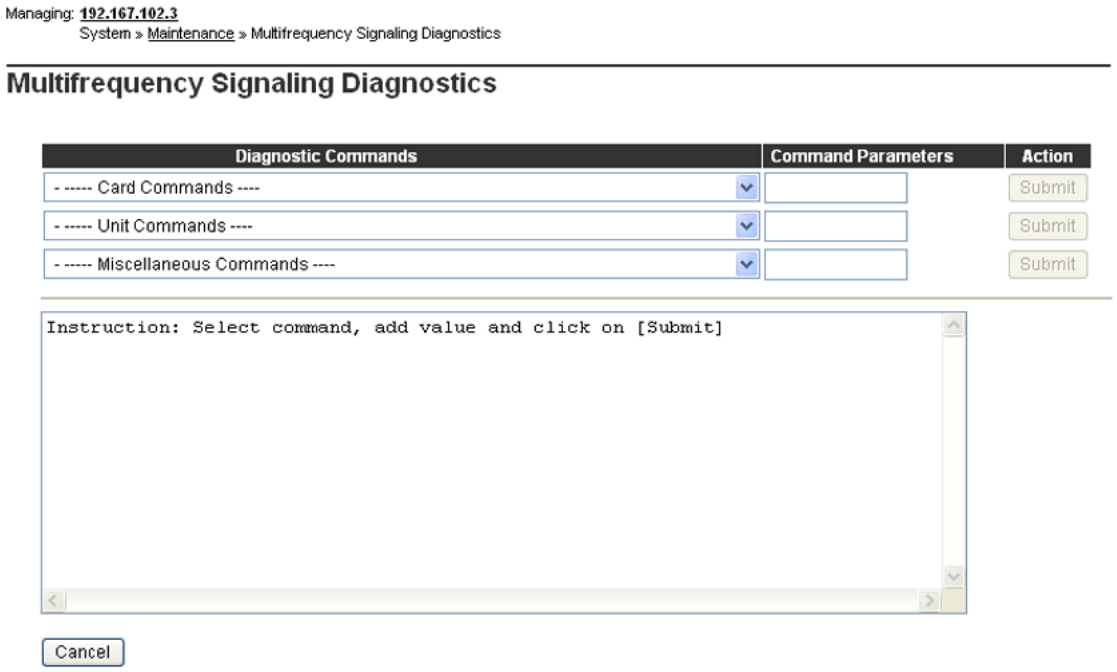


Figure 32: Multifrequency Signaling Diagnostics Web page

The commands available from this Web page correspond to the Multifrequency Signaling diagnostics traditionally performed by using LD 54 - Multifrequency Signaling.

To use the card commands, follow the steps in Performing Multifrequency Signaling card commands on page 93.

Performing Multifrequency Signaling card commands

1. Select one of the following commands from the first **Commands** list:
    a. STAT - Get status of MFC or MFE card
    b. DISC - Disable MFC/MFE card
    c. ENLC - Enable MFC or MFE card
    d. MIDN - Reset/Initialize all idle MFC or MFE cards
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the unit commands, follow the steps in Performing Multifrequency Signaling unit commands on page 93.

Performing Multifrequency Signaling unit commands

1. Select one of the following commands from the second **Commands** list:

a. STAT - Get status of specified MFC or MFE unit
b. DISU - Disable XMFC/XMFE channel
c. ENLU - Enable MFC/MFE channel
d. MTST - Invoke loop around test on unit with digit and level
e. ATST - Invoke automatic loop test for unit

2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the miscellaneous commands, follow the steps in Performing Multifrequency Signaling miscellaneous commands on page 94.

Performing Multifrequency Signaling miscellaneous commands

1. Select one of the following commands from the third **Commands** list:
   a. STAT - List all disabled MFC channels in system
   b. CMIN - Clear minor alarm for all customers
   c. CDSP - Clear the mtc display on active CPU
   d. CMAJ - Clear major alarm and reset power fail transfer
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

Network and Peripheral Equipment Diagnostics

Click the **Network and Peripheral Equipment Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Network & Peripheral Diagnostics Web page as shown in Figure 33: Network and Peripheral Diagnostics Web page on page 95.

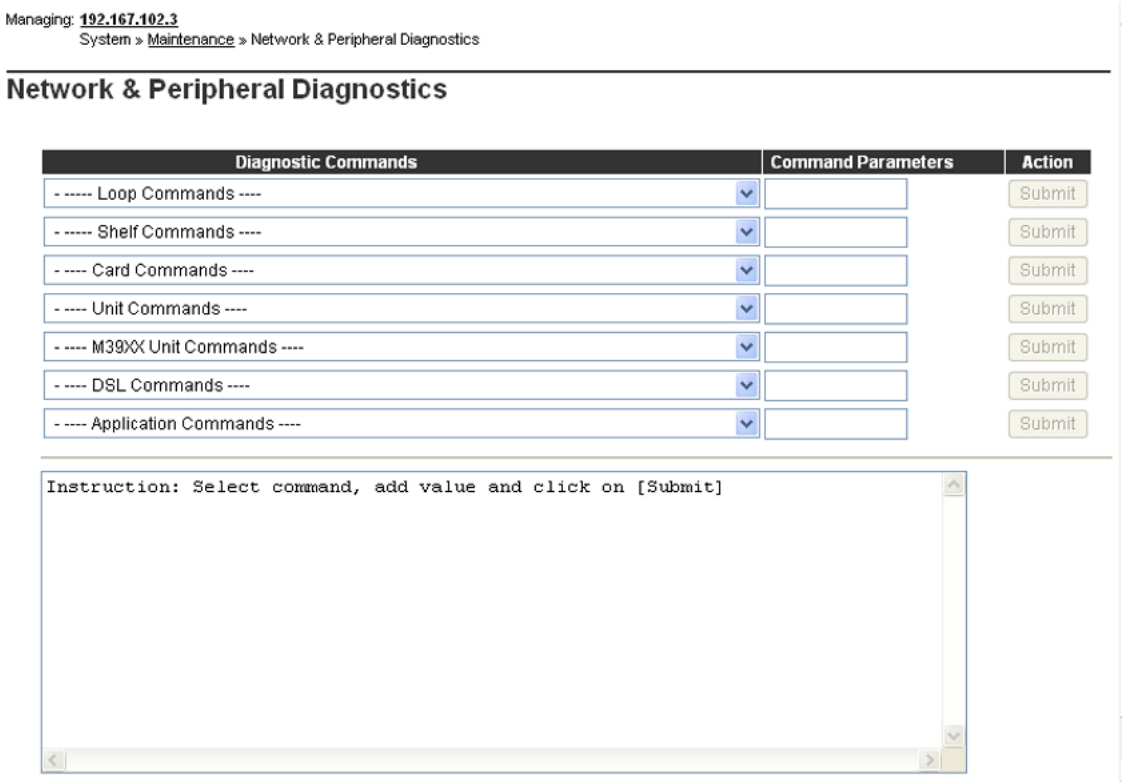


Figure 33: Network and Peripheral Diagnostics Web page

This Web page is used to test and maintain network and peripheral equipment. The commands available from this Web page correspond to the data traditionally maintained by using the LD 32 - Network and Peripheral Equipment Diagnostic.

These commands are split among separate drop-down lists, grouped by equipment type.

The command lists are as follows:

- **Loop Commands**
  - Network Loop
    - ENLL - Enable network loop
    - DISL - Disable network loop
  - Super Loop
    - STAT - Get status of Superloop
    - SUPL - Print data for one or all Superloops
    - IDC - Print Card ID for Superloop and associated Controller
    - XNTT - Do self-test of Network card for specified Superloop
    - ENLL - Enable specified Superloop

- XRST - Reset the specified Superloop

- **Shelf Commands**
  - DISS - Disable the shelf
  - ENLS - Enable specified shelf
  - LBSY - List TNs of all busy units
  - LDIS - List TNs of all disabled units
  - LIDL - List TNs of all idle units
  - LMNT - List TNs of all maint. busy units
- **Card Commands**
  - General Card Commands
    - STAT - Get card status
    - ENLC - Enable and reset card
    - DISC - Disable peripheral card
    - IDC - Print card ID for PE card
  - MISP Card Commands
    - STAT - Print status of MISP appl/card
    - ENLL - Enable MISL loop
    - ENLL BRIL - Enable BRIL application on MISP loop
    - ENLL BRIT - Enable BRIT application on MISP loop
    - IDC - Print MISP card ID
    - DISL - Disable MISP loop
    - DISL BRIL - Disable BRIL application on MISP loop (Large System)
    - DISL BRIT - Disable BRIT application on MISP loop
    - DISL BRIE - Disable BRIE application on MISP loop
  - BRI BRSC Card Commands
    - STAT - Get status of BRI card
    - IDC - Print BRSC card and LW version
    - DISC BRI - Disable the BRSC BRI application
    - DISC - Disable specified card
    - ENLC BRI - Enable the BRSC BRI application
    - ENLC - Enable specified card

- PS Card Commands
  - STAT PER - Get status of PS card
  - ENPS - Enable PS card and associated loops
  - DSPS - Disable Peripheral Signaling card
- Network Card Commands
  - STAT NWK - Check status of N/W card with specified loop
- XPEC Controller Commands
  - XPEC - Print data for all or specified Controller(s)
  - ENXP - Enable Controller and associated cards
  - ENXP XPC - Enable Controller, not the associated cards
  - DSXP - Disable Controller and all connected cards
  - XPCT - Self-test on Controller
  - IDCS - Print card ID for cards

• **Unit Commands**

- General Unit Commands
  - STAT - Get unit status
  - ENLU - Enable unit
  - IDU - Print set ID
  - DISU - Disable unit
  - STAT VTRM - Display virtual trunk unit status

• **M39XX Unit Commands**

- FDLC - Cancel/stop flash download for M39xx
- FDLU - Conditional download to one M39xx
- FWVU - Print firmware versions on M39xx
- FSUM - Print firmware versions on M39xx

• **DSL Commands**

- STAT - Get status of SILC or UILC
- ENL AUTO - Enable automatic link recovery
- ENRB - Enable Remote Loop Back for DSL
- DIS AUTO - Disable automatic link recovery
- DISU - Disable the DSL
- DSRB - Disable Remote Loop Back for DSL

- IDC - Print SILC/UILC card ID
- PERR - Print protocol log for the card
- DISC - Disable SILC/UILC card
- FDIS NCAL - Force disconnect the connection
- STAT NCAL - List all current connections - DSL
- PCON - Print configuration and LAPD parameters for specified DSL
- DISI - Disable the card when idle
- DSTS - Disable Disable Remote Loop Back test mode
- ENLC - Enable SILC/UILC card
- EISI - Enable the card when idle
- EISU - Enable specified DSL
- ESRB - Enable Remote Loop Back
- ESTS - Enable Remote Loop Back test mode
- ESTU - Establish D Channel Link
- PLOG - Print protocol log
- PMES - Print Layer 3 message log
- PTAB - Upload and Print Layer 3 message configuration
- PTRF - Print traffic data
- RLBT - Perform Remote Loop Back test
- RLSU - Release D Channel Link

• **Application Commands**

- DISL BRIL - Disable and remove BRIL application from MISP card
- DISL BRIT - Disable and remove BRIT application from MISP card
- DISL BRIE - Disable and remove BRIE application from MISP card
- ENLL BRIL - Enable BRI application on MISP Card and force download of the loadware
- ENLL BRIT - Enable BRIT application on MISP card and force download of the loadware
- ENLL BRIE - Enable BRIE application on MISP card and force download of the loadware
- DIS BRIL - Disable BRIL application on MISP Card
- DIS BRIT - Disable BRIT application on MISP Card
- DIS BRIE - Disable BRIE application on MISP Card

- PERR BRIL - Upload error log for BRIL application on MISP Card
- PERR BRIT - Upload error log for BRIT application on MISP Card
- PERR BRIE - Upload error log for BRIE application on MISP Card
- PERR BRIL - Print protocol log for BRIL application on MISP Card
- PERR BRIT - Print protocol log for BRIT application on MISP Card
- PERR BRIE - Print protocol log for BRIE application on MISP card
- STAT BRIL - Get status of MISP card and BRIL application
- STAT BRIT - Get status of MISP card and BRIT application
- STAT BRIE - Get status of MISP card and BRIE application

Use this Web page to issue diagnostic commands on the network and peripheral equipment by using the appropriate **Diagnostic Commands** list and the corresponding **Command Parameters** text box. The required parameters for the selected command are indicated to the right of the **Command Parameters** text box after the command is selected.

To perform maintenance activities using this Web page, follow the steps in Performing Network and Peripheral maintenance activities on page 99.

Performing Network and Peripheral maintenance activities

1. Select a command from one of the **Diagnostic Commands** drop-down lists.
2. Enter the appropriate value in the corresponding **Command Parameters** text box. The required parameters for the selected command are indicated to the right of the **Command Parameters** box once the command is selected.
3. Click the corresponding **Submit** button.

Network and Signaling Diagnostics

Click the **Network and Signaling Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Network & Signaling Diagnostics Web page as shown in Figure 34: Network and Signaling Diagnostics Web page on page 100.

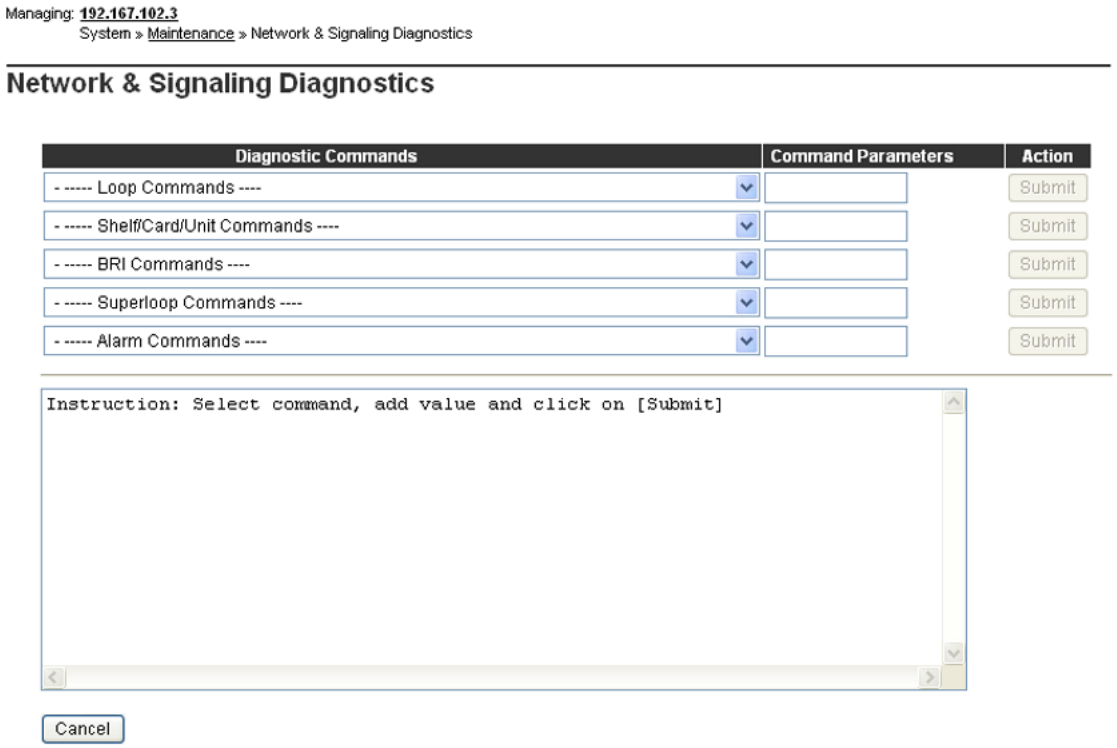


Figure 34: Network and Signaling Diagnostics Web page

The commands available from this Web page correspond to the Network and Signaling diagnostics traditionally performed by using LD 30 - Network and Signaling.

This Web page is used to perform the following Network and Signaling diagnostic functions:

- **Loop Commands**
  - ENLL - Enable network loop
  - DISL - Disable loop
  - LDIS - List disabled loops
  - LENL - List enabled loops
  - LOOP - Test network memory on loop(s)
  - STAT - Get status of all/specified N/W loops
- **Shelf/Card/Unit Commands**
  - UNTT - Signaling test on specified card or unit
  - SHLF - Test loop l, shelf s (Large System)
  - CPED - Clear contents of ctrlr maint display (Large System)
  - RPED - Read contents of ctrlr maint display (Large System)

- **BRI Commands**
  - SLFT - Selftest on ISDN BRI line card
  - SLFT - Selftest ISDN BRI line card (Large System)
  - SLFT - Selftest on MISP card
  - STEI - Query Term Edpt Identifiers and USIDs (Large System)
  - TEIT - Perform TEI check on DSL
- **Superloop Commands**
  - ENLL - Enable specified Superloop
  - DISL - Disable specified Superloop
  - ENLL - Enable sl, download periph s/w ver
- **Alarm Commands**
  - CMAJ - Clear major alarm and reset power fail
  - CDSP - Clear Maint display on active CPU
  - CMIN - Clear minor alarm for all customers

To perform diagnostic activities using this Web page, follow the steps in Performing Network and Signaling diagnostic activities on page 101.

Performing Network and Signaling diagnostic activities

1. Select the required **Diagnostic Command** from the list.
2. Enter any required **Command Parameters**. The required parameters for the selected command are indicated to the right of the **Command Parameters** text box once the command is selected.
3. Click **Submit**.

TMDI Diagnostics

For T1 Multipurpose Digital Interface (TMDI) diagnostics click the **TMDI Diagnostics** link in the list of Call Server diagnostic tools to open the TMDI Diagnostics Web page as shown in Figure 35: TMDI Diagnostics Web page on page 102.

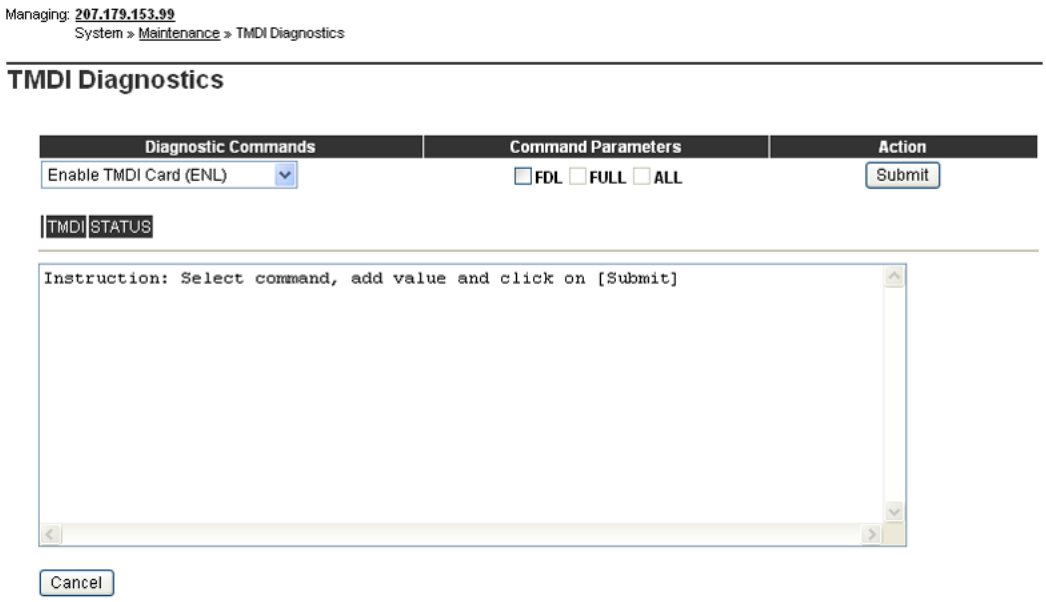


Figure 35: TMDI Diagnostics Web page

This Web page is used to test and maintain TMDI (DTI/PRI/DCH) cards. The commands available from this Web page correspond to the TMDI data traditionally configured by using LD 96 - D-channel.

To perform diagnostic activities using this Web page, follow the steps in Performing TMDI diagnostic activities on page 102.

Performing TMDI diagnostic activities

1. Select one of the following Actions from the **Commands** list:
    a. Enable TMDI Card (ENL)
    b. Disable TMDI card (DIS)
    c. Reset TMDI card (RST)
    d. Self Test on TMDI Card (SLFT)
    e. Get TMDI Status (STAT)
2. Select one of the following **Command Parameters**:
    a. FDL
    b. FULL
    c. ALL
3. Click **Submit**.

Tone and Digit Switch Diagnostics

Click the **Tone and Digit Switch Diagnostics** link in the list of Maintenance diagnostic tools to open the Tone and Digit Switch and Digitone Receiver Diagnostics Web page as shown in Figure 36: Tone and Digit Switch and Digitone Receiver Diagnostics Web page on page 103.

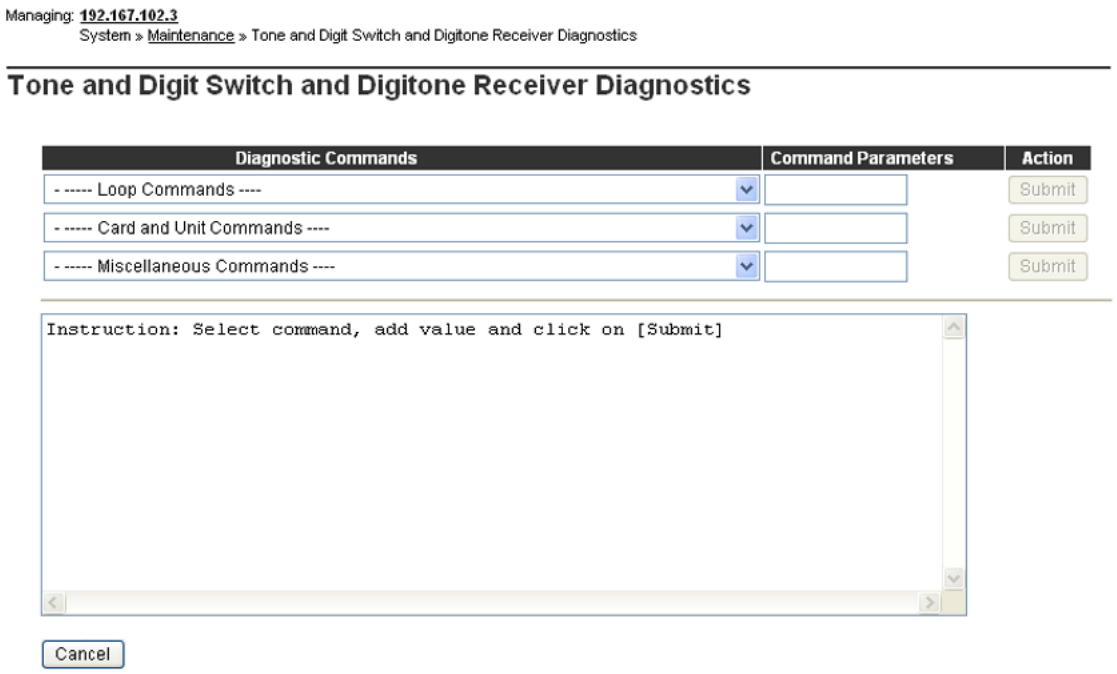


Figure 36: Tone and Digit Switch and Digitone Receiver Diagnostics Web page

This Web page is used to execute tone, digit switch, and digitone receiver diagnostics. The commands available from this Web page correspond to the TMDI data traditionally configured by using LD 34 - Tone and Digital Switch.

To perform diagnostic activities using this Web page, follow the steps in Performing Tone and Digit diagnostic activities on page 103.

Performing Tone and Digit diagnostic activities

1. Select one of the following commands from the **Diagnostic Commands** lists:

   • **Loop Commands**

   - STAT - Get status TDS loop

- DISL - Disable tone and digit loop
- DISX - Disable Conf/TDS/MFS card on loop l and l + 1
- ENLX - Enable Conf/TDS/MFS card on loop l and l + 1
- ENLL - Enable tone and digit loop
- MFR - Test ANI Feature Group D Multifrequency receiver units
- TDS - Test outpulsers and channels on loop

• **Card and Unit Commands**

- SDTR - Get status of DTR/MFR or XDT card/unit
- DISR - Disable specified TDS/MFS card/unit
- ENLR - Enable the DTR/MFR card/unit
- DTR - Test specified Digitone receiver card/unit
- MFR - Test ANI Multifrequency Card/Unit

• **Miscellaneous Commands**

- ENLM - Enable all the TDS loops of the given IPMG
- DISM - Disable all the TDS loops of the given IPMG
- CMIN - Clear the minor alarm for all customers
- CDSP - Clear the mtc display on active CPU
- CMAJ - Clear major alarm and reset power fail transfer
- MFR - Test all ANI Feature Group D MFR receiver units

2. Enter any required **Command Parameters**. The required parameters for the selected command are indicated to the right of the **Command Parameters** text box once the command is selected.
3. Click the corresponding **Submit** button.

Trunk Diagnostics

Click the **Trunk Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Trunk Diagnostics Web page as shown in Figure 37: Trunk Diagnostics Web page on page 105.

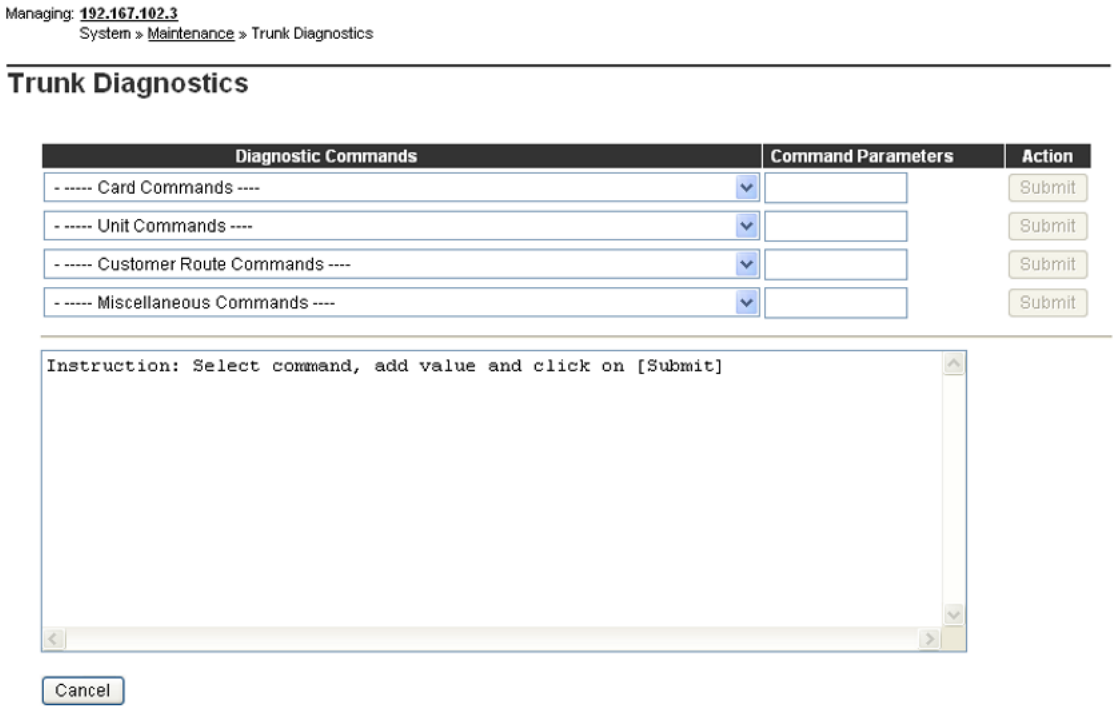


Figure 37: Trunk Diagnostics Web page

This Web page is used to test and maintain trunk cards. The commands available from this Web page correspond to the data traditionally maintained by using LD 36 - Trunk Diagnostic.

To use the card commands, follow the steps in Performing Trunk card commands on page 105.

Performing Trunk card commands

1. Select one of the following commands from the first **Commands** list:
    a. STAT - Get card status
    b. ENLC - Enable and reset card
    c. DISC - Disable card
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the unit commands, follow the steps in Performing Trunk unit commands on page 105.

Performing Trunk unit commands

1. Select one of the following commands from the second **Commands** list:

a. ENLU - Enable unit
b. LDIC - Number of days since last inc. call
c. DISU - Disable unit
d. RSET - Reset thresholds for the trunk
e. TPPM - Test the specified PPM trunk

2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the customer route commands, follow the steps in Performing Trunk customer route commands on page 106.

Performing Trunk customer route commands

1. Select one of the following commands from the third **Commands** list:
   a. LDIC - List days since last incoming call for customer
   b. LMAX - List trunk with max idle days for customer
   c. LNDS - List trunks with no disconnect sup. for customer
   d. LOVF - List threshold overflows for customer
   e. RAN - Test recorded announcement device
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

To use the miscellaneous commands, follow the steps in Performing Trunk miscellaneous commands on page 106.

Performing Trunk miscellaneous commands

1. Select one of the following commands from the fourth **Commands** list:
   a. CMIN - Clear minor alarm for all customers
   b. CDSP - Clear the mtc display on active CPU
2. Enter the required command parameters in the **Command Parameters** text box.
3. Click **Submit**.

Zone Diagnostics

Click the **Zone Diagnostics** link in the list of **Maintenance** diagnostic tools to open the Maintenance Commands for Zones Web page as shown in Figure 38: Maintenance Commands for Zones Web page on page 107.

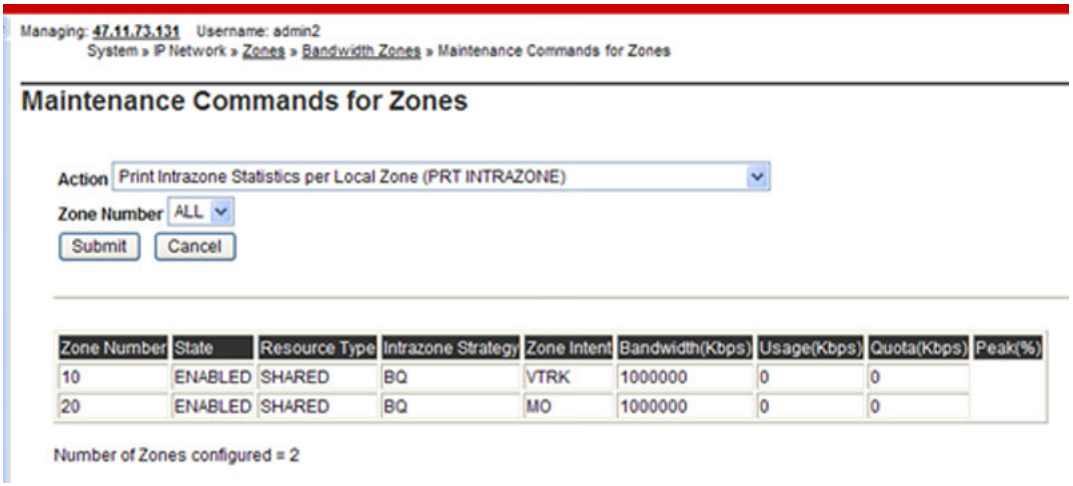


Figure 38: Maintenance Commands for Zones Web page

This Web page is used to enable and disable zones and to view various parameters, properties, and behaviors associated with the configured zones. The commands available from this Web page correspond to the data traditionally maintained by using LD 117 - Ethernet and Alarm Management.

This Web page also includes a table that shows the status and settings for the configured zones.

To perform maintenance activities using this Web page, follow the steps in Performing Zone maintenance activities on page 107.

Performing Zone maintenance activities

1. Select one of the following commands from the **Actions** list:
    a. Print Intrazone Statistics per Local Zone (PRT INTRAZONE)
    b. Print Bandwidth Property (PRT ZBW)
    c. Print Description (PRT ZDES)
    d. Print Dialing Plan and Access Codes (PRT ZDP)
    e. Print Time Change property (PRT ZTP)
    f. Show Branch Office Behaviour (STAT ZBR)
    g. Show Status (STAT ZONE)
    h. Enable a Zone (ENL ZONE)
    i. Disable a Zone (DIS ZONE)
    j. Enable a Zone's Branch Office Behaviour (ENL ZBR)
    k. Disable a Zone's Branch Office Behaviour (DIS ZBR)
    l. Print Adaptive Network Bandwidth Management and CAC Parameters (PRT ZCAC)

m. Print Interzone Statistics (PRT INTERZONE)
n. Reset CAC Statistics (CLR CACR)
o. Print Zone Alternate Prefix Information (PRT ZALT)
p. Show Alternate Routing Status (STAT ZALT)
q. Print Alarm Suppression Time Period (PRT ZAST)
r. Print Shared Bandwidth Management Information (PRT SBWM)
s. Enable Shared Bandwidth Management for the zone (ENL SBWM)
t. Disable Shared Bandwidth Management for the zone (DIS SBWM)
u. Show Shared Bandwidth Management Status (STAT SBWM)
v. Print Zone Location Name (PRT ZNAME)
w. Remove Zone Location Name (OUT ZNAME)

2. Select the **Zone Number** assigned to a configured zone from the list.
3. Click **Submit**.

Loops

To configure or edit Loops (Common Equipment) information, click the **Core Equipment > Loops** link of the**System** branch of the Element Manager navigator. The Common Equipment Web page appears (see Figure 39: Loops Web page on page 109).

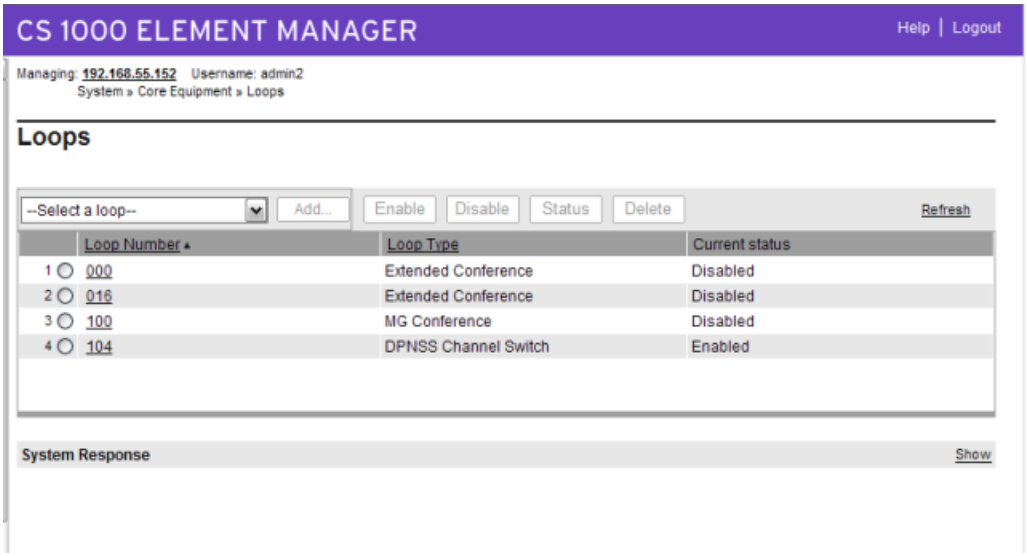


Figure 39: Loops Web page

The Loops Web page contains buttons that act as links to additional Web pages. From these pages, you can perform the following functions:

- Add
- Delete
- Enable
- Disable
- Status

The information entered in this section corresponds to CEQU (Common Equipment) data traditionally configured using LD 17 - Configuration Record 1.

To check the status of a loop, select a loop and click on **Status** button. The loop status is displayed below in the system response pane.

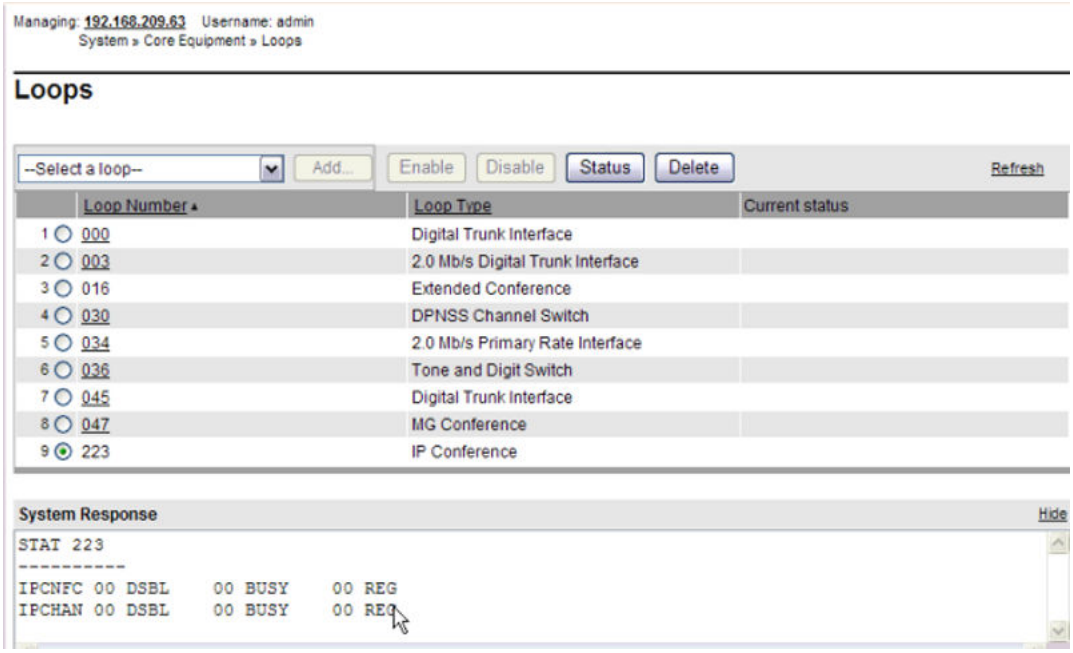


Figure 40: Loops Status

In the above Loops web page, from the **Select a loop** list choose IP Conference and then click **Add**. The IP Conference Loop Number Details Web page appears.

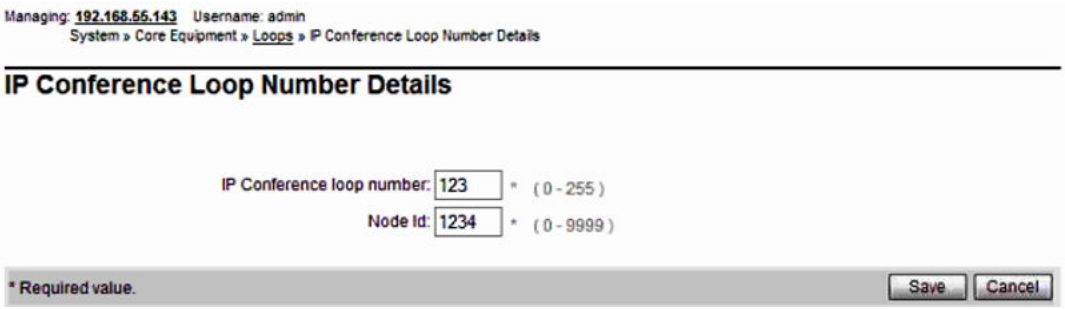


Figure 41: IP Conference Loop Number Details

Type the **IP Conference loop number** and **Node Id**, and then click **Save**.

In the Loops web page, from the **Select a loop** list choose IP Tone and Digit Switch and then click **Add**. The IP TDS Loop Number Details web page appears.

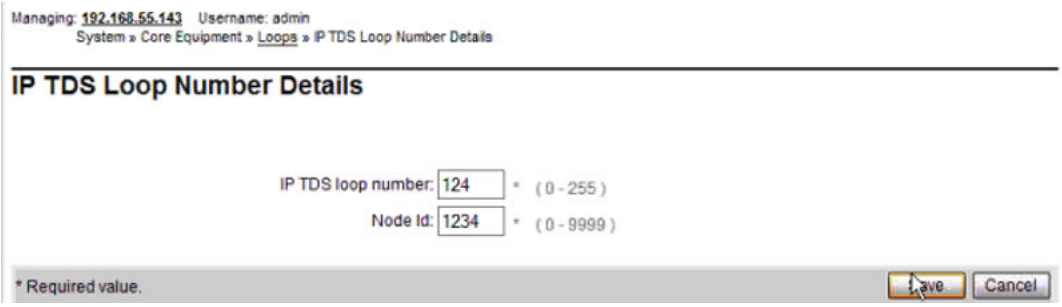


Figure 42: IP TDS Loop Number Details

Enter IP TDS loop number, Node Id and then click **Save**.

Superloops

To view, configure or edit Superloop information, click the **Core Equipment > Superloop** link of the **System** branch of the Element Manager navigator. The Superloops Web page appears, as shown in Figure 43: Superloops Web page on page 111.

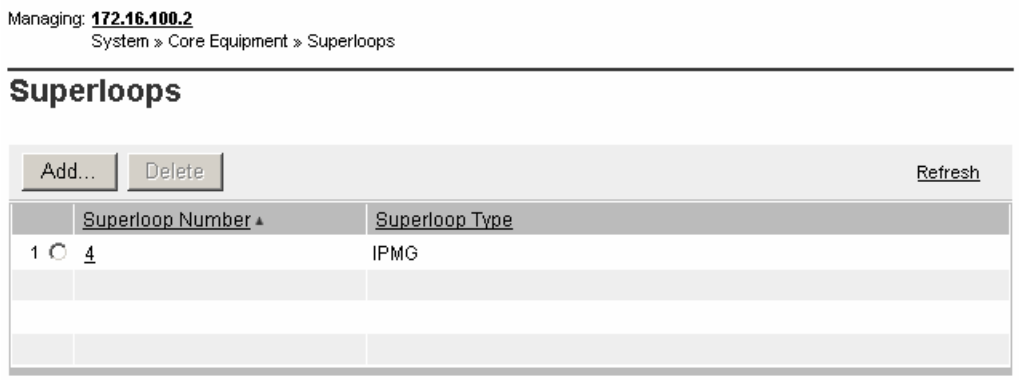


Figure 43: Superloops Web page

To view, configure, or edit a Superloop, click on the corresponding **Superloop Number**. The Superloops Details Web page appears as shown in Figure 44: Superloop Details Web page on page 112

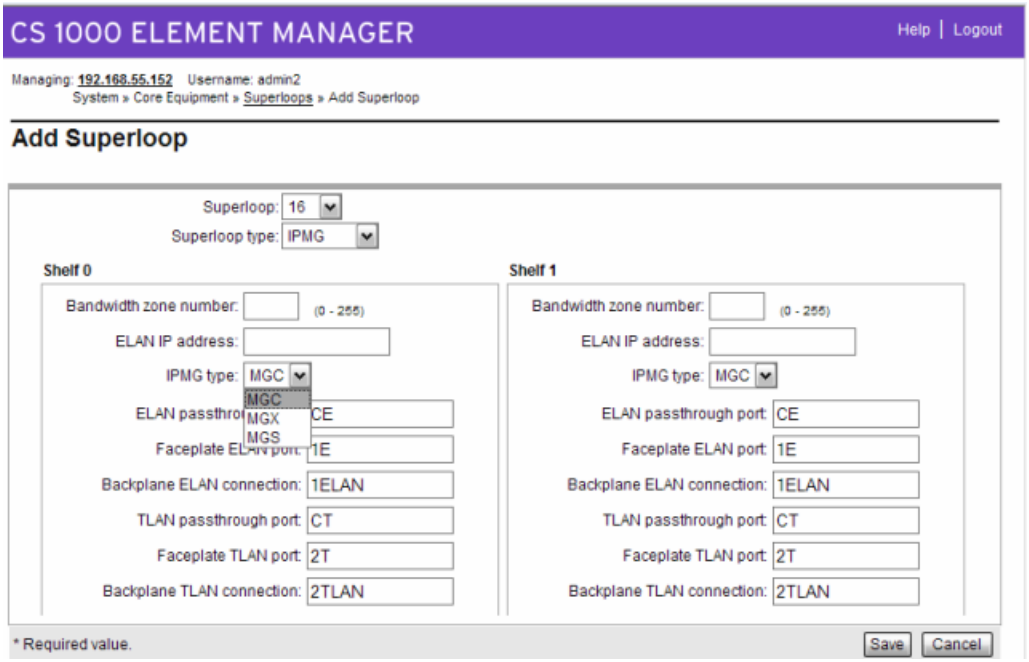


Figure 44: Superloop Details Web page

The information entered on this Web page corresponds to the Superloop (SUPL) command available in LD 97 - Configuration Record 2.

To save changes made on the Superloop Details Web page, click **Save**.

To add a Superloop, click the **Add** button on the Superloops Web page. The Add Superloop Web page appears, as shown in Figure 45: Add Superloop Web page on page 112.

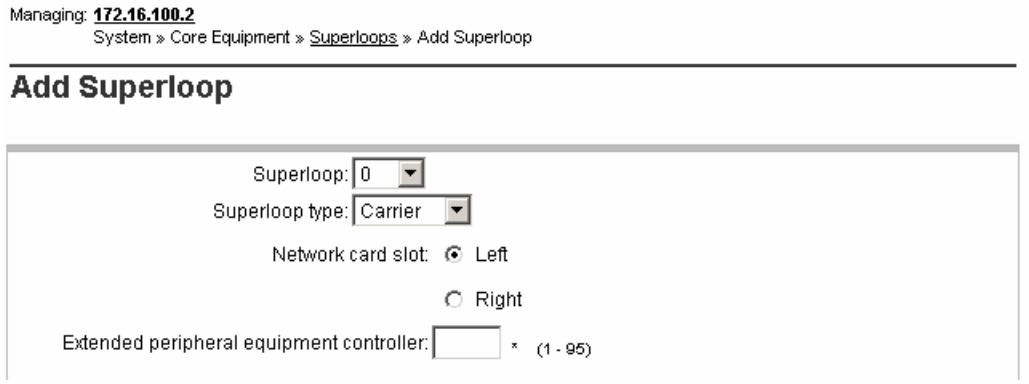


Figure 45: Add Superloop Web page

Select the **Superloop type** from the list. For IPMG superloop type, the Add Superloop Web page appears as shown in the following figure.

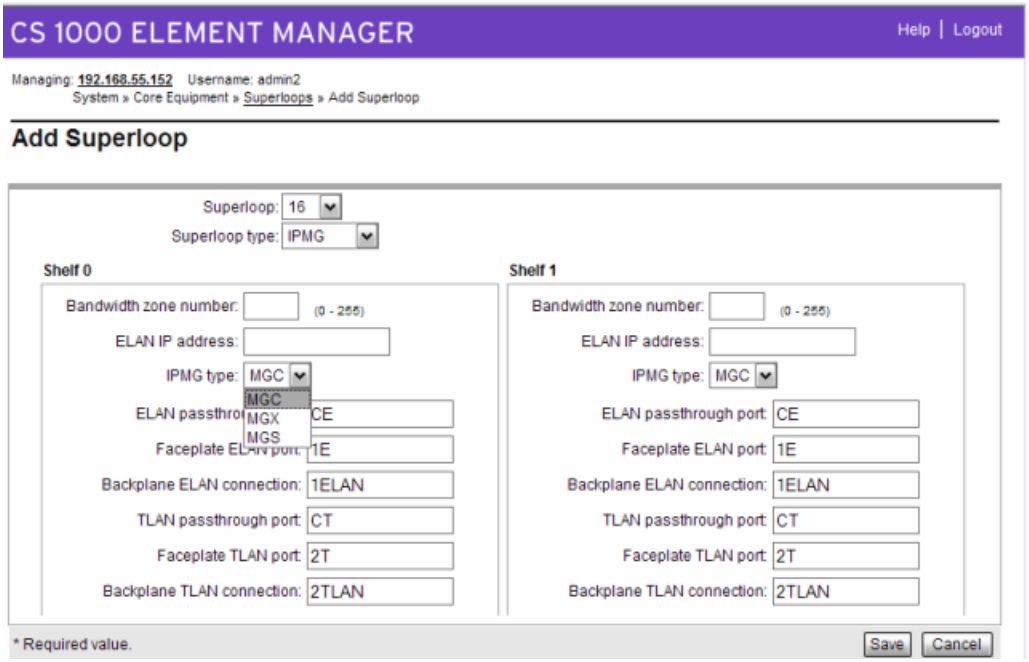
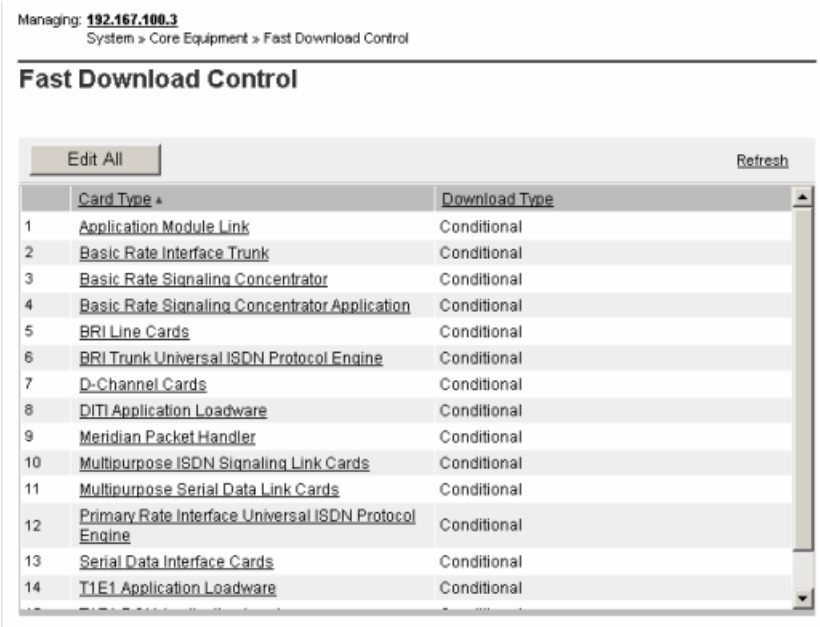


Figure 46: Add IPMG Superloop

Fill in the appropriate information and click **Save** to add the new Superloop.

MSDL/MSIP Cards

The Multipurpose Serial Data Link / Multi-Purpose ISDN Signaling Processor (MSDL/MSIP) Cards navigation link appears the Fast Download Control Web page, as shown in Figure 47: Fast Download Control Web page on page 114.



	Card Type	Download Type
1	Application Module Link	Conditional
2	Basic Rate Interface Trunk	Conditional
3	Basic Rate Signaling Concentrator	Conditional
4	Basic Rate Signaling Concentrator Application	Conditional
5	BRI Line Cards	Conditional
6	BRI Trunk Universal ISDN Protocol Engine	Conditional
7	D-Channel Cards	Conditional
8	DITI Application Loadware	Conditional
9	Meridian Packet Handler	Conditional
10	Multipurpose ISDN Signaling Link Cards	Conditional
11	Multipurpose Serial Data Link Cards	Conditional
12	Primary Rate Interface Universal ISDN Protocol Engine	Conditional
13	Serial Data Interface Cards	Conditional
14	T1E1 Application Loadware	Conditional

Figure 47: Fast Download Control Web page

The Fast Download Control Web page appears only for large systems. The page displays the table with the card type and the download type. The download type for any card can be changed.

To configure download type for a single card, follow the steps in Editing Fast Download Control (single card) on page 114.

Editing Fast Download Control (single card)

1. On the Fast Download Control Web page, click the card that you want to edit.

   The Edit Web page for the selected card appears.
2. Choose the **Download type** from the list.
3. Click **Save** or click **Cancel** to return to the Fast Download Control Web page.

To configure download type for all cards, follow the steps in Editing Fast Download Control all cards on page 114.

Editing Fast Download Control all cards

1. On the Fast Download Control Web page, click **Edit All** to edit all the cards in the list.

   The Edit All Web page appears.
2. Choose the **Download type** from the list.
3. Click **Save** or click **Cancel** to return to the Fast Download Control Web page.

Conference/TDS/Multifrequency Cards

Click the **Conference/TDS/Multifrequency Cards** link of the Element Manager Navigator to open the Conference/TDS/Multifrequency Cards Web page, as shown in Figure 48: Conference/TDS/Multifrequency Cards Web page on page 115.

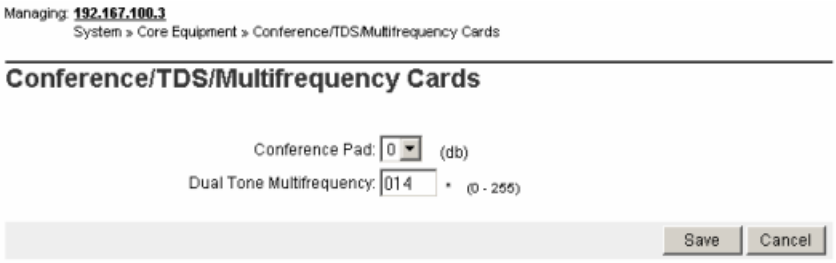


Figure 48: Conference/TDS/Multifrequency Cards Web page

Select a **Conference Pad** from the list, configure the **Dual Tone Multifrequency** value and click **Save** or click **Cancel** to return to the System Overview Web page.

Tone Senders and Detectors

Element Manager supports the configuration of Digitone receivers, Tone Detectors, and Multi Frequency Senders and Receivers. Click the **Core Equipment > Tone Senders And Detectors** link in the **System** branch of the Element Manager navigator. The Tone Senders And Detectors Web page appears, as shown in Figure 49: Tone Senders and Detectors Web page on page 115.

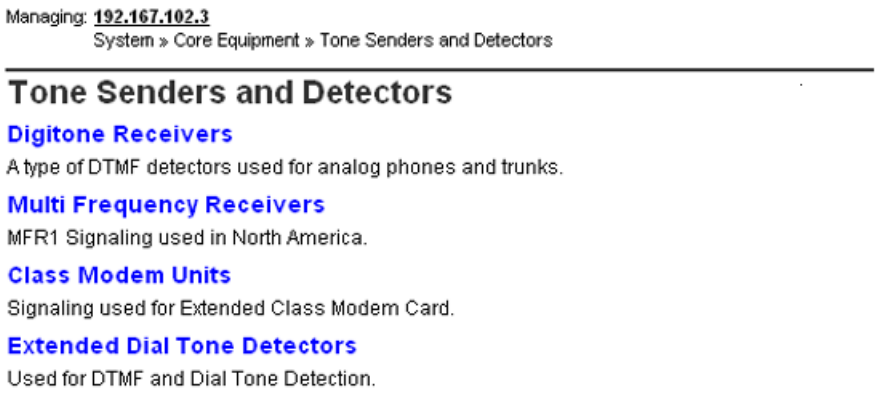


Figure 49: Tone Senders and Detectors Web page

Digitone Receivers

To display details of and to configure Digitone Receivers, from the Tone Senders And Detectors Web page, click the **Digitone Receivers** link. The Digitone Receivers Web page appears, as shown in Figure 50: Digitone Receivers Web page on page 116.

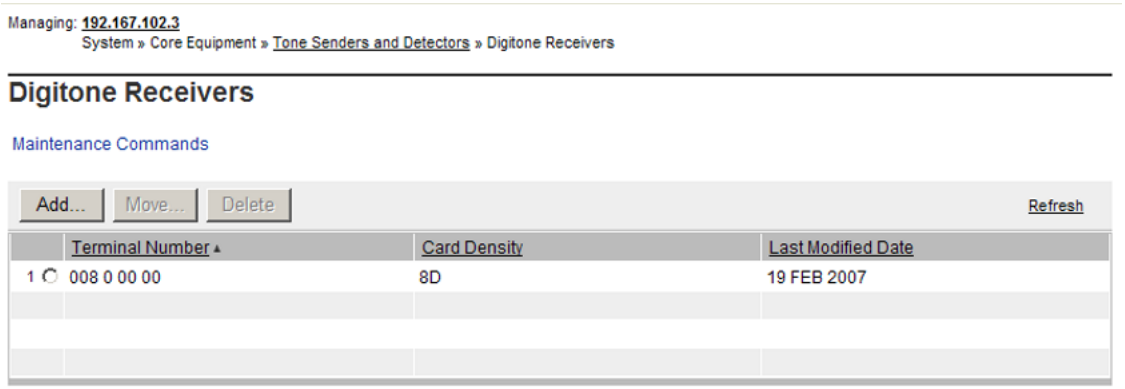


Figure 50: Digitone Receivers Web page

This Web page is used to display details of Digitone Receivers. Users can view, add, delete, and move Terminal Numbers.

To delete a Digitone Receiver, select the radio button beside the **Terminal Number** and click **Delete**.

Multi Frequency Receivers

To display details of and to configure Multi Frequency Receivers, from the Tone Senders And Detectors Web page, click the **Multi Frequency Receivers** link. The Multi Frequency Receivers Web page appears, as shown in Figure 51: Multi Frequency Receivers Web page on page 117.

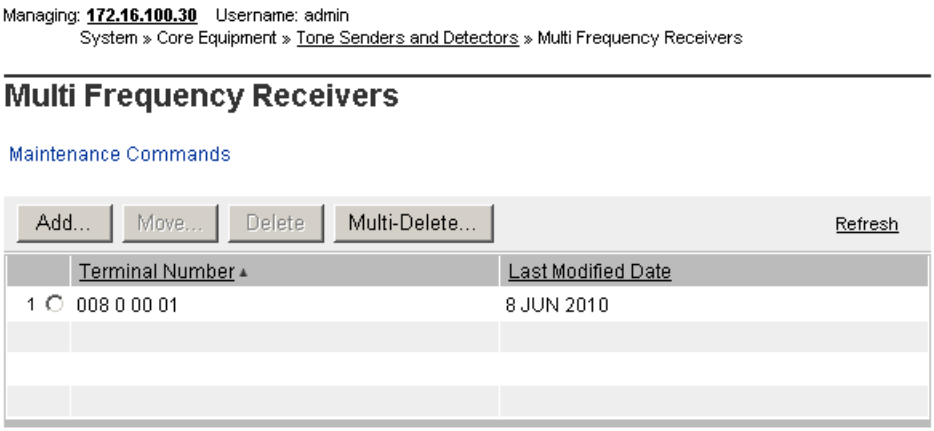


Figure 51: Multi Frequency Receivers Web page

Use this Web page to view details of Multi Frequency Receivers. You can view, add, delete, and move Terminal Numbers.

To delete a Multi Frequency Receiver, select the radio button beside the Terminal Number and click **Delete**.

Delete Multiple Multi Frequency Receivers

To delete Multi Frequency Receivers click **Multi-Delete**. The Delete Multiple Multi Frequency Receivers Web page appears as shown in the following figure.

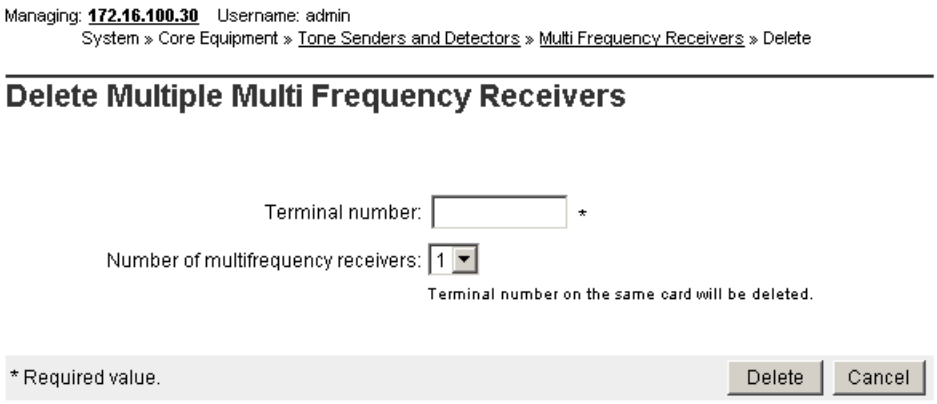


Figure 52: Delete Multiple Multi Frequency Receivers Web page

Deleting Multiple Multi Frequency Receivers

1. Type the **Terminal number** for the Multi Frequency Receivers.
2. From the **Number of multifrequency receivers** list, select the number to delete.
3. Click **Delete**.

Class Modem Units

To display details of and to configure Class Modem Units, on the Tone Senders And Detectors Web page, click the **Class Modem Units** link. The Class Modem Units Web page appears, as shown in Figure 53: Class Modem Units Web page on page 118.

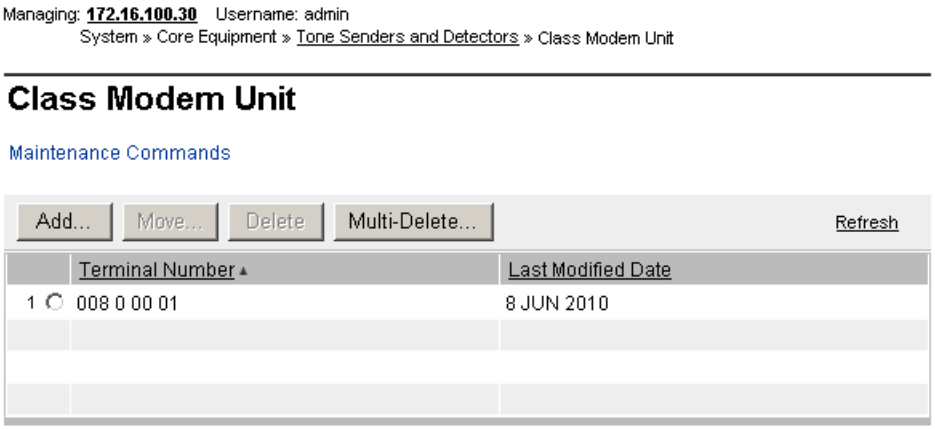


Figure 53: Class Modem Units Web page

Use this Web page to view details for Class Modem Units. You can view, add, delete, and move Terminal Numbers.

To delete a Class Modem Unit, select the radio button beside the **Terminal Number** and click **Delete**.

Delete Multiple Class Modem Units

To delete Multiple Class Modem Units click **Multi-Delete**. The Delete Multiple Class Modem Units Web page appears as shown in the following figure.

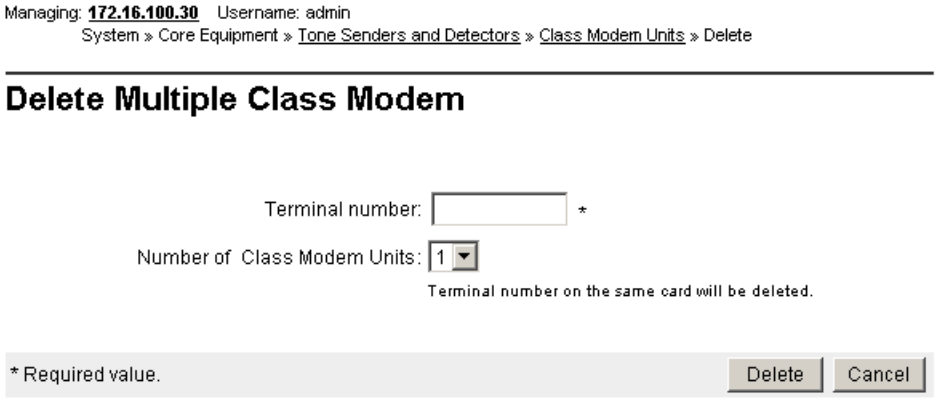


Figure 54: Delete Multiple Class Modem Units Web page

Deleting Multiple Class Modem Units

1. Type the **Terminal number** of the Class Modem.
2. From the **Number of Class Modem Units** list, select the number to delete.
3. Click **Delete**.

Extended Dial Tone Detectors

To display details of and to configure Extended Dial Tone Detectors, from the Tone Senders And Detectors Web page, click the **Extended Dial Tone Detectors** link. The Extended Dial Tone Detectors Web page appears, as shown in Figure 55: Extended Dial Tone Detectors Web page on page 120.

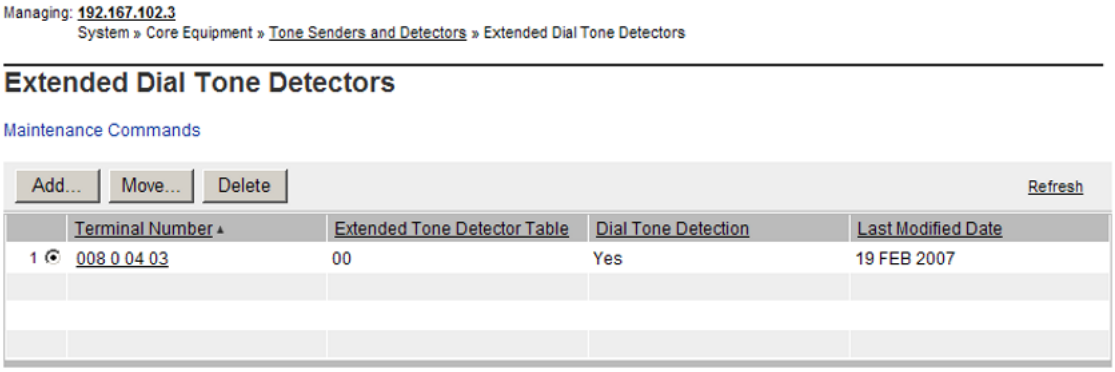


Figure 55: Extended Dial Tone Detectors Web page

Use this Web page to view details of Extended Dial Tone Detectors. You can view, add, delete, and move Terminal Numbers.

To delete an Extended Dial Tone Detector, select the radio button beside the **Terminal Number** and click **Delete**.

To add an Extended Dial Tone Detector, click **Add**. The Add Extended Dial Tone Detector Web page appears, as shown in Figure 56: Add Extended Dial Tone Detector Web page on page 120.

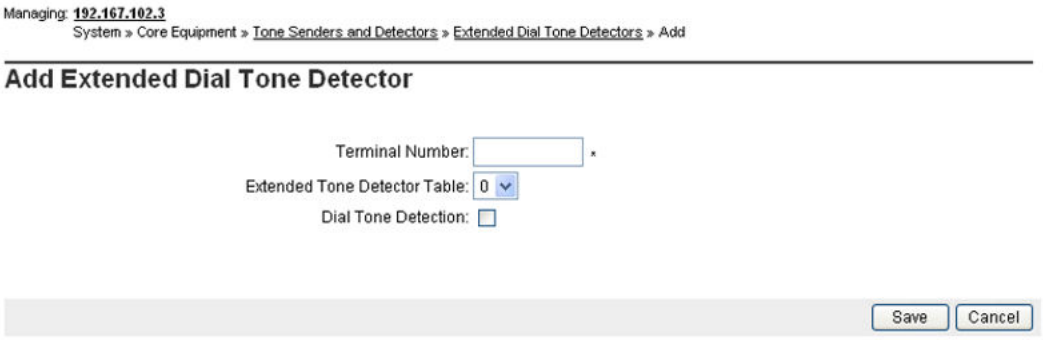


Figure 56: Add Extended Dial Tone Detector Web page

Adding an Extended Dial Tone Detector

1. Type the **Terminal Number** of the Extended Dial Tone Detector.
2. From the list, select the **Extended Tone Detector Table**.
3. If required, select **Dial Tone Detection**.
4. Click **Save**.

To move an Extended Dial Tone Detector card from one terminal to another, on the Extended Dial Tone Detectors Web page, select the radio button beside the **Terminal Number** to move and click **Move**. The Move Extended Dial Tone Detectors Web page appears, as shown in Figure 57: Move Extended Dial Tone Detectors Web page on page 121.

Figure 57: Move Extended Dial Tone Detectors Web page

Type the **Destination Terminal Number** and click **Save** .

Peripheral Equipment

The Peripheral Equipment Web page displays parameters such as Timers, Multi-Frequency levels, and Make-Break ratio.

To view, configure, or edit Peripheral Equipment click the **Peripheral Equipment** link of the **System** branch of the Element Manager navigator. The Peripheral Equipment Web page appears as shown in Figure 58: Peripheral Equipment Web page on page 122.

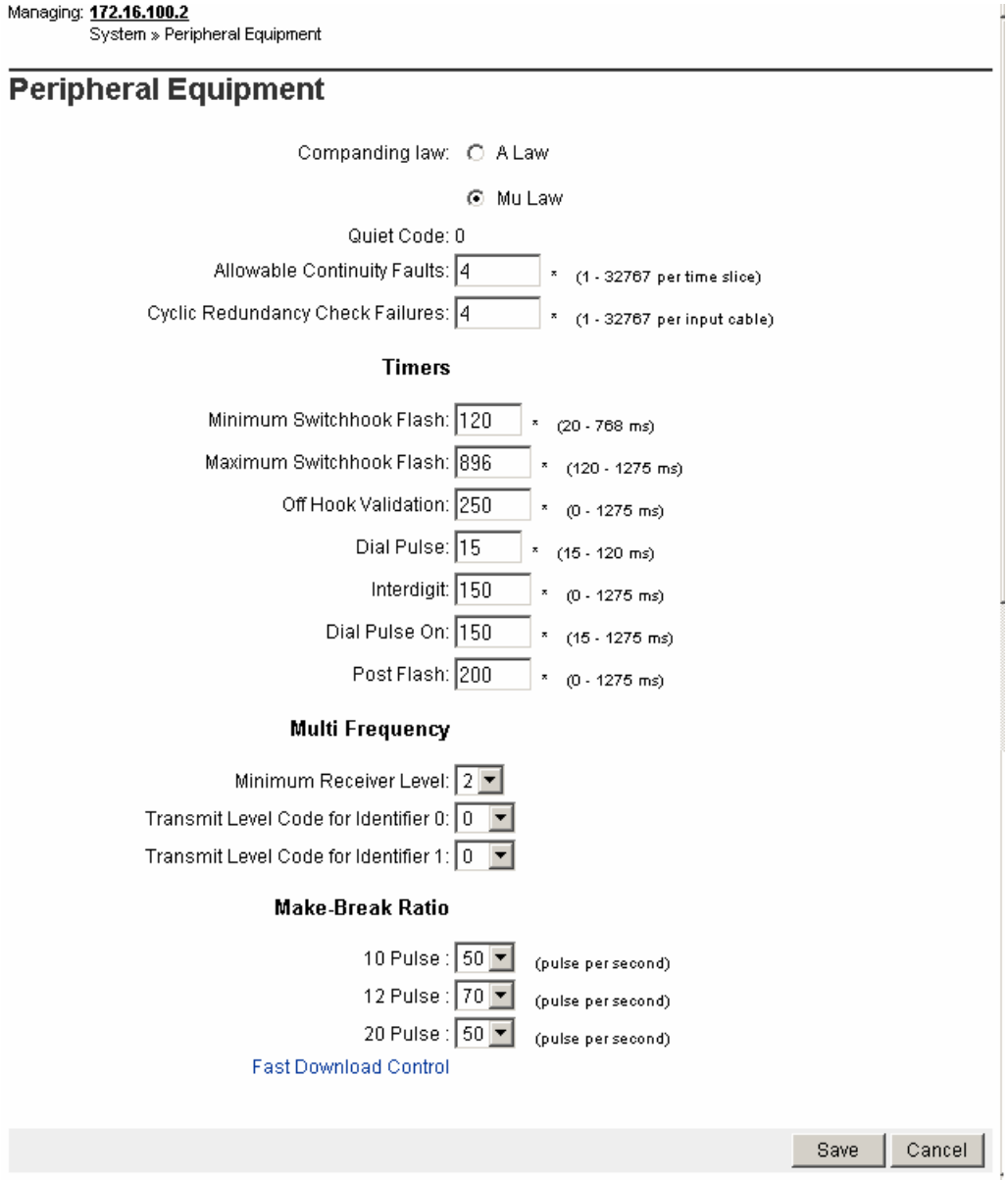


Figure 58: Peripheral Equipment Web page

To configure or edit the Peripheral Equipment, enter the appropriate values and click **Save**. If you enter invalid values, the system displays an error message and retains the original values. A link for **Fast Download Control** is provided.

Chapter 8: IP Network

Contents

This chapter contains information about the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Introduction

To view the version of software that is installed on the elements, click the **IP Network** link of the **System** branch of the Element Manager navigator.

IP Network

IP Telephony Nodes

Node management in Communication Server 1000 includes a work flow on the User Interface (UI), with Add and Modify functions of the Node. This introduces the Cluster concept, where a Cluster represents a group of physical servers that shares the same configuration properties. The same set of services are configured and enabled on all physical servers within a Cluster.

The Nodes also provide scalability (by deploying multiple Nodes) and optionally Load sharing (by distributing processing to other Node members.

Each Node belongs to a Call Server and has a one-to-many relationship with Call Server. The IP Nodes resides on two LAN subnets: ELAN and TLAN.

Important:

For information about node to Call Server mapping and the restore process, see Restoration of IP Telephony Nodes from a prior-Release Call Server on page 369.

The Node must have aminimum of one Signaling Server as a Node element in order for that Node to be operational. The administrator can add many servers to be part of the Node and all the Node elements will have the same set of application services enabled. However, only one physical server can be active at a time. This active server can run all the configured services on that physical server; for example, UNIStim LTPS, SIPGw, and H323Gw can all be configured and enabled on the same server. The LTPS application is one exception where several servers can run active instances of LTPS service. The LTPS application does support load sharing.

Note:

The SIP Line application in CS 1000 cannot co-reside with LTPS or any other virtual trunk applications like SIPGw or H323Gw. The Node management interface does not allow the user to configure SIP Line service any other application services.

The gateway application services operate on a service IP address configured to be on the TLAN of the network and this IP address floats between active and standby servers. The standby server takes over this IP address when the active instance goes down. The active and standby roles are dynamically assigned through a service specific election process that runs on the servers.

In CS 1000, the Centralized Deployment Manager (CDM), deploys software applications from Unified Communication Management (UCM).

The Node management interface adds servers to a Node from the list of servers that UCM has learned. Before you add the servers to a Node, it is required that the CDM feature deploys the necessary software application to each of the Linux servers.

To view the **IP Telephony Nodes** Web page, select the **Nodes: Servers, Media Cards** link in the IP Network branch of the Element Manager navigator. The IP Telephony Node Web page appears as shown in, Figure 59: IP Telephony Nodes Web page on page 125.

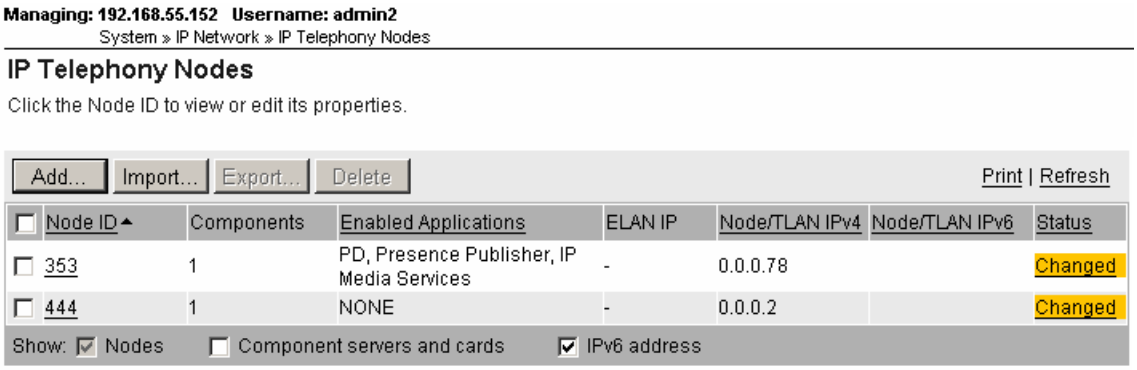


Figure 59: IP Telephony Nodes Web page

The IP Telephony Nodes Web page appears showing the following information:

- Node ID — the ID number for each node
- Components — the number of components associated to each node
- Enabled Applications — the applications enabled to each node
- ELAN IP — the IP address for the ELAN
- Node/TLAN IPv4 — the TLAN IPv4 address of the Node or Servers and Cards
- Node/TLAN IPv6 — the TLAN IPv6 address of the Node or Servers and Cards

Important:

When you select **Components servers and cards**, the servers and cards appear in rows along with the IPv4 and IPv6 addresses.

- Status — the status of the node

The IP Telephony Nodes Web page also contains buttons that link to additional Web pages:

- Add - add a new node
- Import - Import a node files
- Export - export a node file
- Delete - delete a node

To view Component Servers and Cards, select the **Component Servers and Cards** box at the bottom of the IP Telephony Nodes Web page.

To view TLAN IPv6 address, select the **IPv6 Address** box at the bottom of the IP Telephony Nodes Web page.

If you are installing UCM as a new installation (as opposed to an upgrade from a previous release), with elements installed manually, registered to the security domain and grouped using deployment manager, then you must also install the IP Telephony node elements manually using Element Manager. Only UCM registered elements (Signaling Servers and Media Cards) can be grouped and added to the node as elements.

If you do not enter, register and group the elements manually, any attempt to execute a restore operation of the IP Telephony node files on the Call Server fails.

Add a new IP Telephony Node

Click the Add button from the summary page to start the add work flow for creating a new Node to be part of the Call Server where Element Manager is hosted. The New IP Telephony Node Web page appears as shown in, Figure 60: New IP Telephony Node Web page on page 127. For information about adding a new IP Telephony node, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

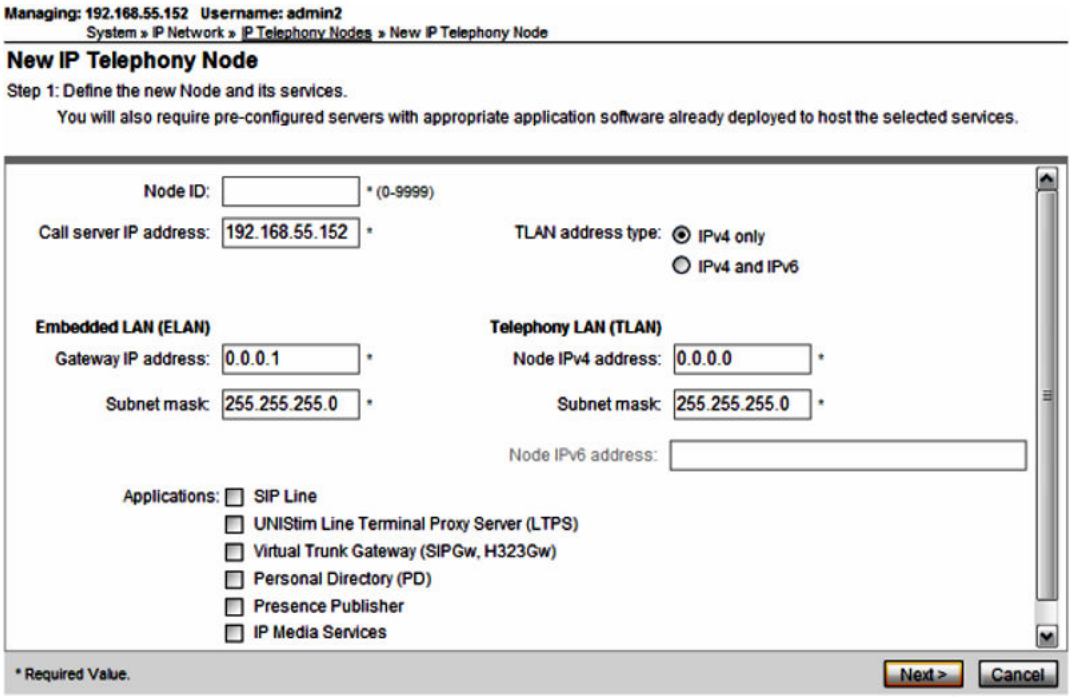


Figure 60: New IP Telephony Node Web page

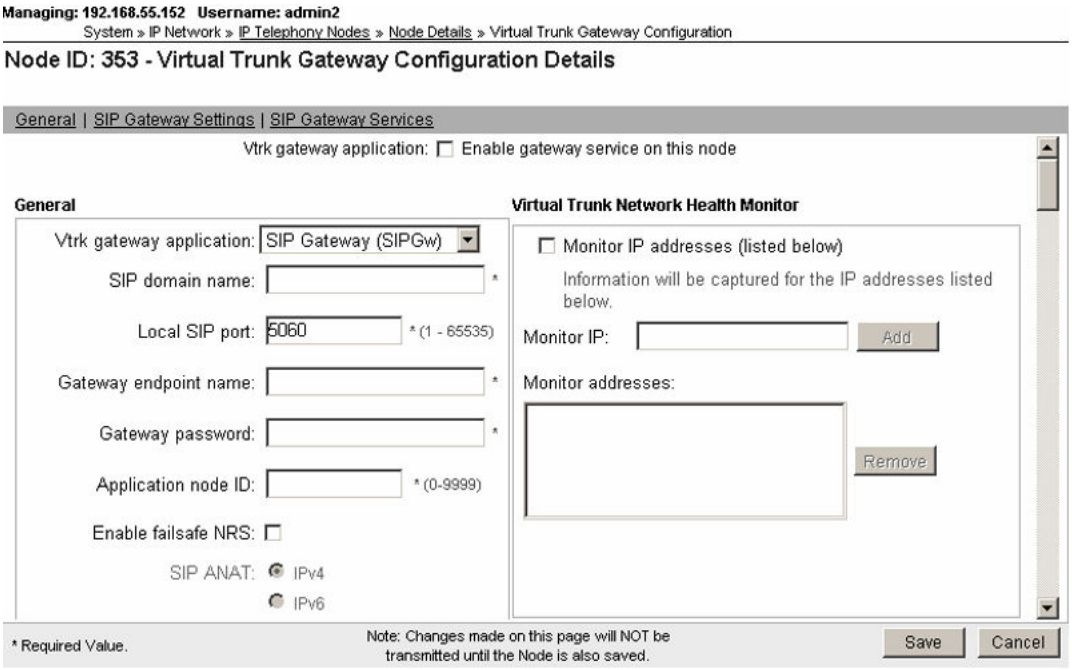


Figure 61: New IP Telephony Node Web page1

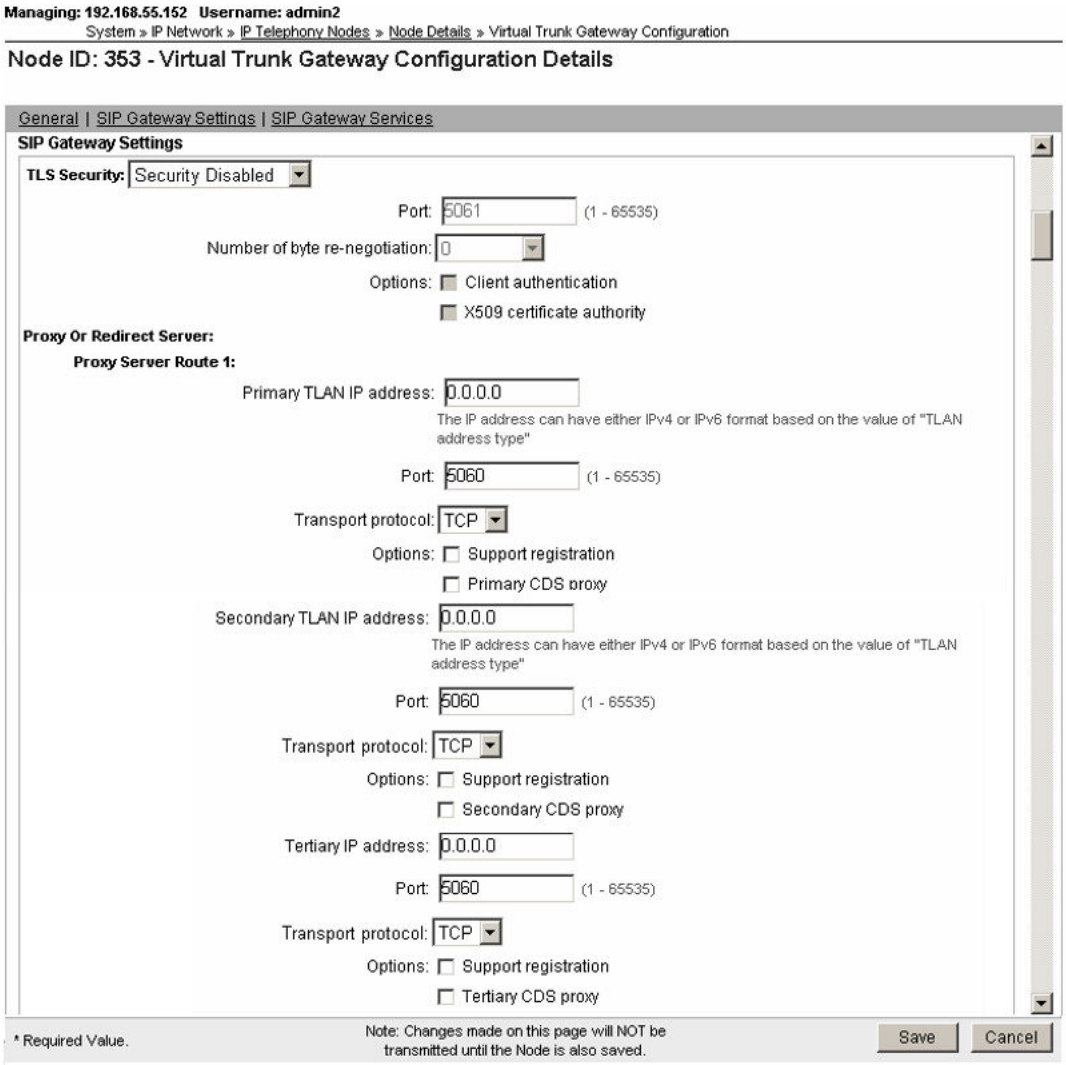


Figure 62: IP Telephony Node - SIP GW settings 1

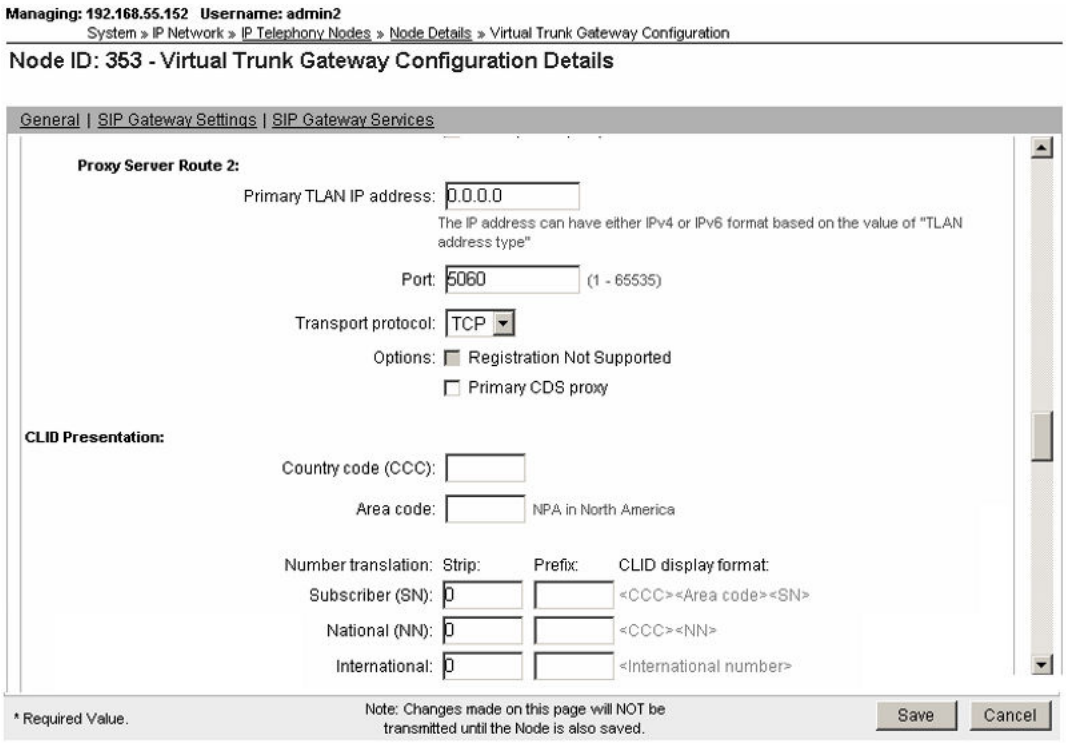


Figure 63: IP Telephony Node - SIP GW settings 2

In the Proxy Server Route 2 block you can configure the following parameters.

- Primary TLAN IP Address
- Port
- Transport Protocol
- Options

You can configure both Proxy Server Routes 1 and 2 for SIP GW. The values from the config.ini file are read based on the preferred route value configured in overlay 86 (PROU).

Enter the required values in the fields and click **Save** .

Import IP Telephony Nodes file

Use the import functionality to import a local configuration file from a local work station (XML format) or from a Linux signaling server.

In the case of configuration file imported from a local work station, you must enter the configuration parameters in the file in a standard template model. This template follows the same model as the existing config.ini file format. You can enter as much as information to a local file and then import, edit, and save, using the import UI page, on the Call Server just like any IP Telephony Node.

Click the **Import** button, the IP Telephony Import Web page appears as shown in, Figure 64: Import IP Telephony Nodes Web page on page 130. The options for the import operation

appear in the IP Telephony Import Web page, the options are import from an XML file stored on local work station or import from a Leader server that is already part of a Node.

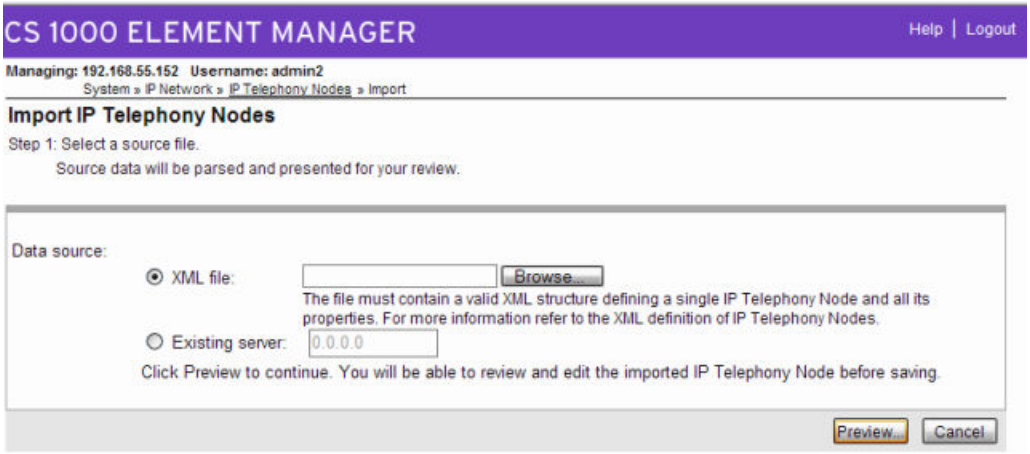


Figure 64: Import IP Telephony Nodes Web page

The selected XML file that is selected to import goes through two sets of validations before the file can be saved on to the system:

- An invalid XML file format is determined when you click the Preview button to preview the content, the UI will be displayed with a message indicating invalid XML file.
- If the file is valid, the next set of validations make sure that the content inside passes the filed and dependency validations. This validation is determined when you click the Save button to save the configuration to the Call Server.

When Node configuration files generated by TM application are to be imported by EM, you must remove the ^M (control M) characters from the Node files using procedure Removing (control M) characters from Telephony Manager configuration files on page 130.

The Node configuration files generated by TM application are obtained from the same place inside the Call Server (`/u/db/node/`) as any of the EM application generated Node files.

Whether TM generated or EM generated, the Node configuration file names would be the same (nodexxxx.cfg and nodexxxx.btp) when stored on the Call Server.

During a Call Server upgrade, if the Node files that are being backed up actually come from TM application then you must remove the ^M characters from the files. Use the following procedure before they are loaded with an EM application.

Removing (control M) characters from Telephony Manager configuration files

1. Use an FTP program to move the Node configuration files from the Call Server to any unix server, the files would have the naming as nodexxxx.cfg and nodexxxx.btp where the xxxx is the node id number.
2. You can edit these config files to see if they have ^M characters present inside
3. If ^M characters are present, run the `dos2unix` command on each of the files.

The `dos2unix` command can be found on any unix server in the `/usr/bin/` folder .

4. The syntax of the command is as follows:

   - **dos2unix *<old file name> <new file name>***

     Keep the output file name the same as the input file name, you can check the time stamp and/or edit the file to verify if ^M characters have been removed.

   - Do this for both the xxxx.cfg and the xxxx .btp files.

     For example for node3434.cfg (config file) and node3434.btp (bootp file) the syntax would be:

     - `dos2unix node3434.cfg node3434.cfg`
     - `dos2unix node3434.btp node3434.btp`

5. Edit the config and bootp files to check if the ^M chars have been removed.
6. Use an FTP program to move the the files back to the Call Server in the `/u/db/node/` folder
7. Launch EM and open the IP Node Telephony page, the Node summary page appears correctly.

Export IP Telephony Node file

You can export a previously configured IP Telephony Node to an XML file format and save it to a local desktop. The Export function is limited to one selected Node at a time. If you select more than one node, the **Export** button remains disabled.

To export a IP Telephony Node to an XML file select a Node on the IP Telephony Nodes Web page and click **Export**. The export saves the configuration files in an XML format file.

Delete an IP Telephony Node

To delete an IP Telephony Node select, the Node and click the **Delete** button. A confirmation window appears.

Node Details

Click the Node ID listed on the IP Telephony Node page to view or edit the properties of that node. The Node Details Web page for the Node selected appears as shown in, Figure 65: Node Details Web page on page 132.

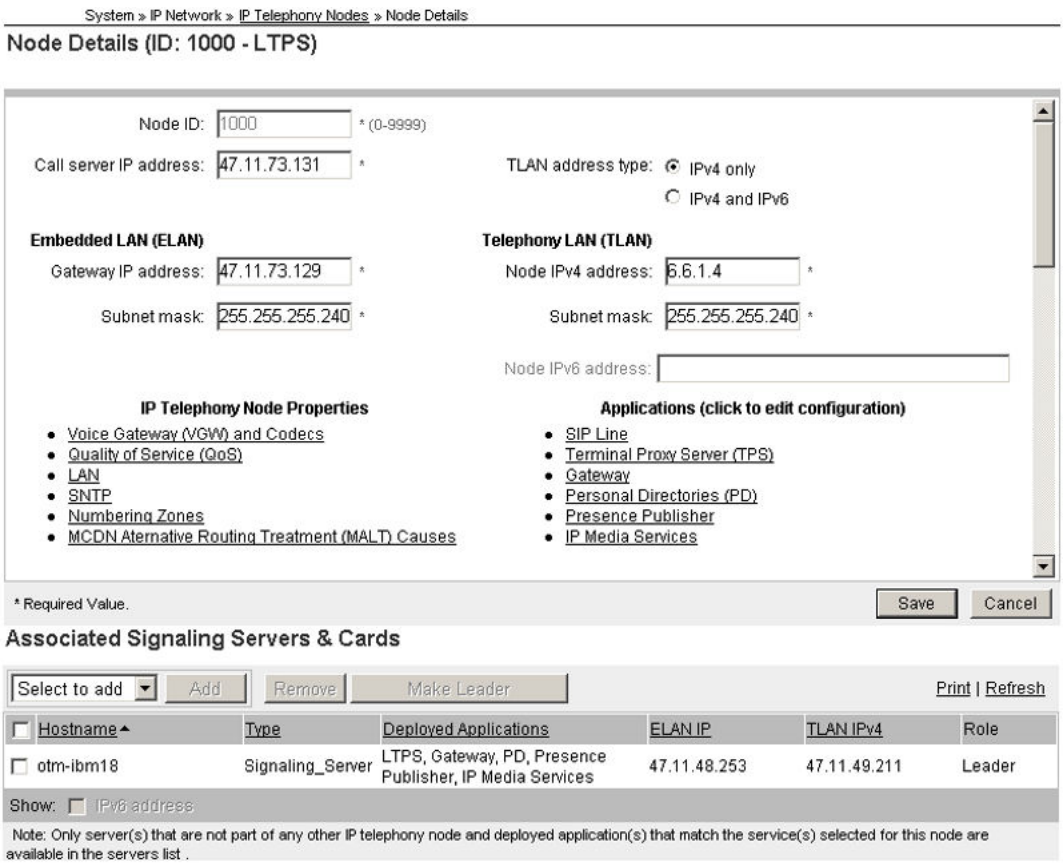


Figure 65: Node Details Web page

The Node Details Web page is organized to list the **IP Telephony Node Properties** on the left side of the page and the **Applications** on the right side of the page. Click on the IP Telephony Node or the Application you want to configure. For example, click **Voice Gateway (VGW) and Codecs** to display the Voice Gateway (VGW) and Codecs Web page as shown in, Figure 66: Voice Gateway (VGW) and Codecs Web page on page 133.

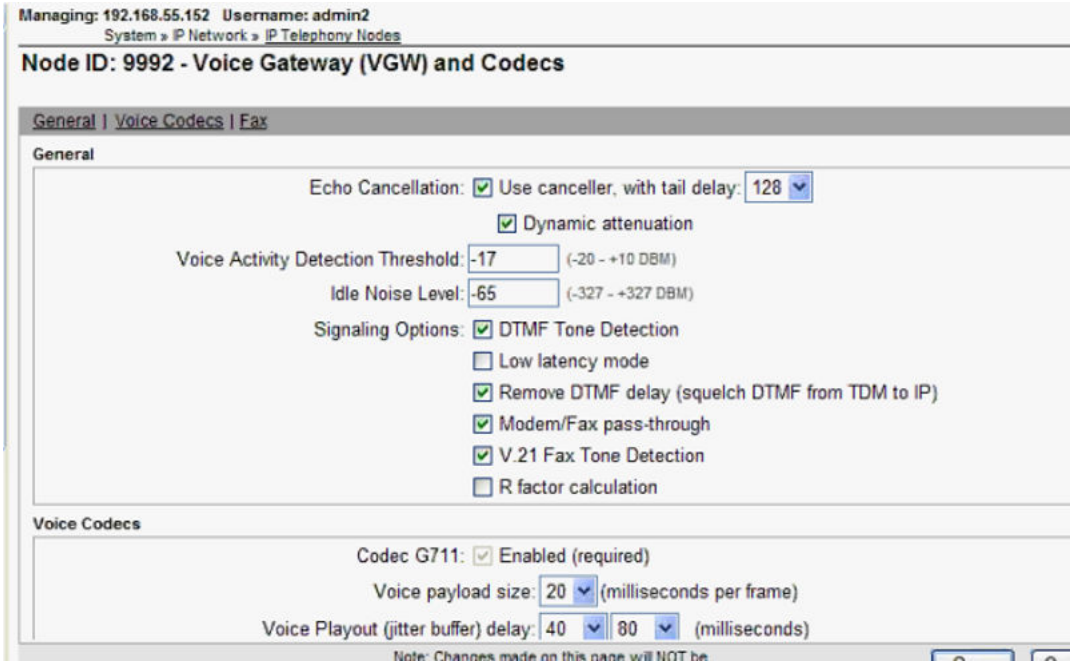


Figure 66: Voice Gateway (VGW) and Codecs Web page

Click **Save** or **Cancel** to return to the Node Details Web page. When you save the parameters configured for the Voice Gateway (VGW) and Codecs Web page, only the codec parameters are saved; you must click **Save** on the Node Details Web page to save the changes to the IP Telephony Node.

You can configure the following IP Telephony Node Properties by clicking on the appropriate link on the Node Details Web page:

- Voice Gateway (VGW) and Codecs
- Quality of Service (QOS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternate Routing Treatment (MALT) Causes

You can configure the applications associated to the Node by clicking the appropriate link on the Node Details Web page. The applications associated to a Node appear on the right and can include applications such as the following:

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway
- Personal Directories (PD)

- Presence Publisher
- IP Media Services

After you click the **SIP Line** link, on the Node Details Web page, the SIP Line Configuration Details Web page appears as shown in the following figure.

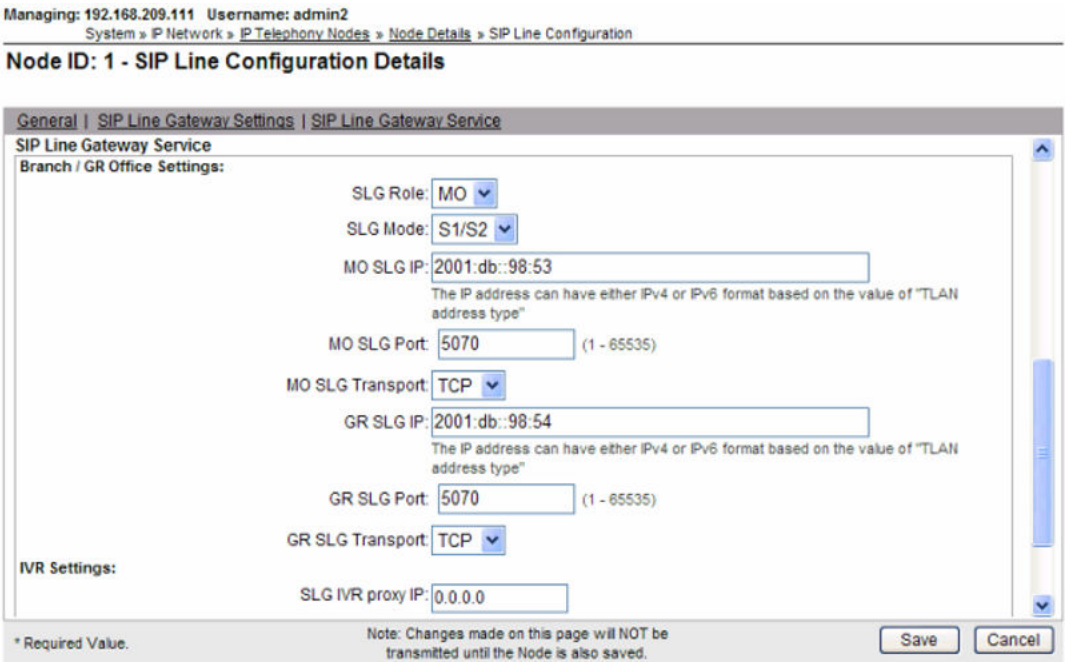


Figure 67: SIP Line configuration

Enter the appropriate values in all the required fields and click **Save** to configure SIP Line.

For complete information about IP Telephony Nodes configuration, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*, *Avaya SIP Line Fundamentals, NN43001-508*, *Avaya Dialing Plans Reference, NN43001-283*, and *Avaya IP Peer Networking Installation and Commissioning, NN43001-313*.

After you click **Terminal Proxy Server (TPS)**, on the Node Details Web page, the Terminal Proxy Server (LTPS) Configuration Details page appears as shown in the following figure Figure 68: Network Connect Server (NCS) configuration on page 135.

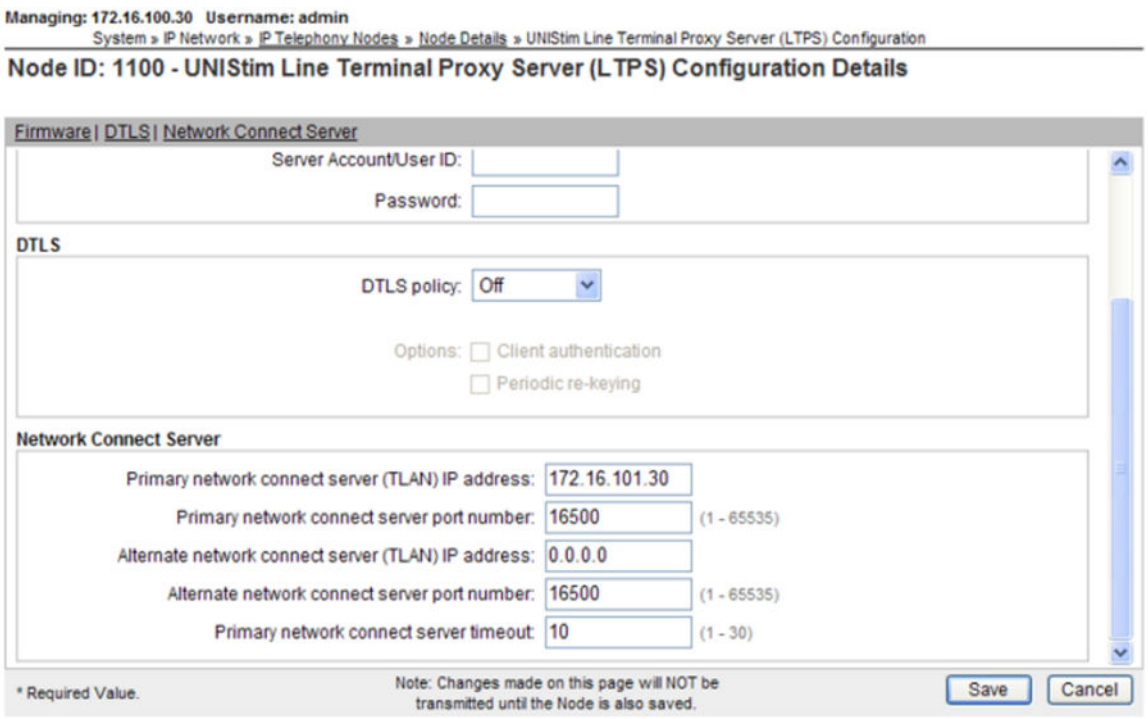


Figure 68: Network Connect Server (NCS) configuration

Configure the **Network Connect Server** (NCS) parameters, and then click **Save**. To apply the NCS configuration, on the Node Details page, click **Save**.

After you click the **Gateway** link, on the Node Details Web page, the Virtual Trunk Gateway Configuration Details Web page appears as shown in the following figure.

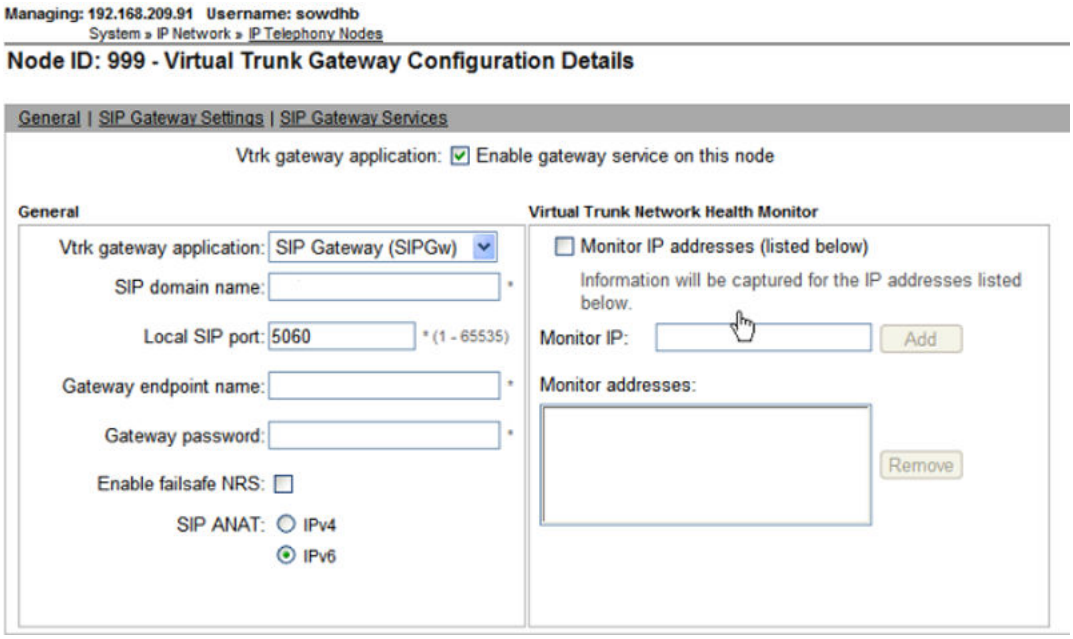


Figure 69: Virtual Trunk Gateway configuration

After you click the **IP Media Services** link, on the Node Details Web page, the IP Media Services Configuration Details Web page appears, as shown in the following figure.

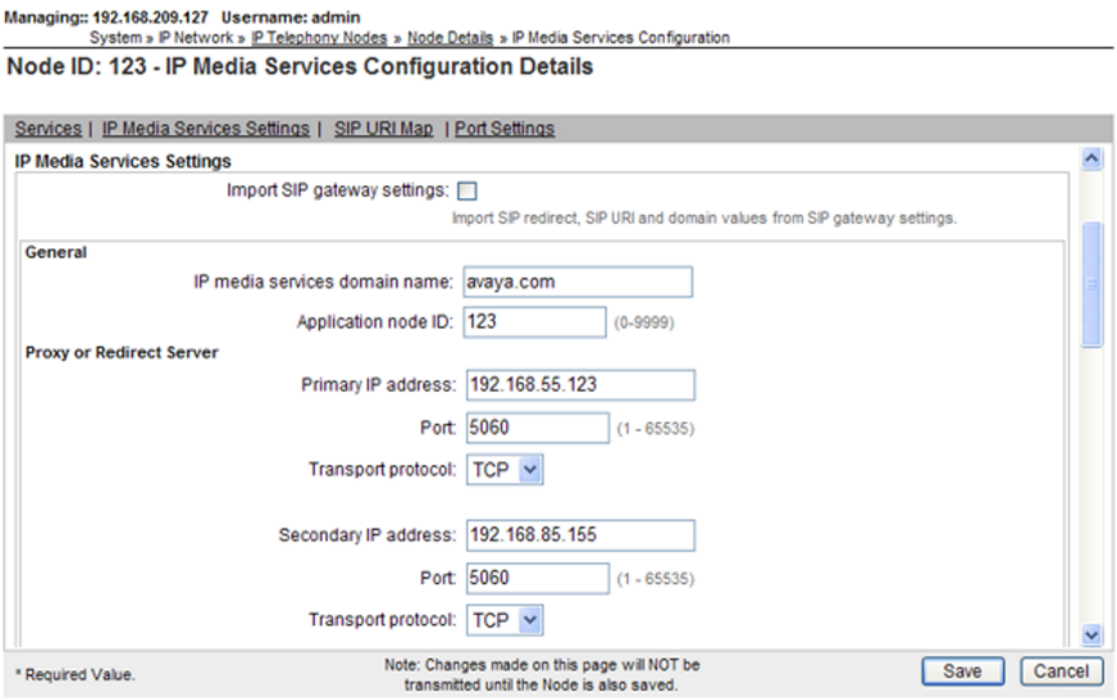


Figure 70: IP Media Services configuration

To configure IP Media Services, enter the appropriate values in the required fields and click **Save**.

For complete information about IP Media Services configuration, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

For complete information about IP Telephony Nodes configuration, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*, *Avaya SIP Line Fundamentals, NN43001-508*, *Avaya Dialing Plans Reference, NN43001-283*, and *Avaya IP Peer Networking Installation and Commissioning, NN43001-313*.

Activate the Presence Publisher in Element Manager for an existing node

Presence Publisher in Element Manager CS 1000 release 7.6

Note:

The CS 1000 (native) IM and Presence application is supported for CS 1000 Releases 6.0 and 7.0. Releases 7.5 and later align with Avaya Aura Presence Services 6.1 for Instant Messaging and Presence across Avaya's Enterprise Communications Manager and CS 1000 Call Servers. CS 1000 Release 7.6 does not support the older IM/Presence application from CS 1000 releases 6.0 and 7.0.

Simple Network Time Protocol

Click **SNTP** to access the SNTP Web page, as shown in the following figure.

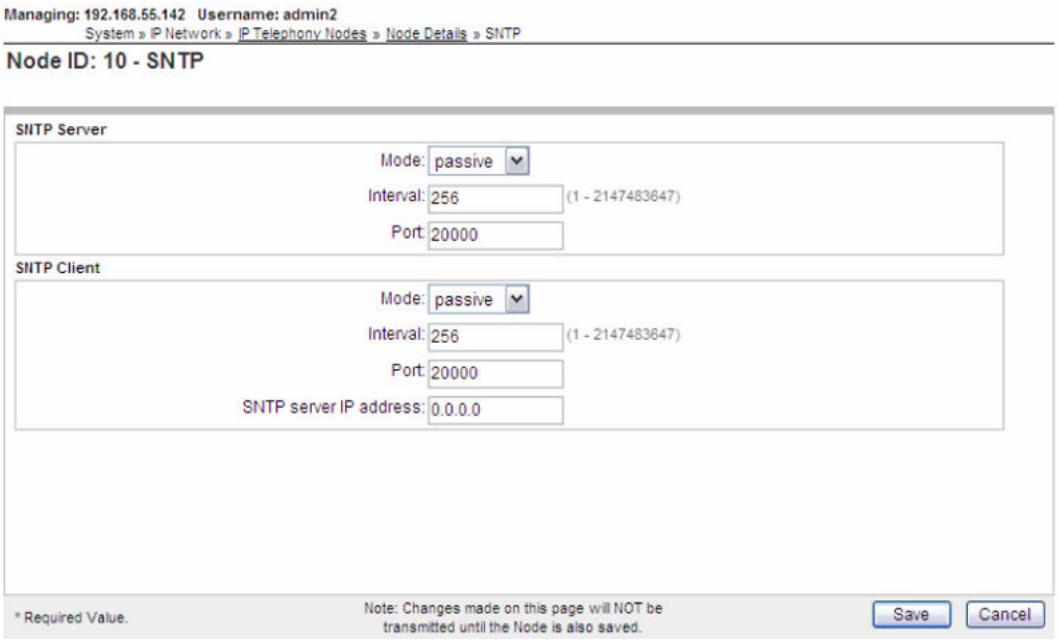


Figure 71: SNTP Web page

The Simple Network Time Protocol (SNTP), is an adaptation of the Network Time Protocol (NTP) used to synchronize computer clocks. It involves no change to the current or previous NTP specification versions or known implementations, but rather a clarification of certain design features of NTP which allow operation in a simple, stateless RPC mode with accuracy and reliability expectations similar to the UDP/TIME protocol. A SNTP server running on the primary Signaling Server or the IP Telephony leader Cards actively push the date and time to the SNTP clients (Voice Gateway Cards and other Signaling Servers). Clients can also pull the date and time from SNTP server.

The following parameters are available for the network time client/server from IP Telephony Nodes page:

- Mode: This field defines the protocol mode. They are three options for this:
  - Active – Sends broadcast of time at defined intervals.
  - Passive – Waits for query from clients (default).

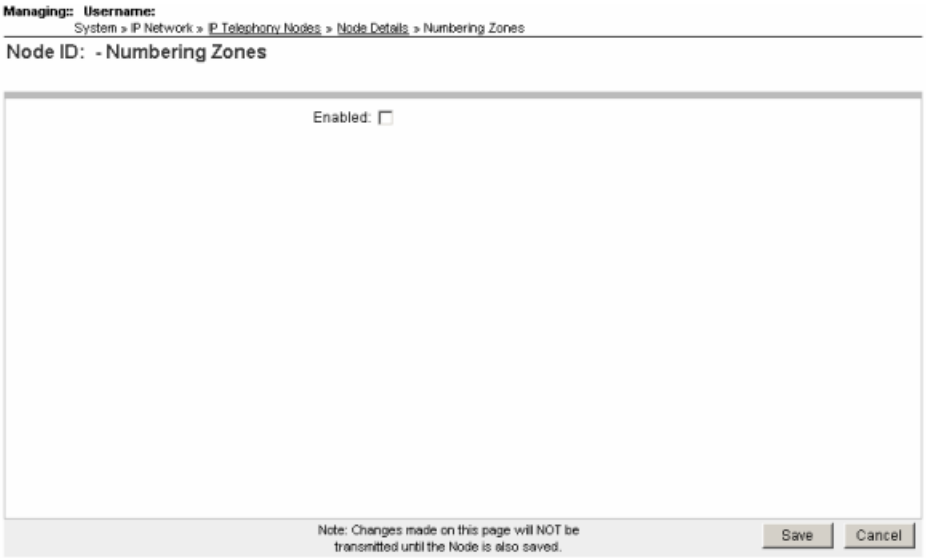
- Disabled – Time server not started.

- Interval: Assigns the interval between time updates and can be set to any 2n value (31 > n > 0) (256).
- Port: This is the network port that the system service listens to for incoming network traffic. The port number is determined when the connection is established. Assigns the UDP port used by time client/server(20,000 + nodeId)

There is one more field under **SNTP CLIENT** section, which is **SNTP server IP address**. This field defines the IP address of the server to which the client communicates. It is an IPv4 address.

Enable Numbering Zones

When you click the **Numbering Zones** link in the Node Details web page, the Node ID xx Numbering Zones Web page appears, as shown in the following figure.



To enable Numbering Zones select **Enabled** and click **Save**.

Nodes: Servers, Media Cards

Click the **IP Network > Maintenance and Reports** link in the **System** branch of the Element Manager navigator to open the Node Maintenance and Reports Web page, as shown in Figure 72: Node Maintenance and Reports Web page on page 140.

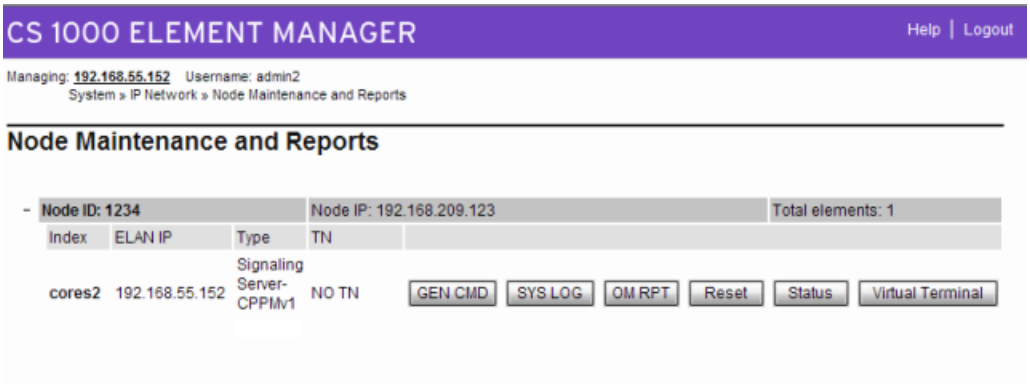


Figure 72: Node Maintenance and Reports Web page

This Web page contains information about configured Signaling Servers and IP Telephony cards and is arranged by node. Click the required buttons such as, GEN CMD, SYS LOG, Reset and others beside the Node ID number to view the elements assigned to the node.

For more information about IP Telephony, see *Avaya Signaling Server IP Line Application Fundamentals, NN43001-125*.

Six buttons are located to the right of the TN column for each IP Telephony element:

- **GEN CMD** — Launches the General Commands Web page.
- **RPT LOG** — Launches the Report Utility Web page.
- SYS LOG — Launches the System log file Web page for Signaling Servers.
- **OM RPT** — Launches the Operational Management Report Web page.
- **Reset** — Resets the element.

Note:

The ELAN IP address of the server must be entered in the host table prior to launching Base Manager using the **Reset** button.

Note:

When resetting the Signaling Server on which the Web server is located, wait approximately five minutes before logging in again.

- **Virtual Terminal** — Opens a Telnet connection to the element over the Telephony Local Area Network (TLAN) subnet using the element's IP Address.
- **Status** — Displays the status of the element.

Meridian Alternate Routing and Vacant Number Routing Causes

This feature deals with Vacant Number Routing (VNR) calls at the CS 1000 that is routed over H323/SIP. Assume that the call fails to route to the destination (for example, with reason: No

entry present in the NRS/SPS or due to rejection from the destination side). With this development, the call gets disconnected with a cause which matches one of the Meridian Alternate Routing (MALT) cause codes, or disconnects with an indication to "use MALT". Based on this information, MALT is performed at the Call Server to retry the call using an alternate route. If MALT exhausts all the MALT routes in the VNR Route List Index then the treatment corresponding to the disconnect cause is provided.

If the call clearing message has the cause as 'unassigned number' or 'invalid Number format' in all the accessed entries of the VNR RLI, then vacant number treatment will be provided.

With the default MALT handling, there are six causes which perform MALT at the CS 1000:

- 3 — No route to destination
- 27 — Destination is out of service
- 34 — No circuit or channel available
- 38 — Network out of service
- 41 — Temporary failure
- 42 — Switching equipment congestion

A configurable option is provided in Element Manager for the different vendors (subdivided into "all Avaya Component" and "third party", but potentially extensible, should the need be identified) in order to configure causes (other then MALT causes) to do MALT at CS 1000. The EM provisions the below causes to be configured to perform MALT. The unassigned number cause will be by default configured to perform MALT for Avaya and Third Party vendors.

- 01 — unassigned number
- 20 — subscriber absent
- 47 — Resources unavailable
- 51 — Call rejected; blocked by MBG
- 52 — Outgoing call barred
- 53 — Outgoing call barred in closed user group
- 54 — Incoming call barred
- 55 — Incoming call barred in closed user group
- 63 — service or option not available
- 127 — Interworking unspecified

To configure MALT, click the **IP Network > Nodes: Severs, Media Cards** link in the **System** branch of the Element Manager navigator. The IP Telephony Nodes Web page appears. Click the **Node ID** of the node you want to configure, and then click **MCDN Aternative Routing Treatment (MALT) Causes** ; the MCDN Aternative Routing Treatment (MALT) Causes Web page appears as shown in Figure 73: MCDN Aternative Routing Treatment (MALT) Causes Web page on page 142.

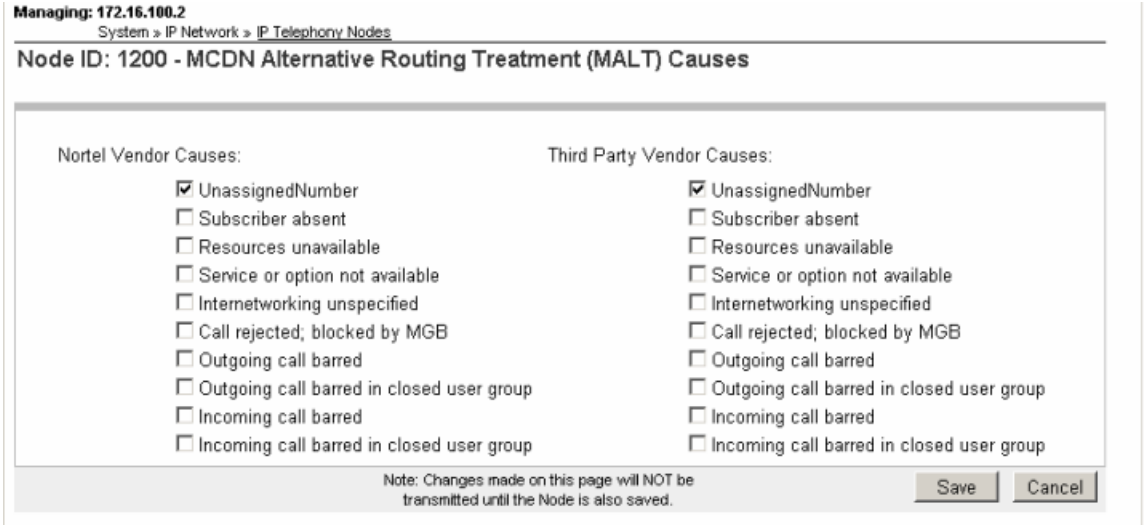


Figure 73: MCDN Aternative Routing Treatment (MALT) Causes Web page

Important:

If you add a Media Card after you upgrade the Linux server, you must perform a Node Save and Transfer. For more information, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

General Commands

Click the **GEN CMD** button, located beside the information for an IP Telephony element as shown in Figure 72: Node Maintenance and Reports Web page on page 140, to open the General Commands Web page for that element. See Figure 74: General Commands Web page on page 143.

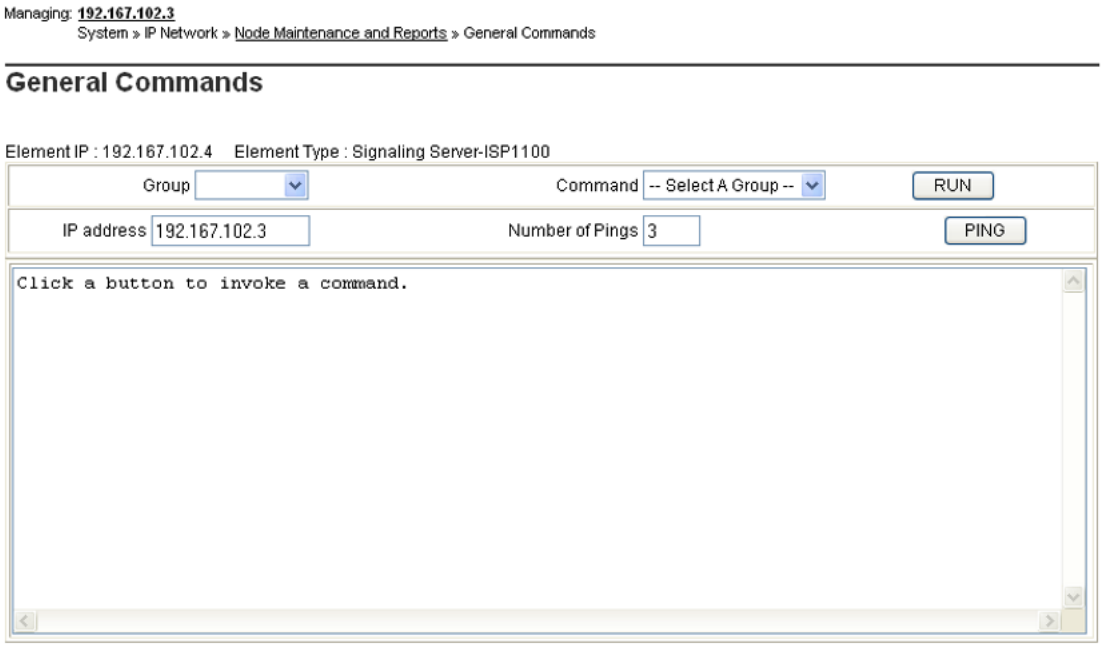


Figure 74: General Commands Web page

From this Web page, users can issue commands to selected groups.

To issue an IP Line application command:

1. Select a group from the left-hand **Group** drop-down list. The corresponding commands for that group display in the **Command** drop-down list.
2. Select a **Command** from the **Command** drop-down list.
3. Click **Run**.

   The results appear in the box at the bottom of the Web page.

Detailed procedures for issuing General Commands can be found in *Avaya Signaling Server IP Line Application Fundamentals, NN43001-125*.

Commands related to the node password include:

- nodePwdDisable — disables the node password
- nodePwdEnable — enables the node password
- nodePwdShow — displays the node password
- nodeTempPwdClear — clears the temporary node password
- nodePwdSet — sets the node password
- nodeTempPwdSet — sets the temporary node password

Passwords must conform to certain compositional rules.

To set the node password:

1. Select **nodePwd** from the **Group** drop-down list.
2. Select **nodePwdSet** from the **Command** drop-down list.
3. Enter the password in the **Node Password** text box.

   The password must be 6 - 14 characters in length. Valid entries are digits 0 through 9, and special character * and #.
4. Click **RUN**.

   If a non-zero length password is configured, all IP Phones that attempt to register after the password is set display a prompt requesting the node password before enabling the TN to be modified.

A temporary node password can be configured to give temporary user access to the TN for configuration. A temporary node password removes the need to distribute the node password and the requirement to change it afterwards. The temporary node password automatically deletes itself after it has been used the defined number of times or when the duration expires, whichever comes first.

To set a temporary node password:

1. Select **nodePwd** from the **Group** drop-down list.
2. Select **nodeTempPwdSet** from the **Command** drop-down list.
3. Enter the temporary password in the **Node Password** text box.

   The password must be 6 - 14 characters in length. Valid entries are digits 0 through 9, and special character * and #.
4. Enter the number of times that you want to enable the temporary password to be used in the **Uses** text box (maximum is 1000 times).
5. Enter the duration, in hours, for the temporary password in the **Timeout** text box (maximum is 240 hours).
6. Click **RUN**.

From the General Commands Web page, any IP address can be pinged from this element. The default IP address is the address of the Call Server.

To ping an IP address, perform the following procedure.

1. Verify that the entry in the **IP address** text box is correct.
2. Enter the number of pings that to send in the **Number of Pings** text box.
3. Click **Ping**.

System Log

Click the **SYS LOG** button, located beside the information for the Signaling Server, to open the Application Logs Web page for the Signaling Server, as shown in Figure 75: Application Web page on page 145. The Application logs are part of the Base Manager.

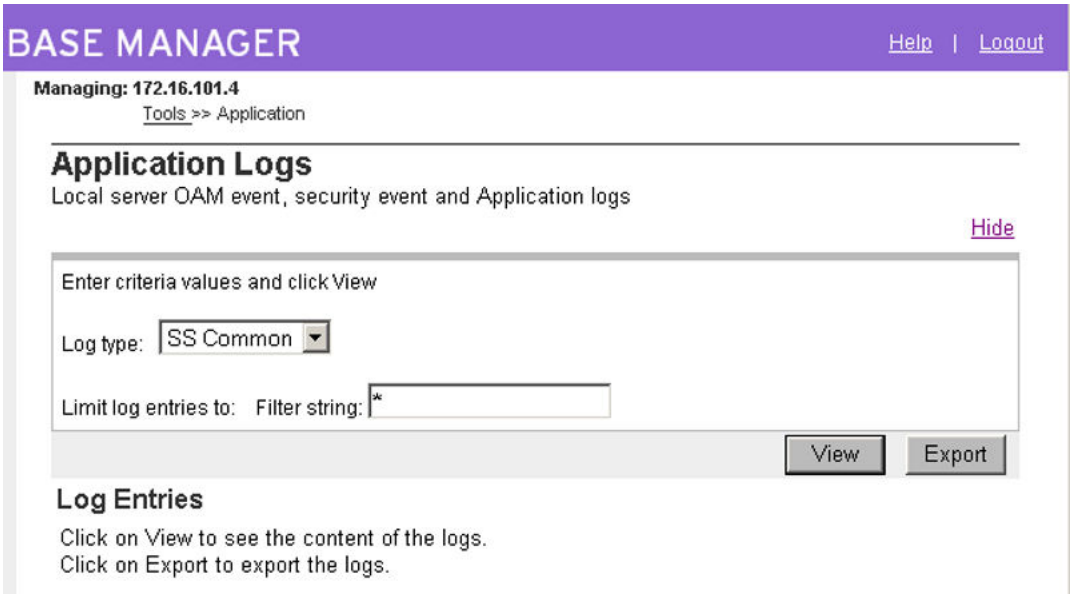


Figure 75: Application Web page

Element Manager redirects you to Base Manager to run the System Log for the Signaling Server. For more information about Application Logs and accessing Base Manager refer to *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315,* and *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

System log

Click the **SYS LOG** button, located beside the information for an IP Telephony card, to open the Syslog Web page for the IP Telephony card, as shown in Figure 76: Syslog Web page on page 146.

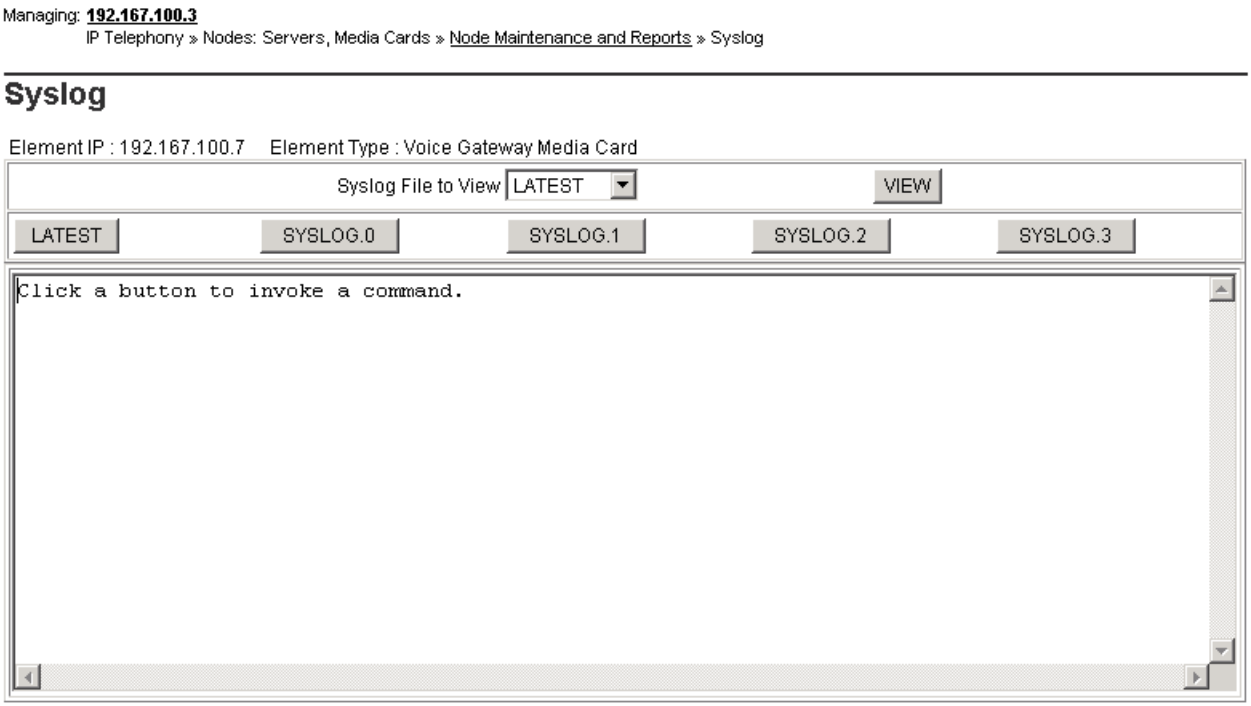


Figure 76: Syslog Web page

To view a System log file, perform the following procedure.

1. Select a file using the **Syslog File to View** drop-down list.
2. Click **VIEW**.

Alternatively, click one of the five buttons below the Syslog File to view the dialog box:

- **LATEST** — Displays the most recent record in the system log file.
- **SYSLOG.0** — Displays the file /C:/log/syslog.0 located on the Media Card.
- **SYSLOG.1** — Displays the file /C:/log/syslog.1 located on the Media Card.
- **SYSLOG.2** — Displays the file /C:/log/syslog.2 located on the Media Card.
- **SYSLOG.3** — Displays the file /C:/log/syslog.3 located on the Media Card.

The contents of the file appears in the box at the bottom of the Web page.

Signaling Server commands

Element Manager provides support for executing Signaling Server command line interface (CLI) maintenance commands.

To run Signaling Server commands from Element Manager, select the Maintenance and Reports link in the IP Network branch of Element Manager navigator. The Node Maintenance

and Reports Web page appears as shown in, Figure 72: Node Maintenance and Reports Web page on page 140.

Running Signaling Server commands

1. Choose a Signaling Server and click **GEN CMD** . T

   he General Commands Web page appears. See, Figure 77: Signaling Server General Commands on page 147.
2. Select the Signaling Server CLI command group that you want to access from the **Group** list.
3. Choose a command from the **Command** list.
4. Click **Run** to run the command.

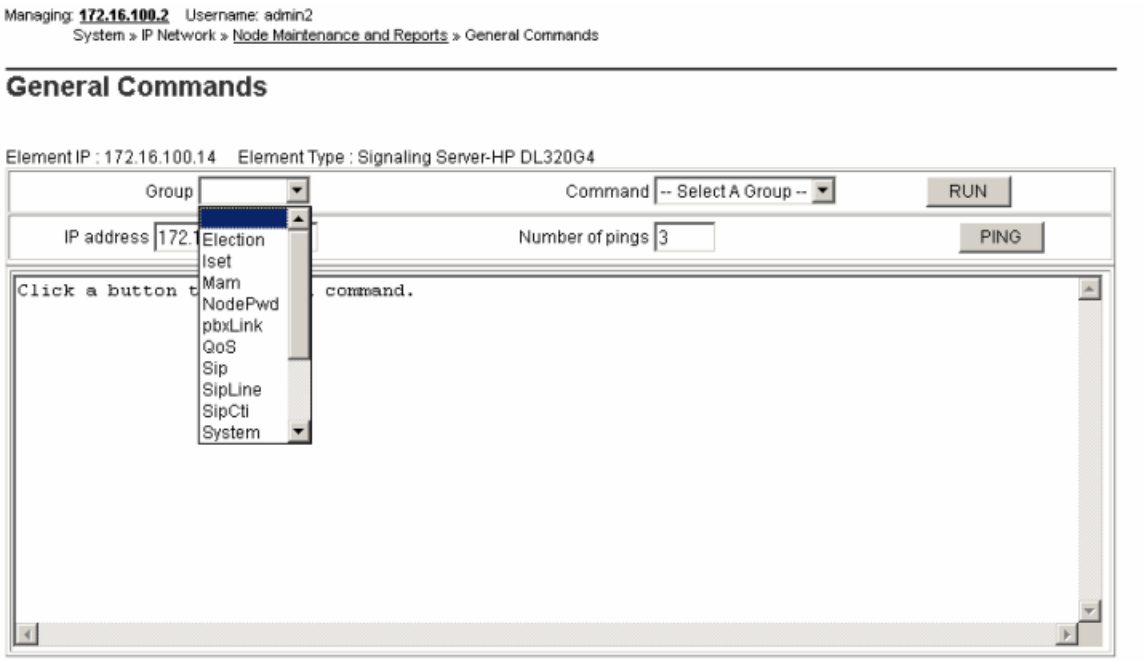


Figure 77: Signaling Server General Commands

For a list of available Signaling Server commands that can be run using Element Manager, see *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

Operational Measurement Reports

The **OM RPT** (Operational Measurement Report) button enables users to view OM information. Click the **OM RPT** button, located beside information for an IP Telephony element as shown in Figure 72: Node Maintenance and Reports Web page on page 140, to open the OM Reports Web page for that element, as shown in Figure 78: OM Reports Web page on page 148.

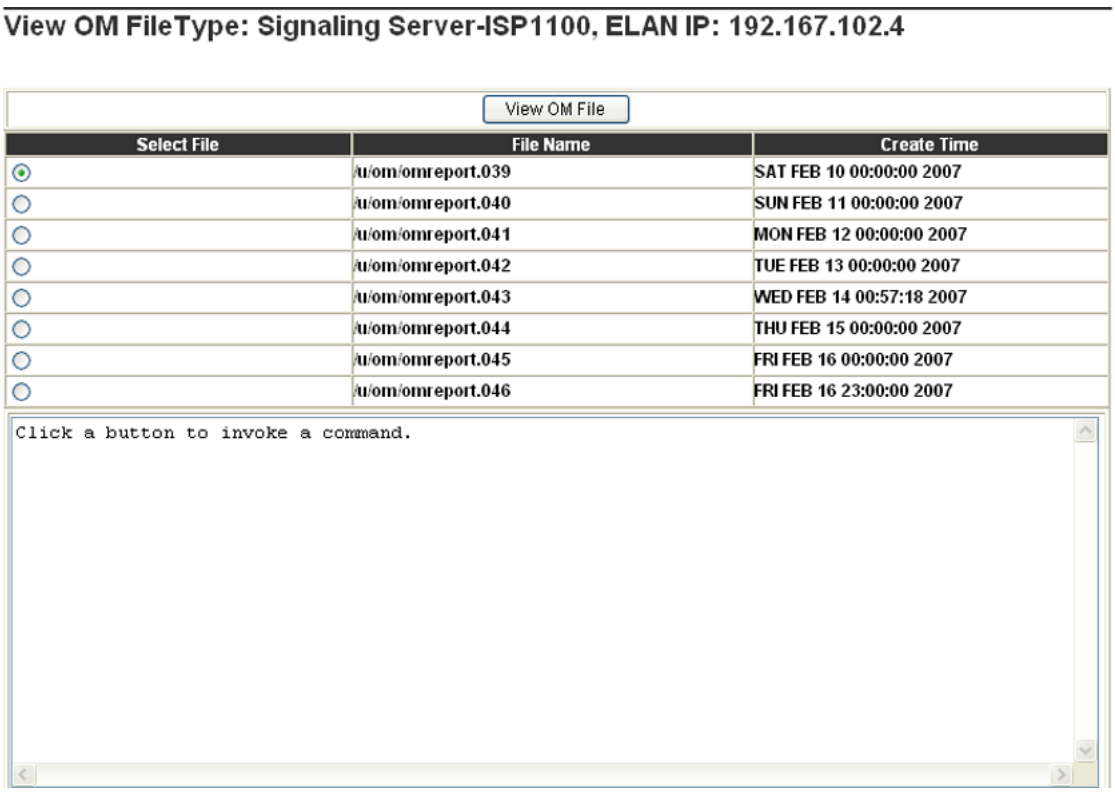


Figure 78: OM Reports Web page

To view an OM Report file, perform the following procedure.

1. In the **Select File** column, click the option button beside the OM Report to be viewed.

   Note:

   The limit of OM Report files is eight. Only the eight most recent OM Report files are available on the system.

2. Click **View OM File**.

The contents of the file appear in the box at the bottom of the Web page.

Virtual Terminal

The Virtual Terminal is an integral part of the enhanced navigation tools for Element Manager.

Click the **Virtual Terminal** button on the Node Maintenance and Reports Web page to open the Virtual Terminal window.

The Virtual Terminal is a Web-based window that enables access to the character-based interfaces supported by the components of the Avaya CS 1000 system, including all overlays

not supported by Element Manager Web pages. The Virtual Terminal can also be used to add new links to the system components or other Element Manager servers using the Bookmarks feature.

Important:

Virtual Terminal requires the Java Runtime Environment (JRE).

To access the Virtual Terminal for a particular IP device, perform the following procedure.

1. Choose the IP device you want to access on the Node Maintenance and Reports Web page.
2. Click the **Virtual Terminal** button beside that node.
3. Enter the user name and password.

For more information about accessing and using the Virtual Terminal, refer to Virtual Terminals on page 37.

Media Gateways

To access Media Gateways in Element Manager click **Media Gateways** in the **IP Network** branch of Element Manager navigator. The Media Gateways Web page appears, as shown in Figure 79: Media Gateways Web Page on page 149.

Element Manager displays Media Gateway type as MGC for a Media Gateway Controller and MGX for an MG XPEC Media Gateway Extended Peripheral Equipment Controller. The MG XPEC is used to convert a CS 1000M Intelligent Peripheral Equipment shelf (IPE) to a CS 1000E Media Gateway.

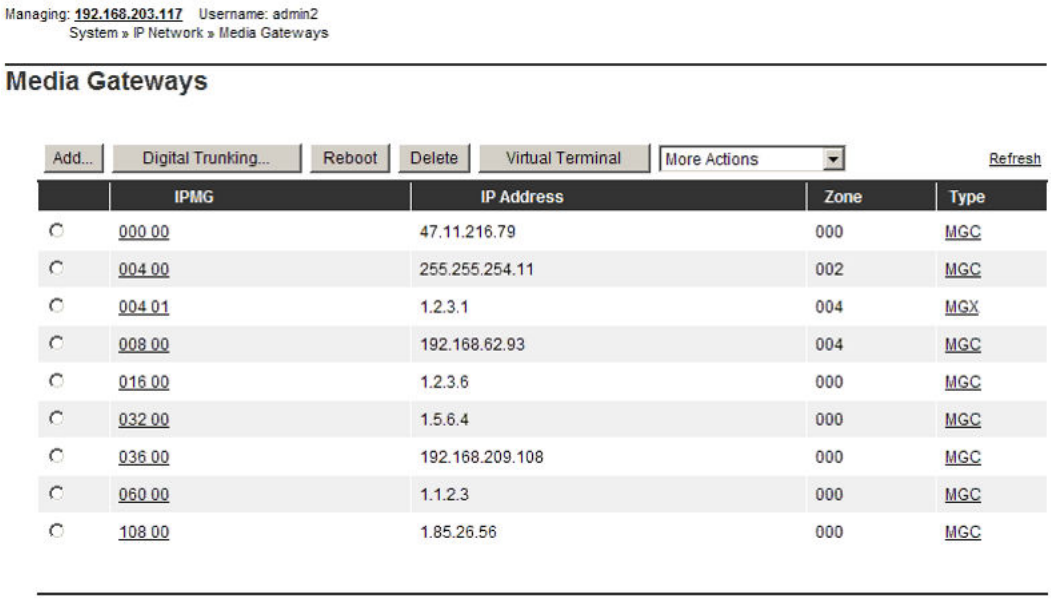


Figure 79: Media Gateways Web Page

IPMG Property Configuration

To configure the properties of an IPMG complete the following procedure.

Configuring IPMG properties

1. Select the **IPMG** from the list of IPMGs on the Media Gateways Web page. The IPMG Property Configuration Web page appears as shown in the following figure.

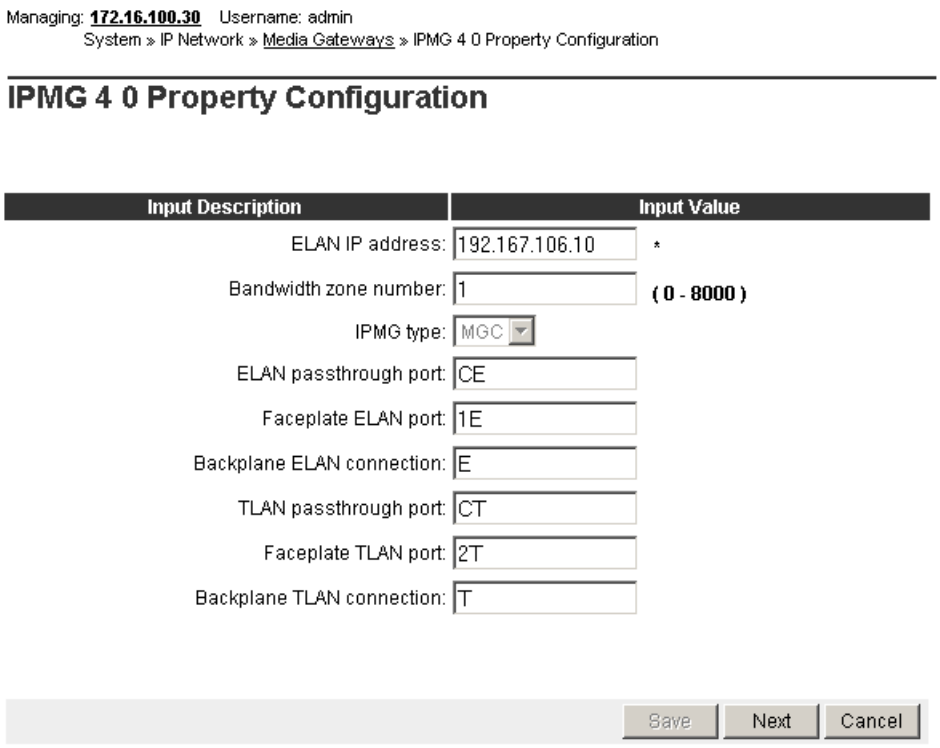


Figure 80: IPMG Property Configuration Web page

2. Enter the appropriate values.
3. Click **Next**
4. Continue as described in Media Gateway configuration on page 152

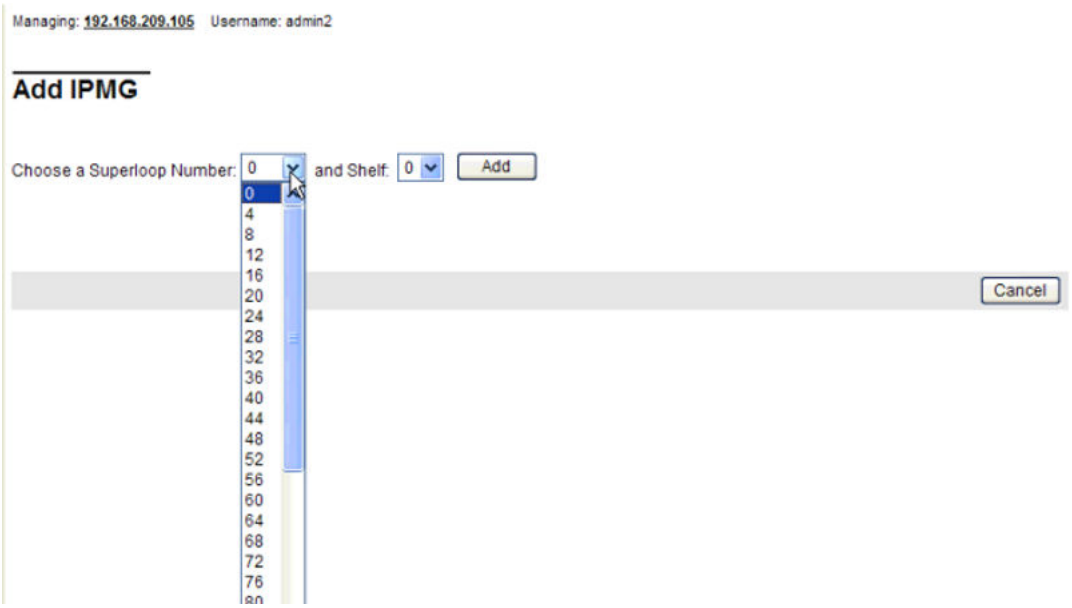
Adding an IPMG

Perform the following procedure to add an IPMG.

Adding an IPMG

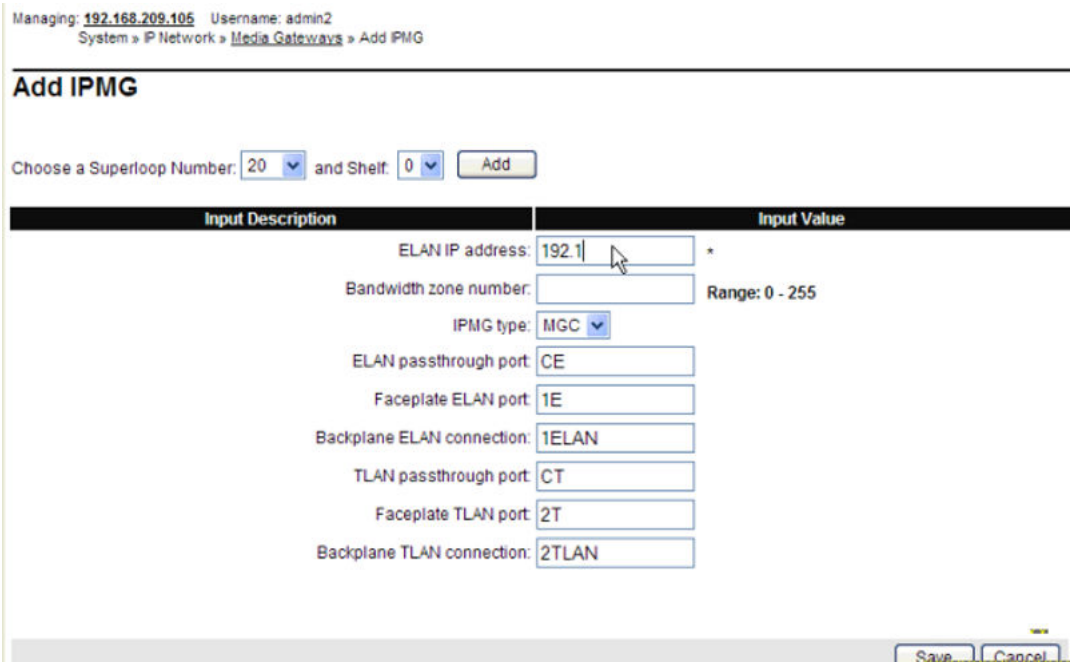
1. On the Media Gateways Web page, click **Add**.

The Add IPMG Web page appears.



2. Choose a number and required shelf from **Choose a Superloop Number** and **Shelf** lists.
3. Click **Add**.

   The Add IPMG with Input Description and Input Value fields Web page appears.



4. Enter the appropriate values in the fields and select the required IPMG type from the **IPMG type** list.

The available values are MGC, MGX, and MGS. For more details about the MGS configuration, see Media Gateway configuration on page 152.

5. Click **Save**.

Media Gateway configuration

To view or configure the current settings of a Media Gateway Controller, click **Media Gateways** in the **IP Network** branch of Element Manager navigator as shown in the following figure. For information about the configuration of the Media Gateway Controller, refer to *Avaya Communication Server 1000E Installation and Commissioning, NN43041-310*, *Avaya Communication Server 1000E - Upgrades, NN43041-458*, and *Avaya Communication Server 1000M and Meridian 1 Large System Installation and Commissioning, NN43021-310*.

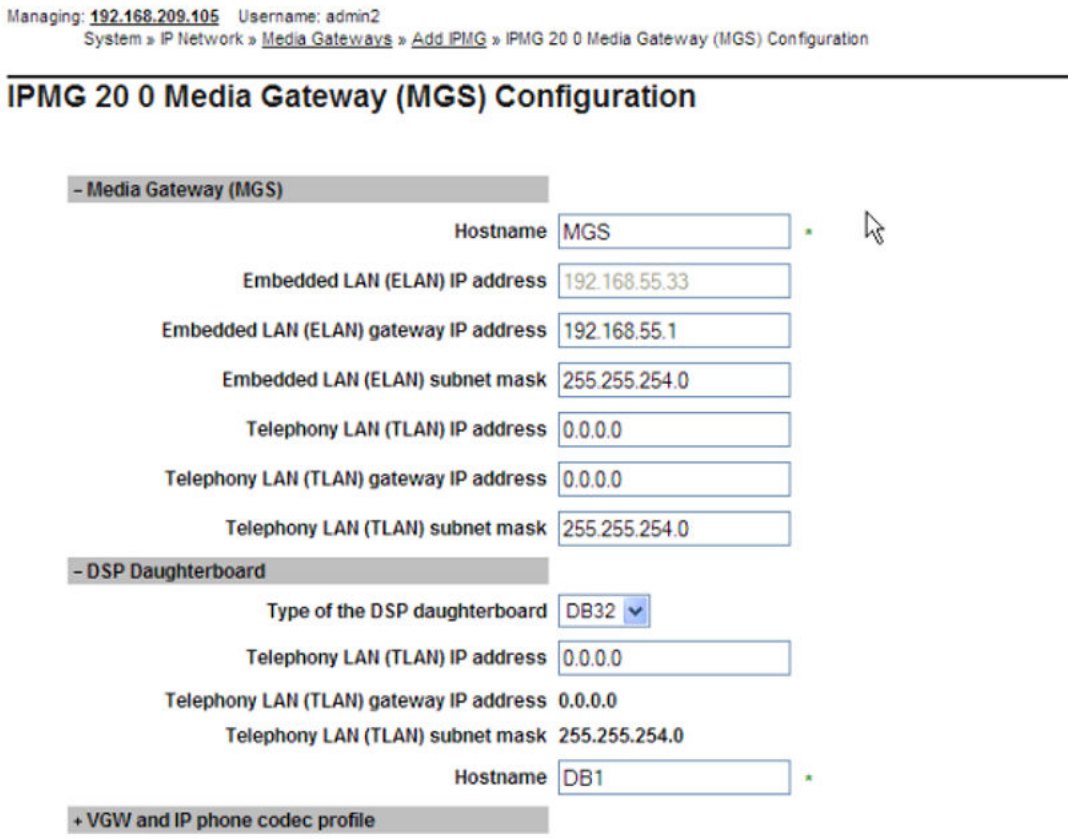


Figure 81: Media Gateway Configuration

Media Gateway Configuration has the option to enable or disable the R-factor option for the MGC card. R-factor is disabled by default as it has an impact on the density of DSP DB. When configuring DSPs on an MGC card, the values available in **Type of DSP daugtherboard** field are NODB, DB32, DB96, and DB128.

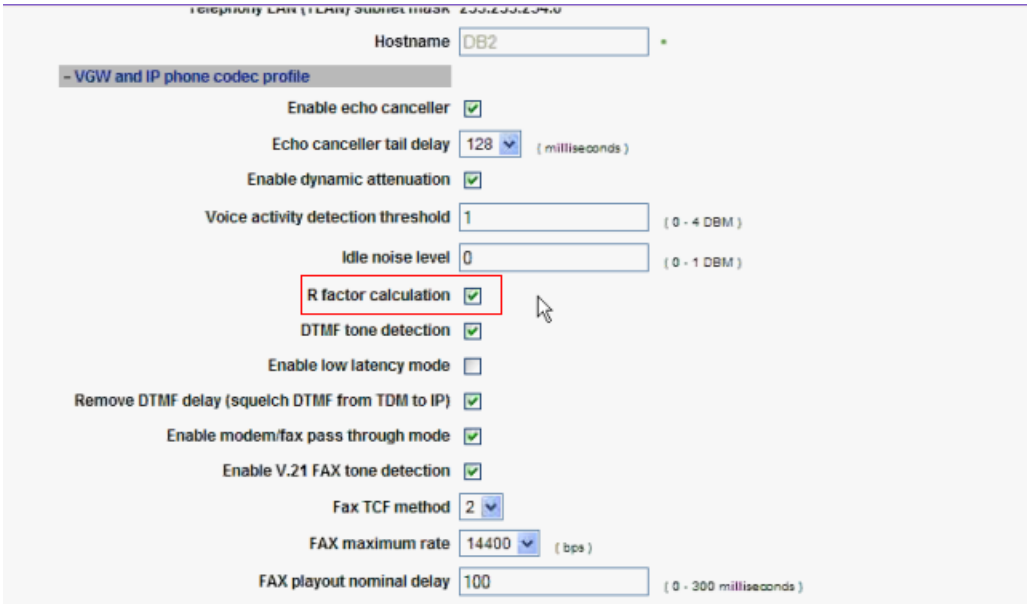


Figure 82: Media Gateway Configuration (continued)

Using the Media Based CLID you can enable or disable the Media based CLID for the Media Gateway Configuration.

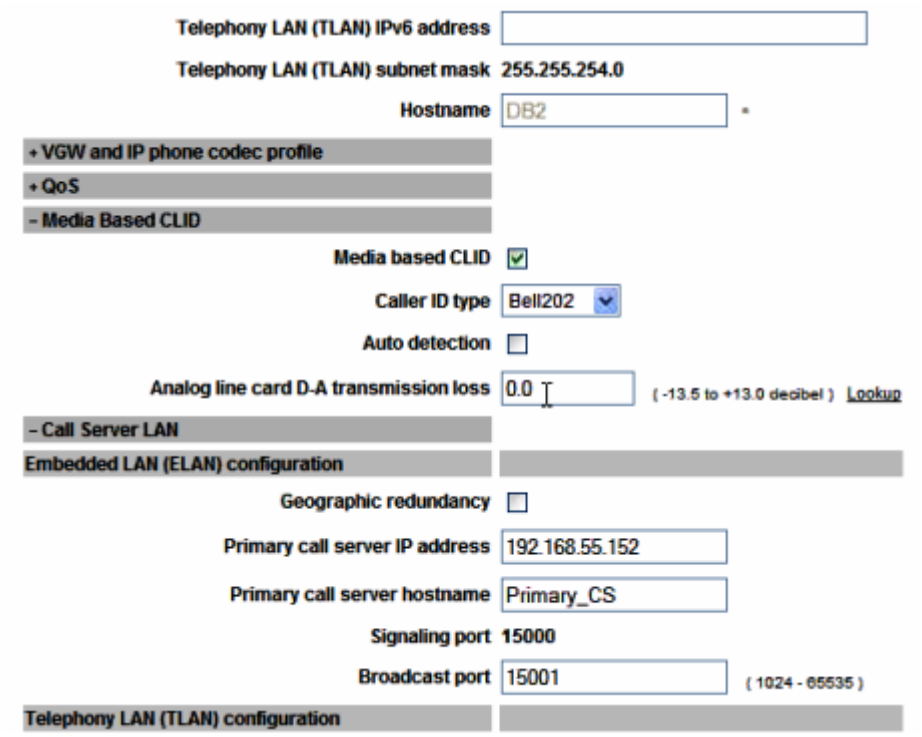


Figure 83: Media Gateway Configuration (continued1)

The **Caller ID Type** and **Auto detection** fields appear only if the **Media based CLID** check box is selected.

The **Caller ID Type** has two options, Bell202 and ETSIV.23. To configure these prompts, select Bell202 or ETSIV.23 prompts from the **Caller Type** list and click **Submit** .

When **Auto detection** check box is not selected, you must enter a value in the **Analog line card D-A transmission loss** field or click **Lookup** to select the Analog Line Card (ALC) type and the transmission loss value in decibels.

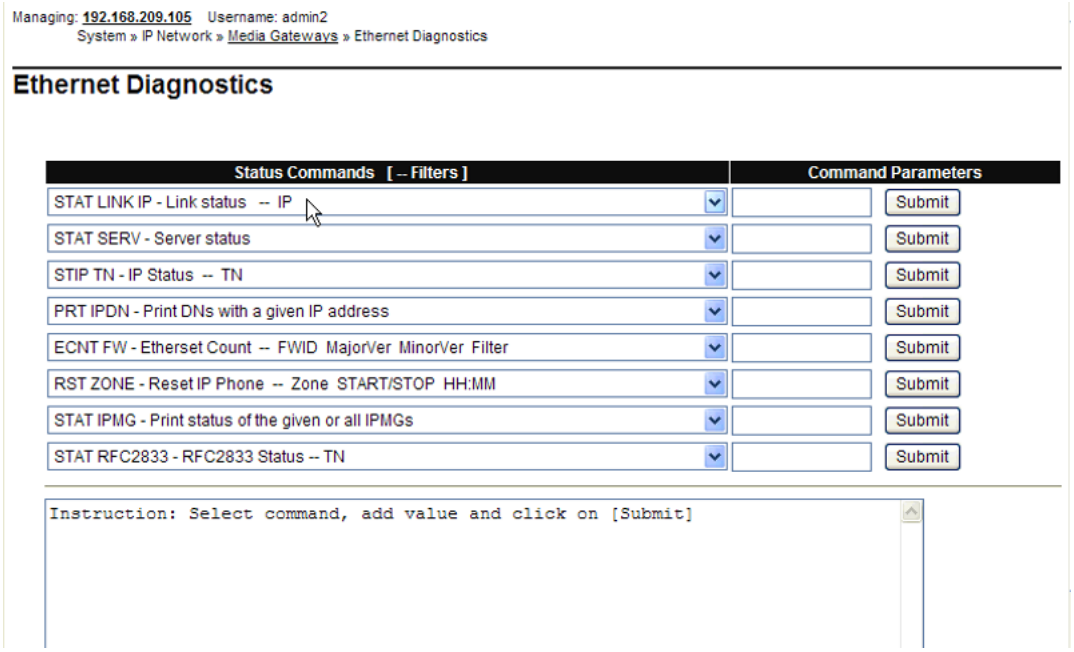
When you have finished entering the values, click **Save** .

Ethernet Diagnostics

To run the MGC Ethernet Diagnostic commands from Element Manager, select **Media Gateways** in the **IP Network** branch of Element Manager navigator. The Media Gateways Web page appears.

Running MGC Ethernet Diagnostics

1. Choose an MGC and select **Ethernet Diagnostics** from the **More Actions** list. The Ethernet Diagnostics Web page appears.



2. Select the MGC status command group that you want to access from the **Command** list.
3. Click **Submit** to execute the command.

Media Gateway Controller commands

Element Manager provides support for executing the Media Gateway Controller (MGC) command line interface (CLI) maintenance commands.

Note:

Not all MGC commands are supported from Element Manager as they affect basic system configuration parameters and are used by the system administrator to closely monitor the system using serial connection.

The following MGC CLI command groups are supported from Element Manager:

- General — General purpose commands
- System — MGC platform administration and maintenance commands
- Voice Gateway —- Voice Gateway application administration and maintenance commands
- Special — Special purpose PDT commands
- Security —- Intra-system and cryptographic key support commands

To run MGC commands from Element Manager, select the **Media Gateways** link in the **IP Network** branch of Element Manager navigator. The Media Gateways Web page appears.

Running MGC commands

1. Choose an MGC and select **General Commands** from the **More Actions** list.

   The General Commands Web page appears. See, Figure 84: General Commands on page 156.
2. Select the MGC CLI command group that you want to access from the **Group** list.
3. Choose a command from the **Command** list.
4. Click **Run** .

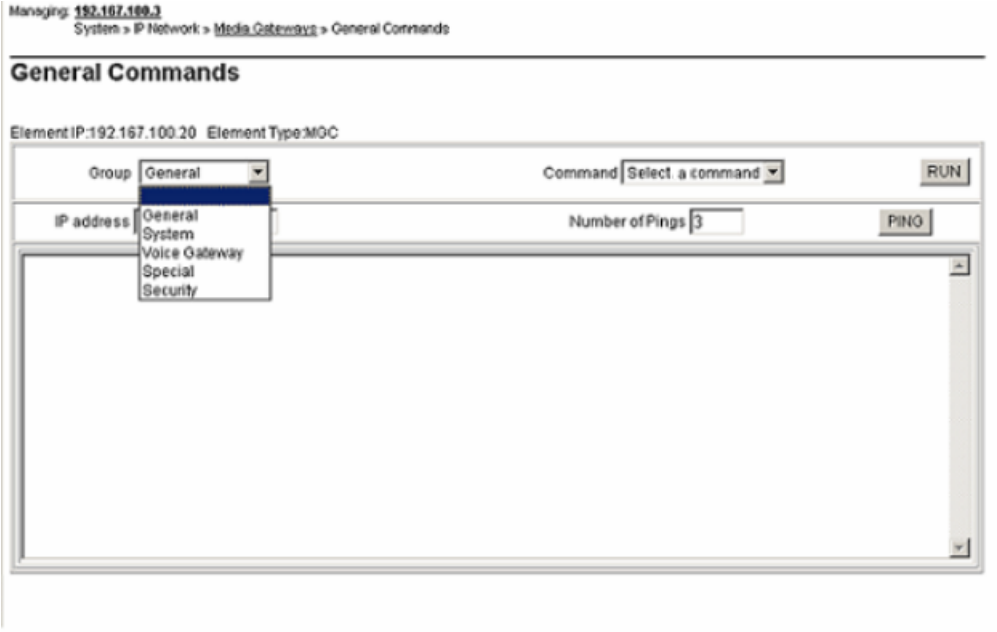


Figure 84: General Commands

For a list of available MGC commands that can be run using Element Manager, refer to *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

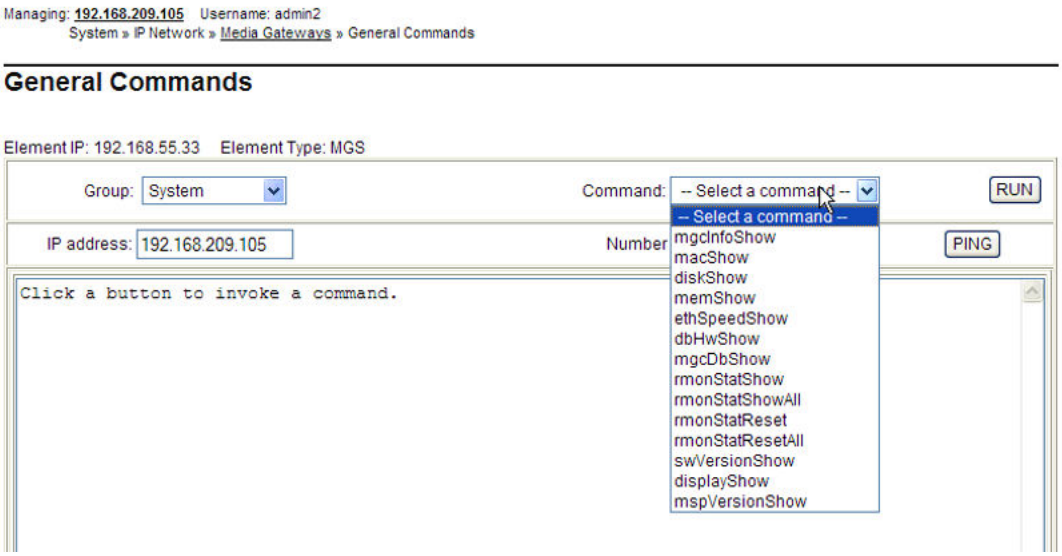
General purpose commands

The following General purpose commands are supported from Element Manager in General Commands Web page:

- hosts — Prints a list of all known hosts on the network
- version — Identifies the version

System platform administration and maintenance commands

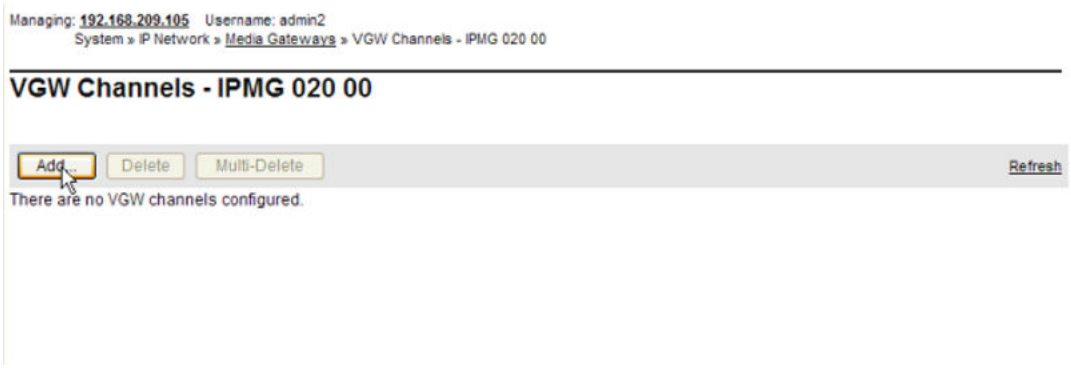
The following MGC platform administration and maintenance commands are supported from Element Manager under the System group in General Commands Web page.



- mgcInfoShow — Displays basic setup information
- macShow — Display MAC addresses
- diskShow — Display compact flash size
- memShow — Display memory usage
- ethSpeedShow — Show port speed and duplex setting
- dbHwShow — Display the model and revision numbers for installed DBs
- mgcDbShow — Display information about DSP DB
- rmonStatShow — Display RMON statistics for one port
- rmonStatShowAll — Display all RMON statistics
- rmonStatReset — Reset RMON statistics for one port
- rmonStatResetAll — Reset all RMON statistics
- swVersionShow — Show software version
- displayShow — Show the faceplate message
- mspVersionShow — Display MSP Device type, ARM code, Voice DSP Revision, and T.38 Version

Voice Gateway commands

The following Voice Gateway commands under the Voice Gateway group are supported from Element Manager in General Commands Web page.



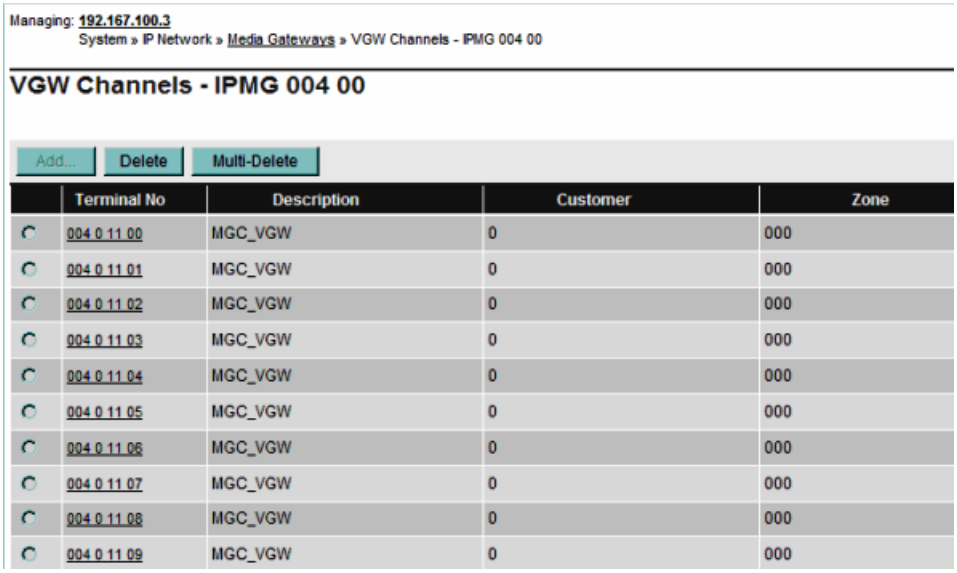
- dspNumShow — Displays the number of DSP channels for each DSP DB
- dspChanStateShow — Lists the state of all the channels on the DSP DBs
- dspHwCheck — Perform a basic DSP hardware diagnostic check
- dspLoopTest — Perform DSP loopback test for all inactive channels or for the channels entered
- vgwShow — Show information about busy gateway channels
- vgwCardShow — Show all channel's information for specified card
- vgwShowAll — Show information about all the gateway channels
- ommShow — Print the current OM data to the console

Adding VGW channels

To open the VGW channel from Element Manager, select the **Media Gateways** link in the **IP Network** branch of Element Manager navigator. The Media Gateways Web page appears.

1. Choose an IPMG and select **VGW Channels** from the **More Actions** drop-down list.

   The VGW Channels Web page appears.



2. Click **Add** to add a VGW channel.

   The Add VGW Channels Web page appears.

3. Select the number of required channels from the **Number of VGW Channels** drop-down list.
4. Enter the **Terminal Number** (the superloop and shelf numbers of the IPMG, the card number, and the unit).
5. Enter the appropriate values in all the fields and click **Save** .

   The VGW Channels IPMG Web page appears. The MGC has been added to the list.

Editing VGW channels

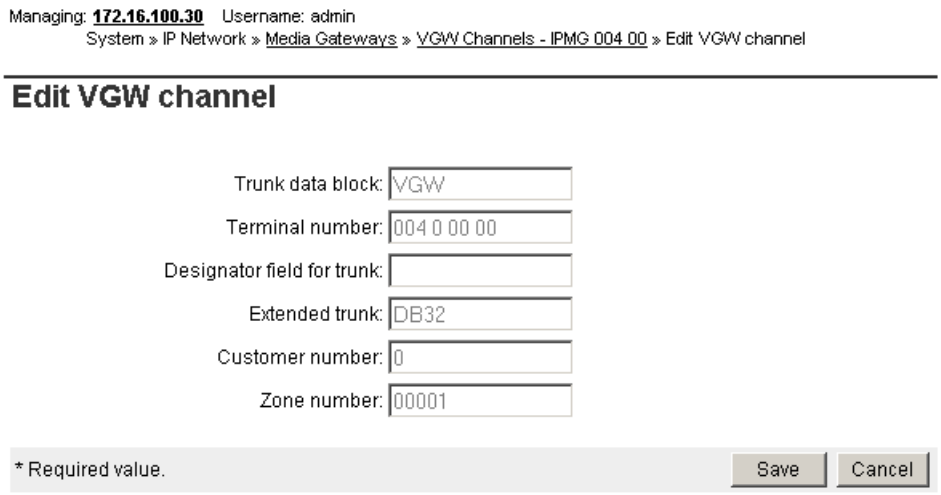
To open the VGW channel, select the **Media Gateways** link in the **IP Network** branch of Element Manager navigator. The Media Gateways Web page appears.

1. Choose an IPMG and select **VGW Channels** from the **More Actions** drop-down list.

   The VGW Channels Web page appears.

2. Select the **VGW channel** to edit from the list.

   The Edit VGW Channels Web page appears as shown in the figure below.



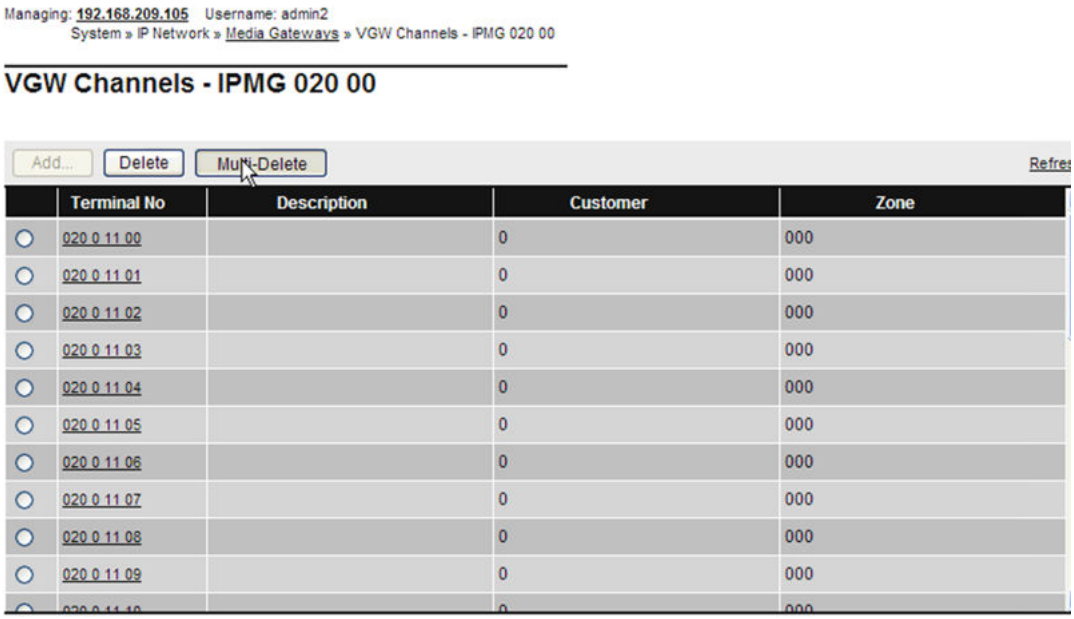
3. Make the necessary changes and click **Save** .

Deleting VGW channels

To open the VGW channel from Element Manager, select the **Media Gateways** link in the **IP Network** branch of Element Manager navigator. The Media Gateways Web page appears as shown in the following figure.

1. Choose an IPMG and select **VGW Channels** from the **More Actions** drop-down list.

   The VGW Channels Web page appears.



2. Select the number of required channels to delete from the list.
3. Click **Delete** to delete an VGW channel.

   or click **Multi-Delete** to delete multiple channels as shown in the preceding figure.

Digital Trunking for IPMG

Perform the following procedure for digital trunking in media gateways.

Configuring conference TDS

1. On the Element Manager page, select **IP Network, Media Gateways** .

   The Media Gateway Web page appears.

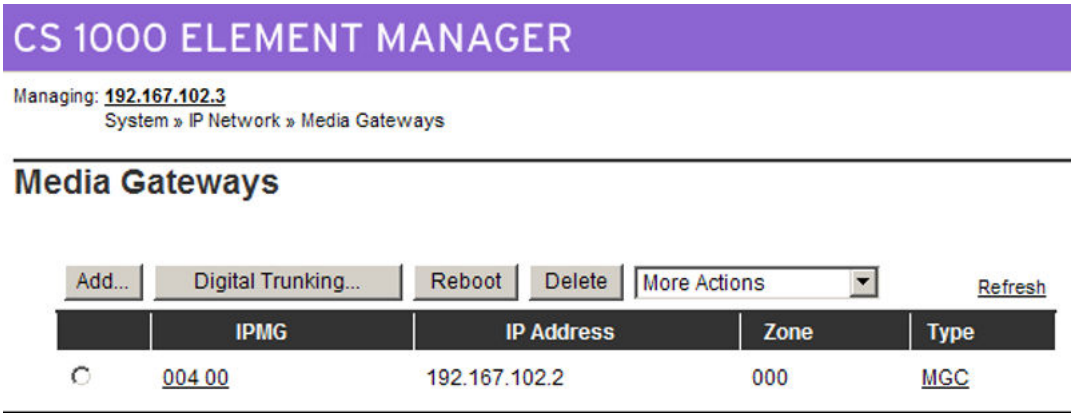


Figure 85: Media Gateways Web page

2. Select the IPMG superloop and click the **Digital Trunking** button.

   The Digital Trunking Web page appears as shown in the following figure.

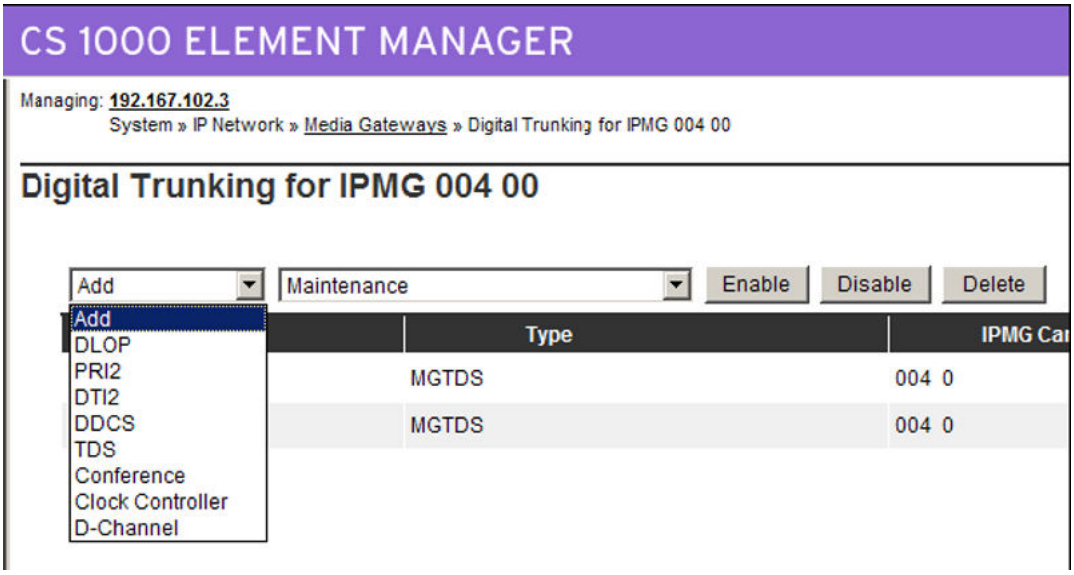


Figure 86: Digital Trunking for IPMG Web page

3. From the Add drop down menu, select DLOP to add a DLOP loop.

   The IPMG DLOP Web page appears as shown in the following figure.

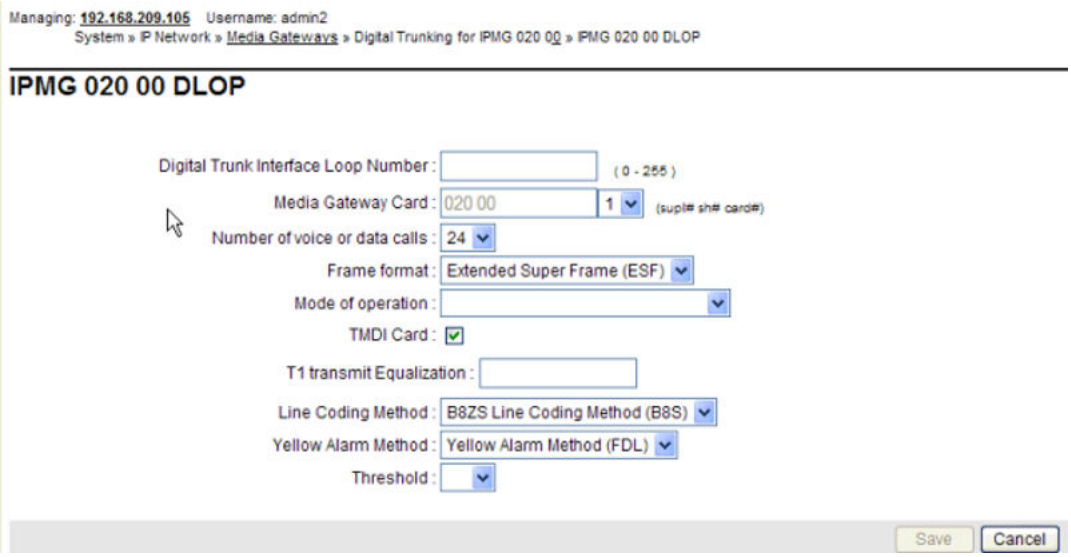


Figure 87: IPMG DLOP Web page

4. Type the **Digital Trunk Interface Loop Number** (0 — 255).
5. Enter appropriate values in all the fields.
6. Click **Save** .

   The Save button is not available until after you type a loop number and press TAB to move the cursor. A confirmation box appears.
7. Click **OK** to complete the configuration.
8. The updated loop configuration page appears and shows the new Conference loop.

Special purpose PDT commands

The following Special purpose PDT command is supported from Element Manager in the General Commands Web page:

- testAlarm — Test SNMP alarm

IP Security commands

The following Intra-system and cryptographic key support commands are supported from Element Manager under Security group in the General Commands Web page:

- disInsecureShells — Disables all insecure shells in the system
- disSecureShells — Disable all secure shells in the system
- enlInsecureShells — Enable all insecure shells in the system

- enlSecureShells — Enables all secure shells
- isecChgPsk — Change ISEC Psk locally
- isecChgLevel — Change ISEC security level locally
- isecNewTarget — Add a new target to the ISEC target list
- isecOutTarget — Delete a target from the ISEC target list
- isecEnlTarget — Enable the target ISEC
- isecDisTarget — Disable the target ISEC
- isecProfileShow — Show all ISEC profiles
- sshKeyActivate — Activate the SSH key
- sshKeyClear — Clears the SSH key
- sshKeyGenerate — Generate the SSH key
- sshKeyShow — Generate the SSH key
- statInsecureShells — Show whether insecure shell access is enabled or disabled
- statSecureShells — Show whether secure shell access is enabled or disabled

MGC Report logs

To generate MGC report logs from Element Manager, select the **Media Gateways** link in the **IP Network** branch of Element Manager navigator. The Media Gateways Web page appears. Choose an MGC and select **Report Log** from the **More Actions** drop-down list. The MGC Report Log Web page appears, as shown in Figure 88: MGC Report Logs Web page on page 165.

The following buttons at the top of this Web page provide one-click access to the following functions:

- **RDSCONVERT** — Convert a report log file to text
- **RDPREV** — Open the previous log file
- **RDNEXT** — Open the next log file
- **RDOPEN** — Open the latest report file
- **RDSHOW** — Show a summary of the report file
- **RDTAIL** — Show x records up to the newest record in the report file (where x is the configured display size).
- **RDHEAD** — Show x records starting from the oldest record in the report file (where x is the configured display size).

To view selected detail data on records in the report file, use the text boxes, the drop-down lists, and the following buttons:

- **RDGO** — Displays the record specified in the adjacent text box (where -1 is the oldest record and 1000 is the most recent).
- **RD** — Browses the report records. Enter the number of records to skip and the number of records to display in the adjacent text boxes.
- **RDS** — Browses the report records with (symbolic) memory dump. Enter the number of records to skip, and select the number of records to display using the adjacent text box and drop-down list.
- **VIEW** — Views selected records. Enter a starting record number and select the number of records to view using the adjacent text box and drop-down list. Negative numbers indicate records previous to the starting record.

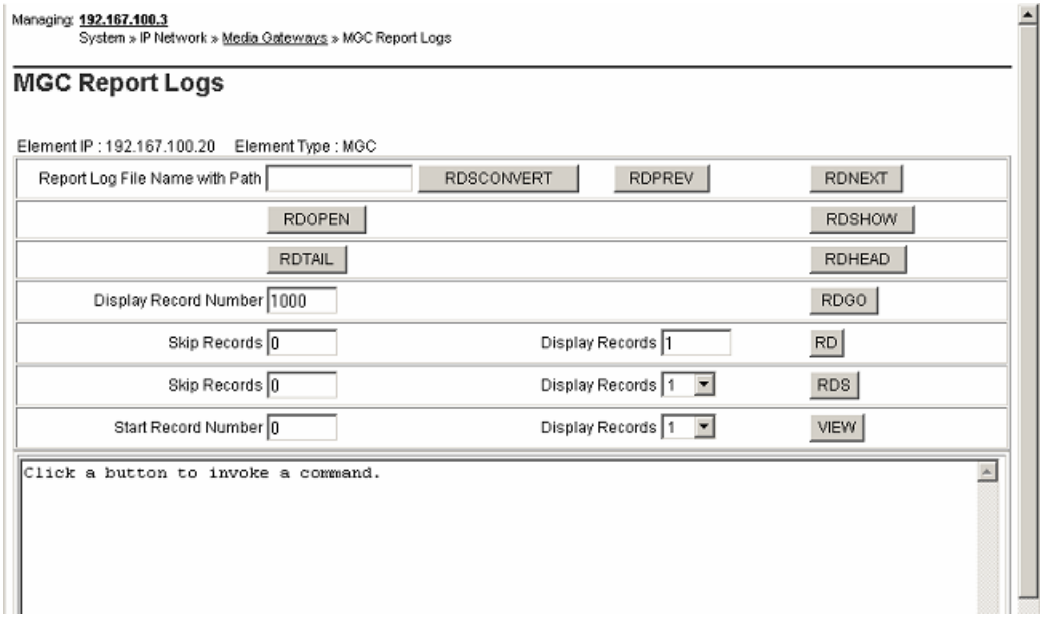


Figure 88: MGC Report Logs Web page

For more information about Media Gateway commands see, *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

32 Channel Secure Media Card (MC32S) commands

Element Manager provides support for executing MC32S command line interface (CLI) maintenance commands.

The following MC32S CLI command groups are supported from Element Manager:

- General — General purpose commands
- System — System commands

- Voice Gateway — Voice Gateway application administration and maintenance commands
- Special — Special purpose (PDT commands)
- Security — Intra-system and cryptographic key support commands

Note:

Not all MC32S commands are supported from Element Manager as they affect basic system configuration parameters and are used by the system administrator to closely monitor the system using serial connection.

To run MC32S commands from Element Manager, select the **Maintenance and Reports** link in the **IP Network** branch of Element Manager navigator. The Node Maintenance and Reports Web page appears. Click **GEN CMD** for the MC32S card from the list. The General Commands Web page appears for the MC32S card, as shown in Figure 89: MC32S General Commands Web page on page 166.

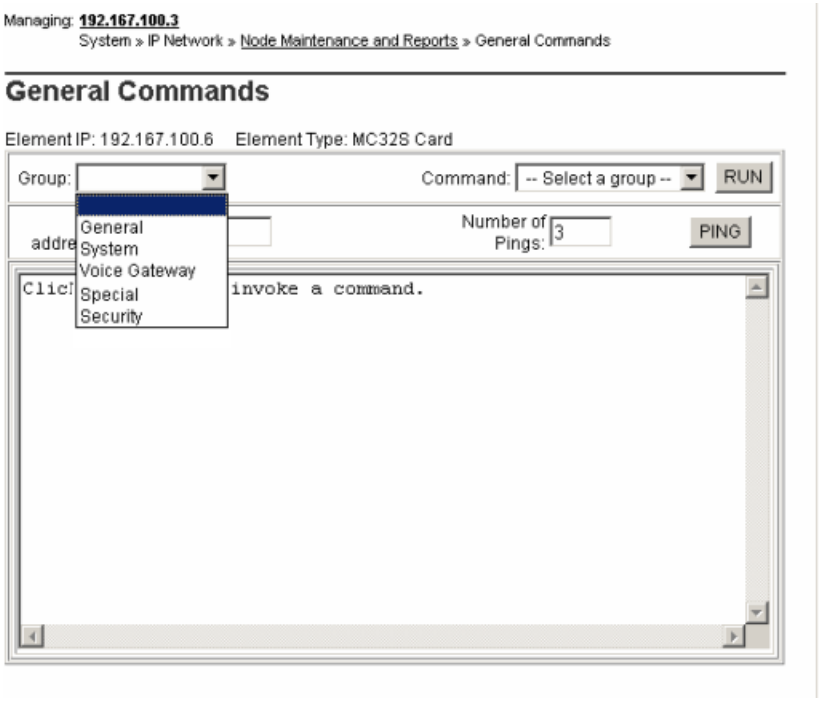


Figure 89: MC32S General Commands Web page

Running MC32S commands

1. Select the MC32S CLI command group that you want to access from the **Group** drop-down list.
2. Choose a command from the **Command** drop-down list.
3. Click **Run** .

For a list of available MC32S commands that can be run using Element Manager, refer to *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

General commands

The following MC32S General purpose commands are supported from Element Manager under **General** group on the General Commands Web page:

- hosts
- version
- ifShow

System commands

The following MC32S System commands are supported from Element Manager under System group in the General Commands Web page:

- mc32sInfoShow — Display basic setup information
- macShow — Display MAC Addresses
- diskShow — Display compact flash size
- memShow — Display memory usage
- ethSpeedShow — Show port speed and duplex setting
- dbHwshow — Display the model and revision numbers for installed DBs
- rmonStatShow — Display RMON statistics for one port
- rmonStatShowAll — Display all RMON statistics
- rmonStatReset — Reset RMON statistics for one port
- rmonStatResetAll — Reset all RMON statistics
- IPInfoShow — Display basic setup information
- logConsoleOn — Turn on logging to the console
- logConsoleOff — Turn off logging to the console
- logShow — Show information about the current logging configuration
- pbxLinkShow — Show PBX link status
- routeAdd — Add a route to the routing tables
- routeShow — Display host and network routing tables
- serialNumShow — Print out card serial number
- swVersionShow — Display software version
- setLeader — Set a leader card

- clearLeader — Clear the leader info in NVRAM
- disiAll — Graceful disable VGW
- enaAll — Enable VGW (opposite of disiAll)
- firmwareVersionShow — Prints out firmware version number
- itgAlarmTest — Generates ITGXXXX test alarms
- itgCardShow — Show card info
- itgMemShow — Show the memory usage
- displayShow — Show the faceplate message
- mspVersionShow — Display MSP Device type, ARM code, Voice DSP Revision, and T.38 Version

Voice Gateway commands

The following Voice Gateway commands under Voice Gateway group are supported from Element Manager in the General Commands Web page:

- dspNumShow — Displays the number of DSP channels for each DSP DB
- dspChanStateShow — Lists the state of all the channels on the DSP DBs
- dspHwCheck — Perform a basic DSP hardware diagnostic check
- dspLoopTest — Perform DSP loopback
- vgwCardShow — Show all channel's information for specified card
- vgwShow — Show information about busy gateway channels
- vgwShowAll — Show information about all the gateway channels
- numChannelsShow — Prints out number of available channels
- ommShow — Print the current OM data to the console
- resetOm — Reset the operational measurement file timer
- itgChanStateShow — Show State for channels, e.g. busy or idle

IP Security commands

The following Intra-system and cryptographic key support commands are supported from Element Manager under Security group in the General Commands Web page:

- disInsecureShells — Disables all insecure shells in the system
- disSecureShells — Disable all secure shells in the system

- enlInsecureShells — Enable all insecure shells in the system
- enlSecureShells — Enables all secure shells
- isecChgPsk — Change ISEC Psk locally
- isecChgLevel — Change ISEC security level locally
- isecNewTarget — Add a new target to the ISEC target list
- isecOutTarget — Delete a target from the ISEC target list
- isecEnlTarget — Enable the target ISEC
- isecDisTarget — Disable the target ISEC
- isecProfileShow — Show all ISEC profiles
- sshKeyActivate — Activate the SSH key
- sshKeyClear — Clears the SSH key
- sshKeyGenerate — Clears the SSH key
- sshKeyShow — Display the SSH key
- statInsecureShells — Show whether insecure shell access is enabled or disabled
- statSecureShells — Show whether secure shell access is enabled or disabled

Special Purpose PDT commands

The following Special purpose PDT command is supported from Element Manager under Special group in the General Commands Web page:

- testAlarm — Test SNMP alarm

Report logs

To generate MC32S report logs from Element Manager, select the **Maintenance and Reports** link in the **IP Network** branch of Element Manager navigator. The Node Maintenance and Reports Web page appears. Choose an MC32S card and click **RPT Log** . The Node Report Logs Web page appears, as shown in Figure 90: MC32S Node Report Logs Web page on page 170.

The following buttons at the top of this Web page provide one-click access to the following functions:

- **RDSCONVERT** — Convert a report log file to text
- **RDPREV** — Open the previous log file
- **RDNEXT** — Open the next log file

- **RDOPEN** — Open the latest report file
- **RDSHOW** — Show a summary of the report file
- **RDTAIL** — Show x records up to the newest record in the report file (where x is the configured display size).
- **RDHEAD** — Show x records starting from the oldest record in the report file (where x is the configured display size).

To view selected detail data on records in the report file, use the text boxes, the drop-down lists, and the following buttons:

- **RDGO** — Displays the record specified in the adjacent text box (where -1 is the oldest record and 1000 is the most recent).
- **RD** — Browses the report records. Enter the number of records to skip and the number of records to display in the adjacent text boxes.
- **RDS** — Browses the report records with (symbolic) memory dump. Enter the number of records to skip, and select the number of records to display using the adjacent text box and drop-down list.
- **VIEW** — Views selected records. Enter a starting record number and select the number of records to view using the adjacent text box and drop-down list. Negative numbers indicate records previous to the starting record.

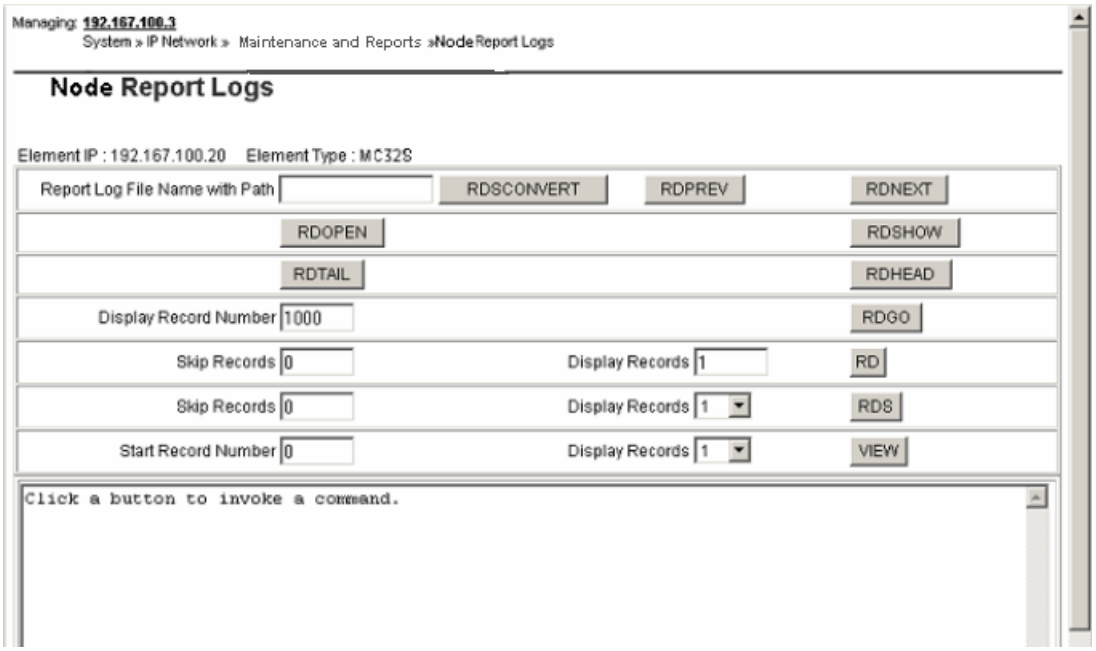


Figure 90: MC32S Node Report Logs Web page

For more information about MC32S commands see, *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

Zones

To configure or edit Bandwidth Zone information or Numbering Zone information, click the **Zones** link in the **IP Network** branch of the Element Manager navigator. The Zones Web page appears as shown in Figure 91: Zones Web page on page 171.

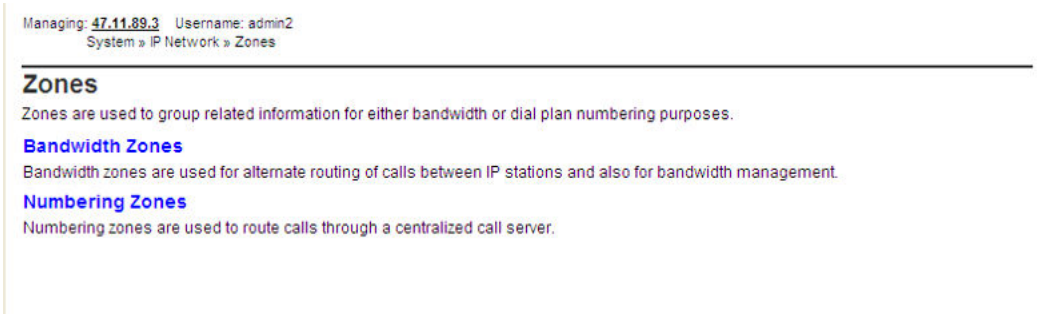


Figure 91: Zones Web page

Bandwidth Zones are used for alternate call routing between IP stations and for Bandwidth management. Numbering Zones are used to route calls through a centralized call server.

Note:

For High Scalability (HS) systems, after you use the Avaya CS 1000 Element Manager High Scalability (EM HS) interface to add zones, or to edit any of the values for Bandwidth Zones or Numbering Zones, on the reference High Availability (HA) group, the system updates the new values on all of the HA groups.

To view, configure, or edit Bandwidth Zones click on the **Bandwidth Zones** link on the Zones Web page. The Bandwidth Zones Web page appears as shown in the following figure.

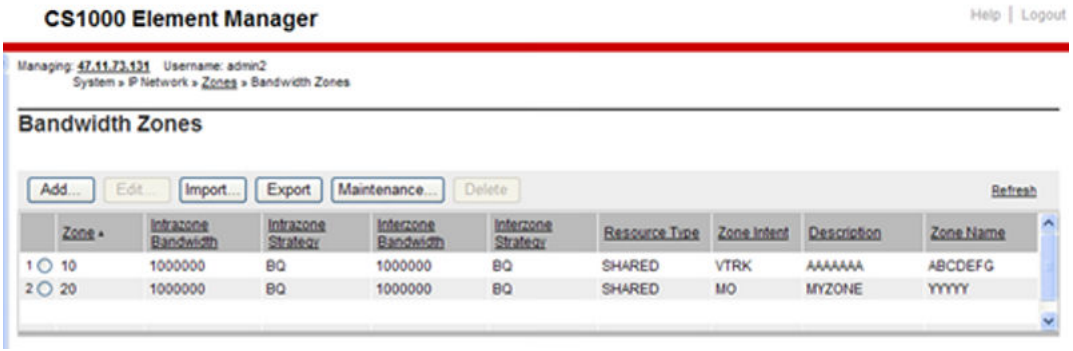


Figure 92: Bandwidth Zones

To add zones on the Zones Web page, click **Add**.

The Zone Basic Property and Bandwidth Management Web page appears. See Figure 93: Zone Basic Property and Bandwidth Management Web page on page 172.

⚠ Caution:

Beginning in Release 7.0, Adaptive Network Bandwidth Management provides bandwidth zone numbers in the range 0–8000. If you are interoperating with an earlier release you must use bandwidth zone numbers in the range 0–255; call processing issues occur if you use bandwidth zone numbers greater than 255.

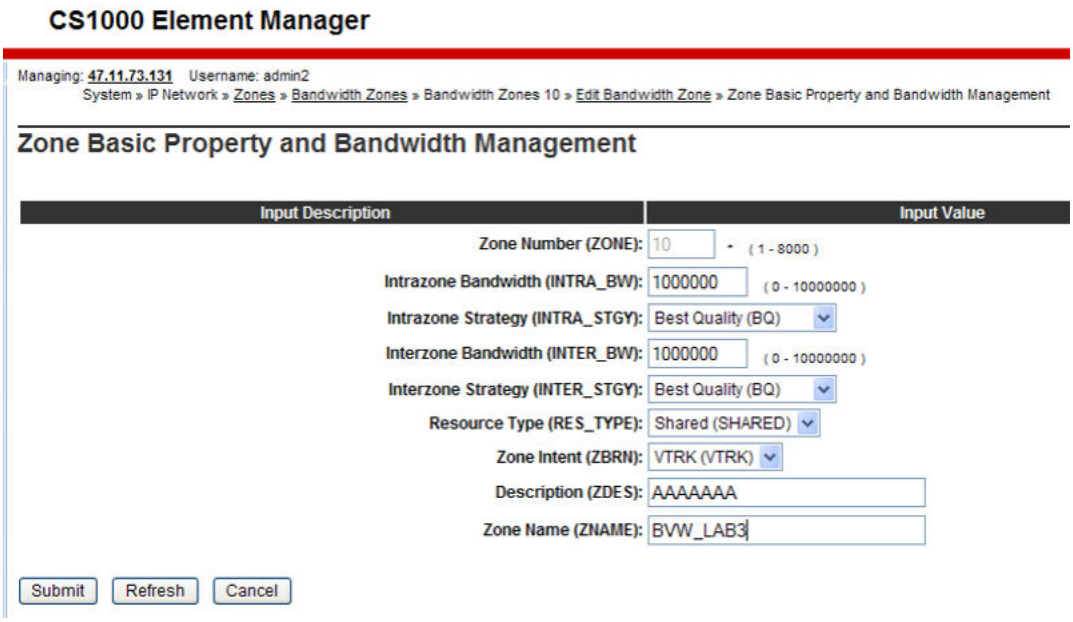


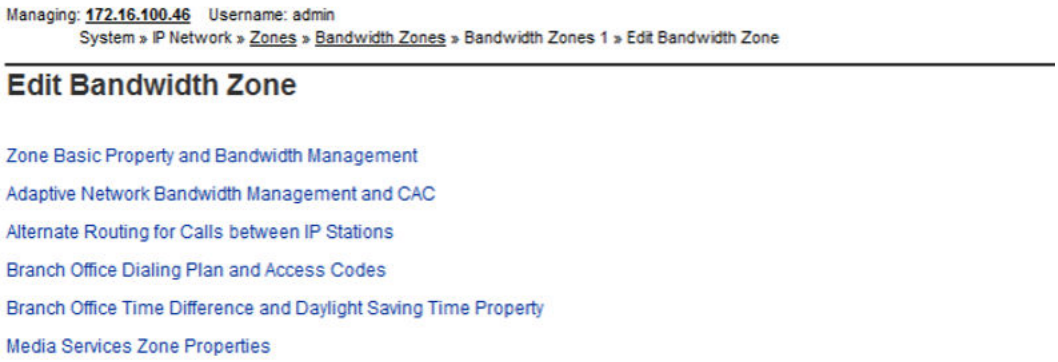
Figure 93: Zone Basic Property and Bandwidth Management Web page

The information entered on this Web page corresponds to the ZONE, ZBRN, and ZDES data traditionally configured using LD 117 - Ethernet and Alarm Management.

To save changes made in **Zone Basic Property and Bandwidth Management** parameters, click **Submit** at the bottom of the Web page.

To return to the Zones Web page, click the **Zones** link in the navigation path at the top of the Web page.

Click **Edit** in the Zones Web page. The Edit Bandwidth Zone web page appears.



This Web page contains links to the following six categories of Zone configuration data for each Zone configured.

- Basic Property and Bandwidth Management
- Adaptive Network Bandwidth Management and CAC
- Alternate Routing for Calls between IP Stations
- Branch Office Dialing Plan and Access Codes
- Branch Office Time Difference and Daylight Saving Time Property
- Media Services Zone properties

For information about configuring the MG 1000B, see *Avaya Branch Office Installation and Commissioning, NN43001-314*.

To configure the Adaptive Network Bandwidth Management feature, click the **Adaptive Network Bandwidth Management and CAC** link in the Edit Bandwidth Zone Web page. The Adaptive Network Bandwidth Management and CAC Web page appears, as shown in Figure 94: Adaptive Network Bandwidth Management and CAC Web page on page 174.

Note:

Do not configure ANBWM for Zone 0 or Virtual Trunk zones. ANBWM is not supported in Zone 0 or VTRK zone.

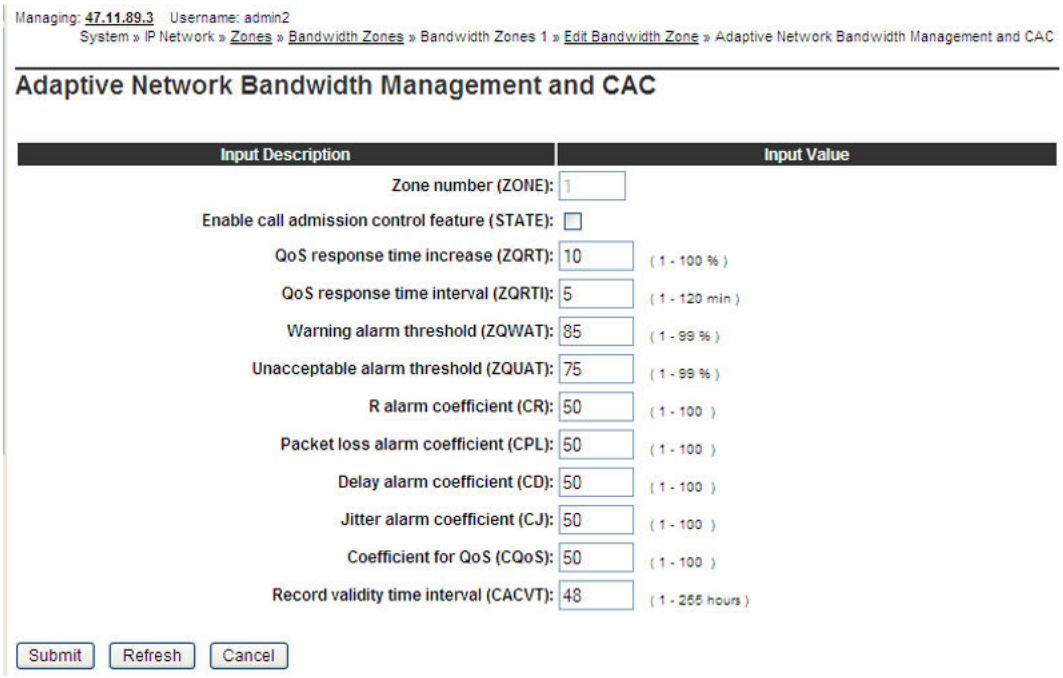


Figure 94: Adaptive Network Bandwidth Management and CAC Web page

If the Adaptive Network Bandwidth Management feature is enabled using the **Enable Call Admission Control Feature (STATE)** check box, then the other parameters can be adjusted as required:

- QoS Response Time Increase (ZQRT): Bandwidth limit increment, as a percentage of the QoS factor for the zone
- QoS Response Time Interval (ZQRTI): Time (in minutes) between bandwidth limit increments
- Warning Alarm Threshold (ZQWAT): A QoS value, which is lower than this value, but higher than the Critical (Unacceptable) Alarm Threshold, triggers a Major Alarm.
- Unacceptable Alarm Threshold (ZQUAT): A QoS value, which is lower than this value, triggers an Unacceptable (Critical) Alarm.
- R Alarm Coefficient (CR): Value used to calculate the QoS value for the zone.
- Packet Loss Alarm Coefficient (CPL): Value used to calculate the QoS value for the zone.
- Delay Alarm Coefficient (CD): Value used to calculate the QoS value for the zone.
- Jitter Alarm Coefficient (CJ): Value used to calculate the QoS value for the zone.
- Coefficient of QoS (CQoS): Value used to calculate the overall QoS value for the zone.
- Reord Validity Time Interval (CACVT): Amount of time (in hours) for zone-to-zone record validity. When this interval expires, records for unused zones are purged from the tables.

To configure the Alternate Routing feature, click the **Alternate Routing for Calls between IP Stations** link in the Edit Bandwidth Zone Web page. The Alternate Routing for Calls between

IP Stations Web page appears, as shown in Figure 95: Alternate Routing for Calls between IP Stations on page 175.

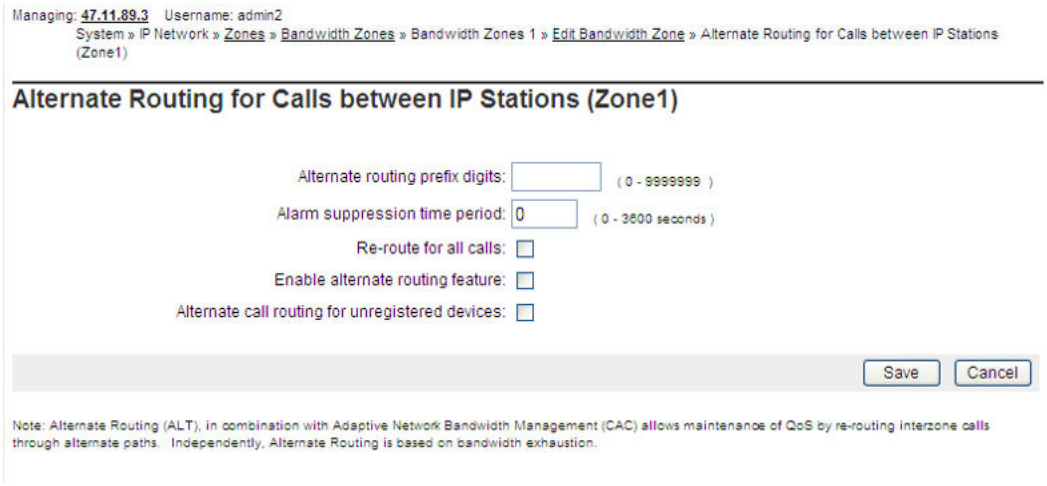


Figure 95: Alternate Routing for Calls between IP Stations

- Enter a maximum of 7 digits in **Alternate Routing Prefix Digits**.
- Enter an Alarm suppression time period.
- Select the **Re-route for All Calls** check box to enable the feature for all calls.
- Select the **Enable Alternate Routing feature** check box to enable the Alternative Call Routing for NBWM feature.
- Select the **Alternate call routing for unregistered devices** check box to enable the Alternative Call Routing for unregistered devices.
- Click **Save** to enter the data.

To edit dialing plan and access code parameters for a Zone's MG 1000B offices, click the **Branch Office Dialing Plan and Access Codes** link in the Edit Bandwidth Zones Web page. The Zone Dialing Plan and Access Codes Web page appears. See Figure 96: Zone Dialing Plan and Access Codes Web page on page 176.

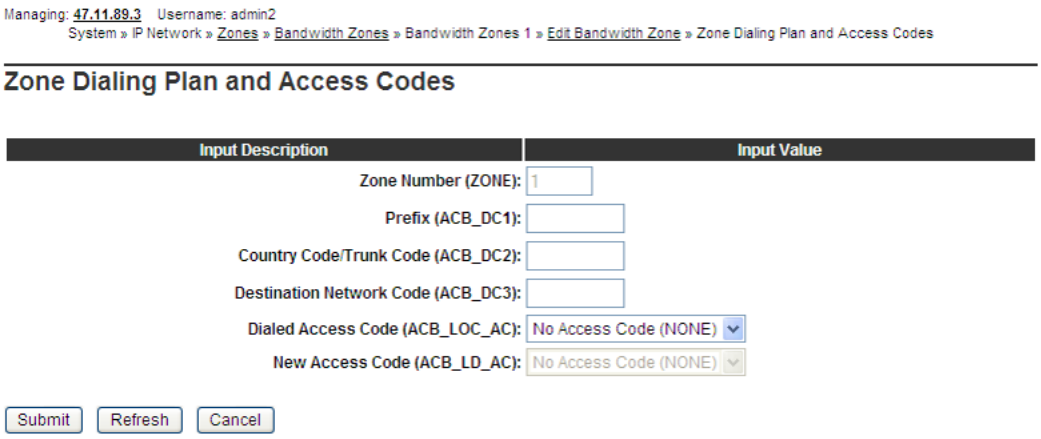


Figure 96: Zone Dialing Plan and Access Codes Web page

The information entered on this Web page corresponds to the Zone Dialing Plan and Access Codes (ZACB) command available in LD 117 - Ethernet and Alarm Management.

To save changes made in **Zone Dialing Plan and Access Code** parameters, click **Submit** at the bottom of the Web page.

To return to the Zones Web page, click the **Zones** link in the navigation path at the top of the page.

To access the time difference and daylight saving time properties for a Zone's MG 1000B Offices, click the **Branch Office Time Difference and Daylight Saving Time Property** link on the Edit Bandwidth Zones Web page. The Time Difference and Daylight Saving Time Property Web page appears (see Figure 97: Time Difference and Daylight Saving Time Property Web page on page 177).

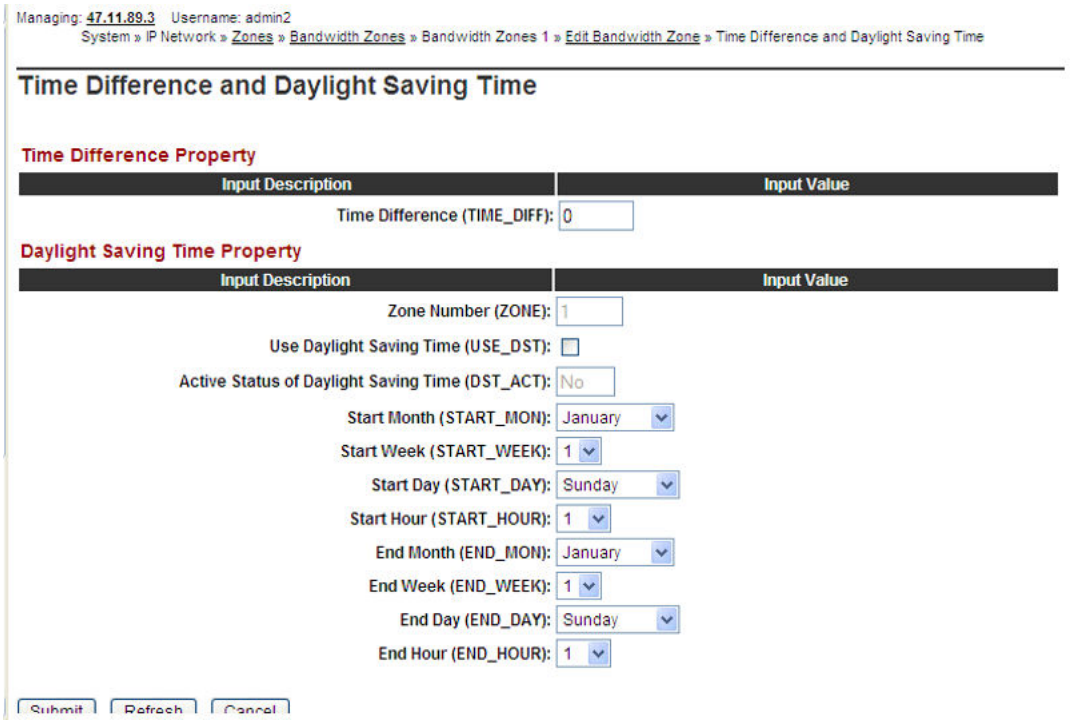


Figure 97: Time Difference and Daylight Saving Time Property Web page

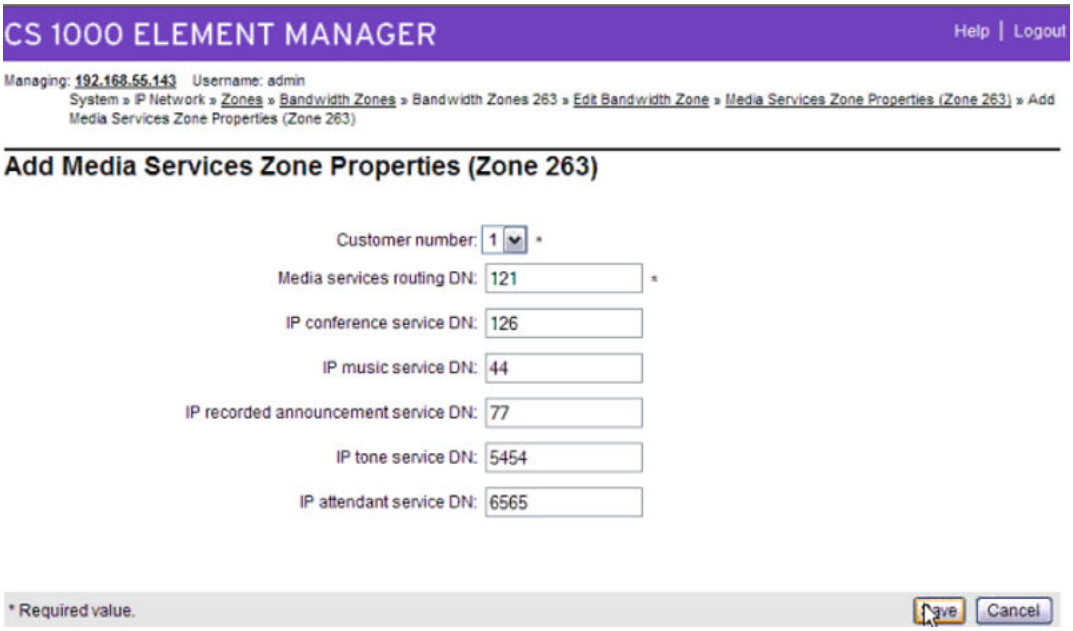
The information entered on this Web page corresponds to the ZTDF and ZDST command data traditionally configured using LD 117 - Ethernet and Alarm Management.

To save changes made in Time Difference and Daylight Saving Time properties, click **Submit** at the bottom of the Web page.

To return to the Zones Web page, click the **Zones** link in the navigation path at the top of the page.

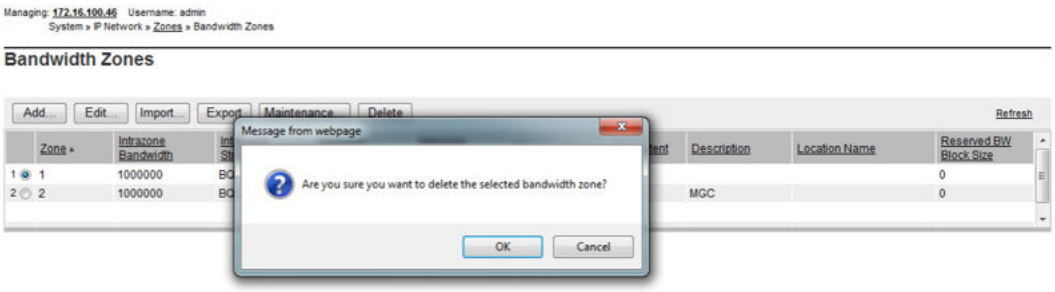
Click the **Media Services Zone Properties** link on the Edit Bandwidth Zone Web page. The Media Services Zone Properties Web page appears.

To add media services zone properties, click **Add** on the Media Services Zone Properties Web page. The Add Media Services Zone Properties Web page appears.

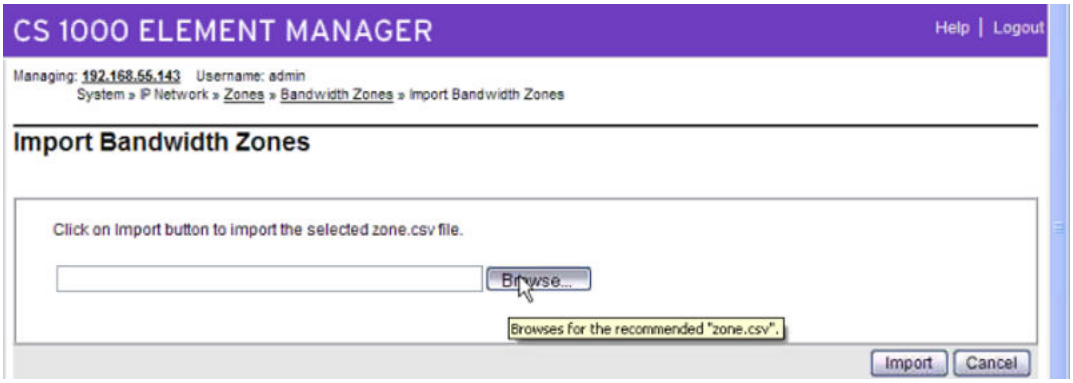


Enter all the fields and click **Save** to add the media services.

To delete any zone, select the zone in the Zones Web page and then click **Delete** in the Bandwidth zones Web page. The Message from web page dialog appears asking for the confirmation to delete. Click **OK**, to delete the selected bandwidth zone.



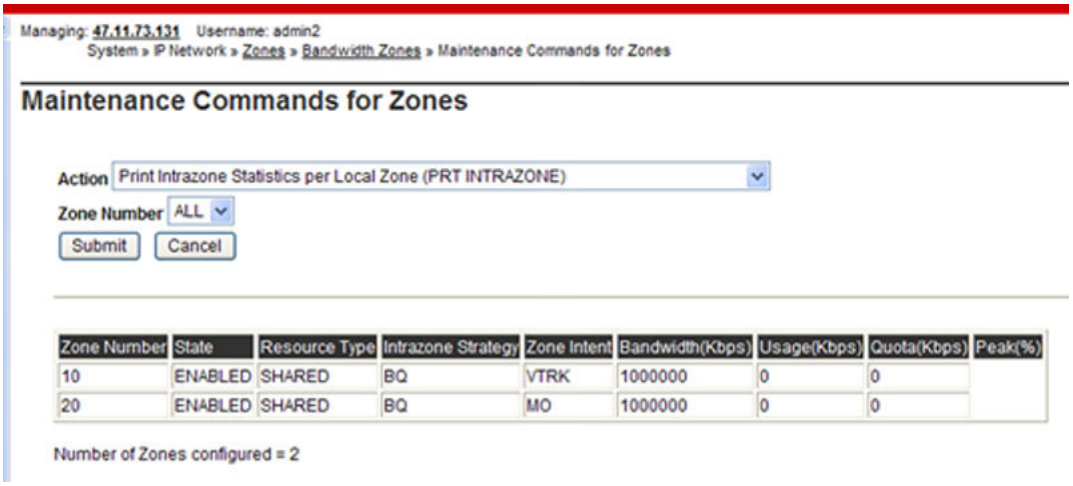
If you want to import any zone from the server, click **Import**. The Import Bandwidth Zones Web page appears.



Click **Browse** to search for the zone.csv file from the server desktop. Select the file and then click **Import** to import the bandwidth zone.

If you want to export any zone to your local server, select the required zone and click **Export**. The zone.csv file downloads.

To add the maintenance commands, click **Maintenance**. The Maintenance Commands for Zones Web page appears.



Select the required Action and Zone number from the drop-down lists and click **Submit**.

Numbering Zones

Numbering Zones provides you with an interface to configure various parameters for Zones-based Parameters, Flexible Dial Plan, and Direct Inward Dial number and provides an option for every customer to enable the Zone Based Dialing (ZBD) feature.

Element Manager provides the following capabilities to configure NUMZONE for the ZBD feature:

- adding a new Numbering Zone
- deleting a Numbering Zone

- editing the Zone Based Parameters
- flexible Dial Plan and Direct Inward Dial Number Configurations
- config.ini changes in Nodes page
- enabling Numbering Zones for every customer in Feature Options

To view, configure, or edit Numbering Zones click on the **Numbering Zones** link of Zones Web page. The Numbering Zones Web page appears as shown in the following figure.

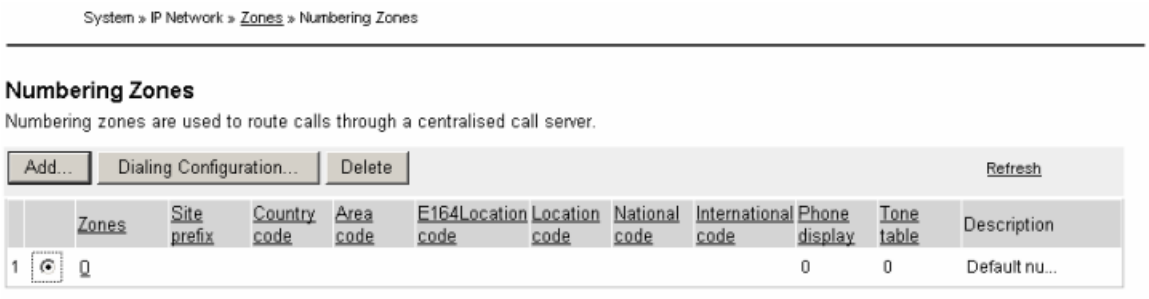


Figure 98: Numbering Zones Web page

For information about configuring of ZBD in the IP Telephony Nodes Web page and configuration of a Numbering Zone, see *Avaya Dialing Plans Reference, NN43001-283*.

Host and Route Tables

Host and Route tables are located on the Ethernet LAN configuration page, that is used to configure and list the Ethernet LAN settings of the Call Server.

A host name can be up to 16 characters in length. The first character of a host name must be a letter of the alphabet. A character may be a letter or a number. A period is the delimiter between domain names. Spaces and tabs are not permitted. There is no distinction between upper and lower case.

To access the Host and Route Tables click **Host and Route Tables** link of the **IP Network** branch of the Element Manager navigator. The Host and Route Tables Web page appears as shown in the following figure.

For more information refer to *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

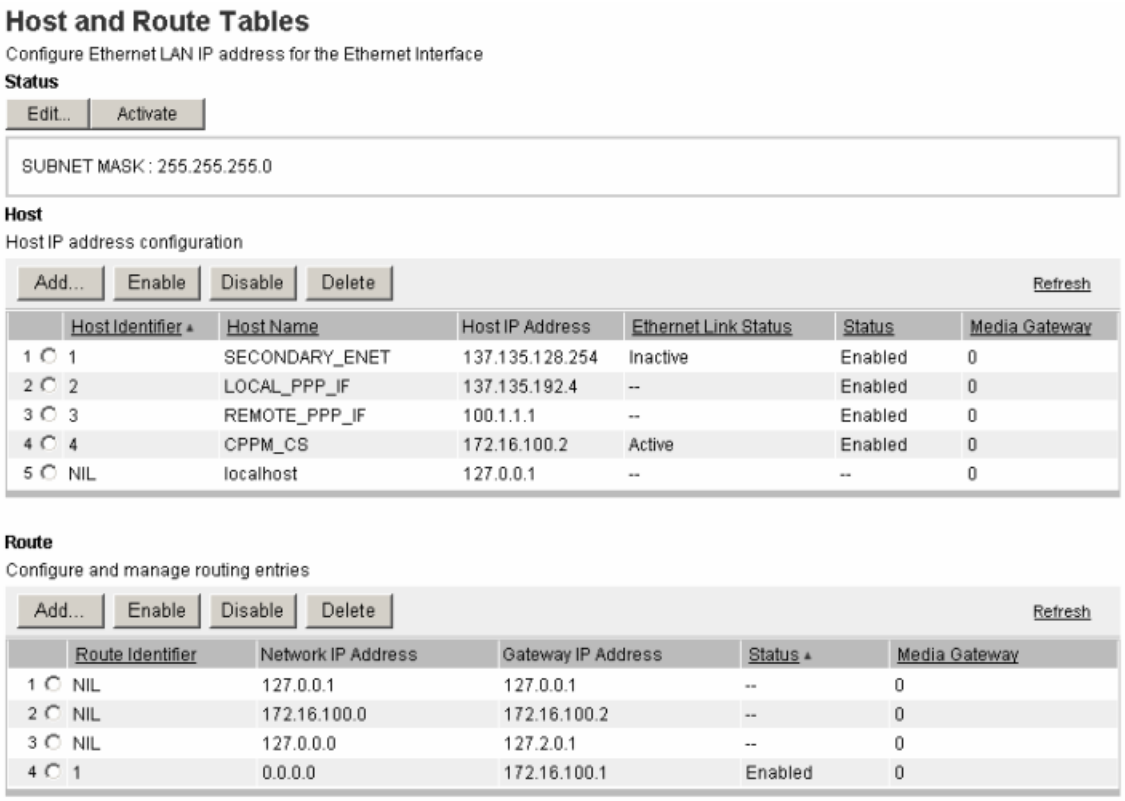


Figure 99: Host and Route Tables Web page

Network Address Translation (NAT)

To configure or edit Network Address Translation (NAT) information, click the **Network Address Translation** link in the **IP Network** branch of the Element Manager navigator. The Network Address Translation (NAT) Web page appears, as shown in Figure 100: Network Address Translation (NAT) Web page on page 182.

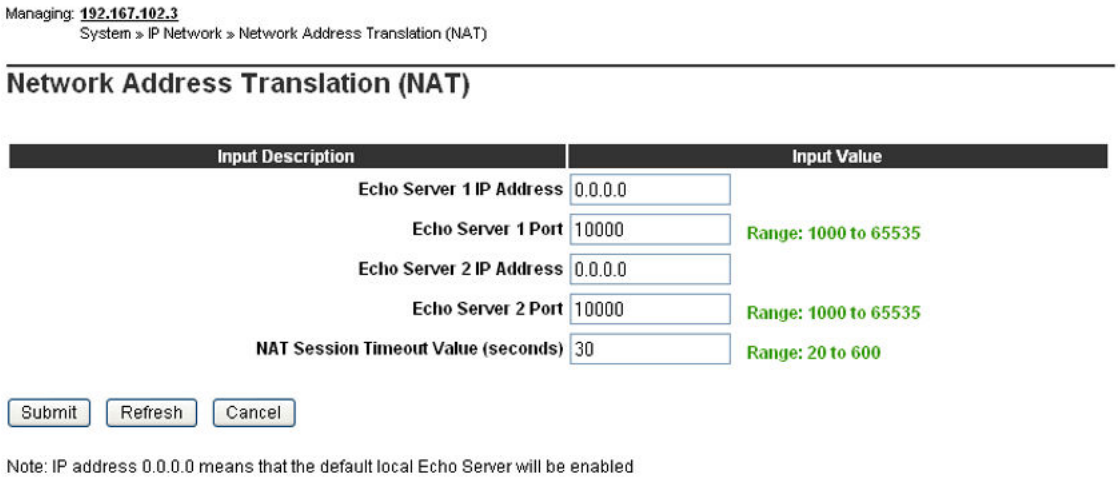


Figure 100: Network Address Translation (NAT) Web page

The information entered on this Web page corresponds to data traditionally configured using LD 117 - Ethernet and Alarm Management.

To configure the Echo Server 1 and 2 IP addresses and port numbers, type the values in the corresponding input fields.

Note:

Echo Server 1 and 2 default IP addresses use the TLAN network interface IP address of the LTPS card.

Enter the NAT session timeout value. Click the **Submit** button to save the changes. For more information, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

Quality of Service Thresholds (QoS)

The threshold values chosen provide accurate statistics without unnecessary network loading. If you increase your sample rate or your sample duration you will utilize/consume more of the bandwidth.

Avaya recommends that you use the default values. You can change thresholds depending on the voice quality level you want to have without alarms reported. For example, Call Packet Loss Unacceptable Threshold (UPKL) - default is 7 percent (entered as 70).

The zone basis threshold parameters allow for an overall level of alerts based on aggregated data for the zone. QoS samples are collected from active sets in the zone periodically by polling or received asynchronously, depending on the set firmware. The statistics received are compared to the call basis thresholds and violations are counted. The zone basis threshold parameters define the level at which alarms are sent out. These indicate the percentage of the samples that may exceed the defined per call thresholds for the different QoS metrics. For example, if the zone threshold for a particular metric is set to 2 percent, then zone alarms are issued if over 2 percent of the samples for that metric exceed the per call unacceptable threshold set for that metric.

The zone defaults for the warning items are higher than those for the unacceptable items (20 percent compared to 2 percent). The assumption is that the per call warnings thresholds are set at levels such that several warning alarms are normally issued. However, an overall problem with the zone should only be indicated if there are a significant number of such violations. On the other hand, there should be almost no unacceptable alarms and it is appropriate that these be set to a far lower zone percentage threshold.

The per call thresholds should be first adjusted to a level appropriate for the installation. After that the zone thresholds should be set, taking into consideration the per call threshold settings. If the per call thresholds are set low then more violations are to be expected, and the zone thresholds should be set higher to compensate. The converse is true for high per call threshold settings.

To configure or edit Quality of Service Threshold information, click the **Quality of Service Thresholds (QoS)** link in the **IP Network** branch of the Element Manager navigator. The Quality of Service (QoS) Thresholds Web page appears (see Figure 101: Quality of Service (QoS) Thresholds Web page on page 184).

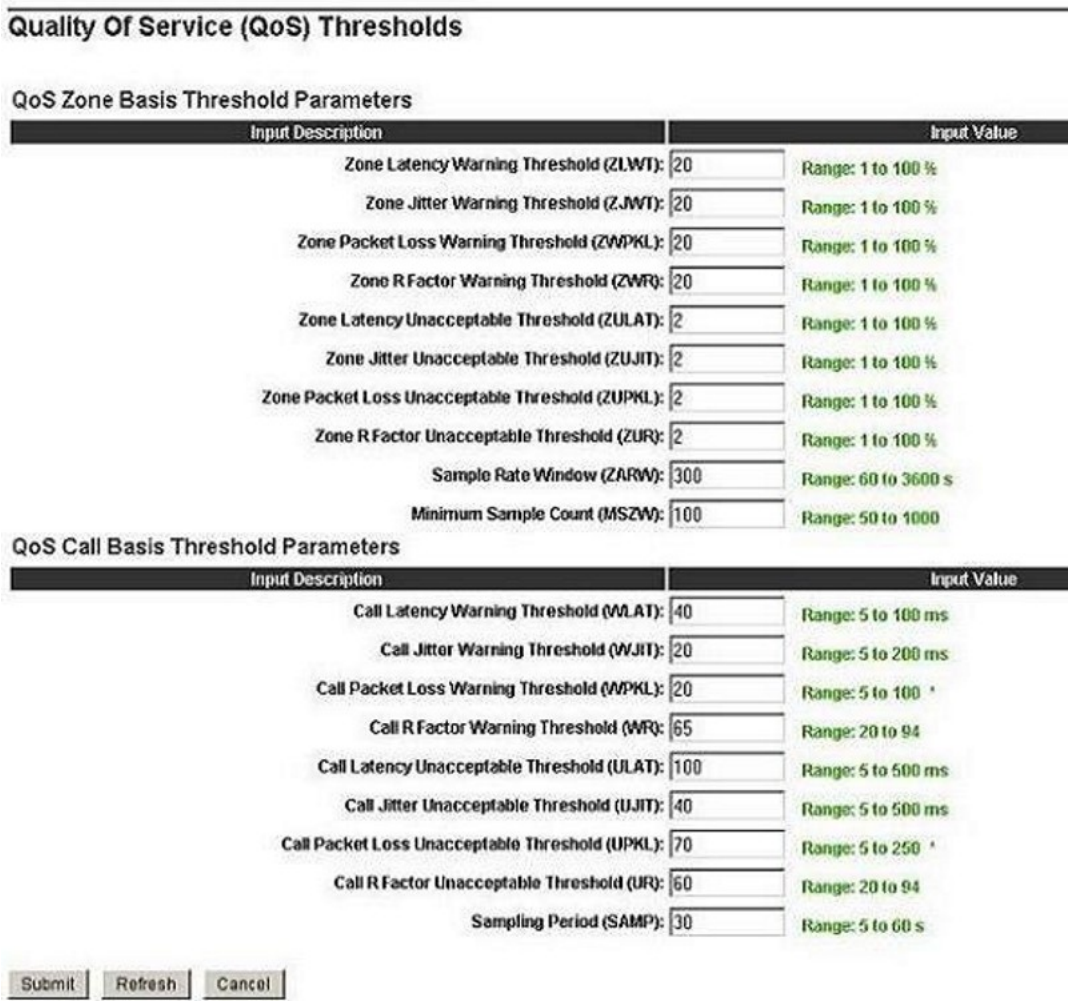


Figure 101: Quality of Service (QoS) Thresholds Web page

From this Web page, you can view or edit Quality of Service (QoS) Thresholds. Every node in the system has the same threshold values.

The information entered on this Web page corresponds to data traditionally configured using LD 117 - Ethernet and Alarm Management.

The threshold parameters are grouped as follows:

- **QoS Zone Basis Threshold Parameters**
- **QoS Call Basis Threshold Parameters**

To save changes made to the threshold parameters, click **Submit** at the bottom of the Web page.

For more information, see *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

Important:

Changes to Quality of Service parameters do not take effect until a Call Server data dump is performed.

Personal Directories

The Personal Directories Web page provides access to two links:

- **Server Configuration** : allows the administrator to enter the database backup and restore configuration details
- **User Profile Configuration** : allows the administrator to modify a user profile in the database

To access the Personal Directories Web page click the **IP Network > Personal Directories** link in the **System** branch of the Element Manager navigator.

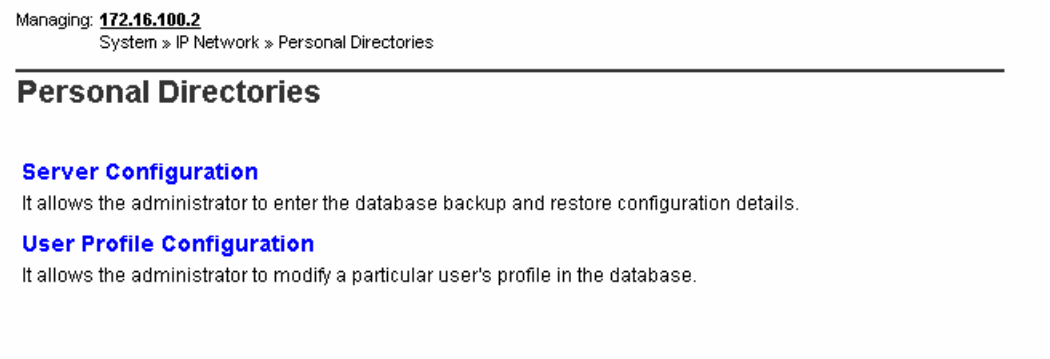
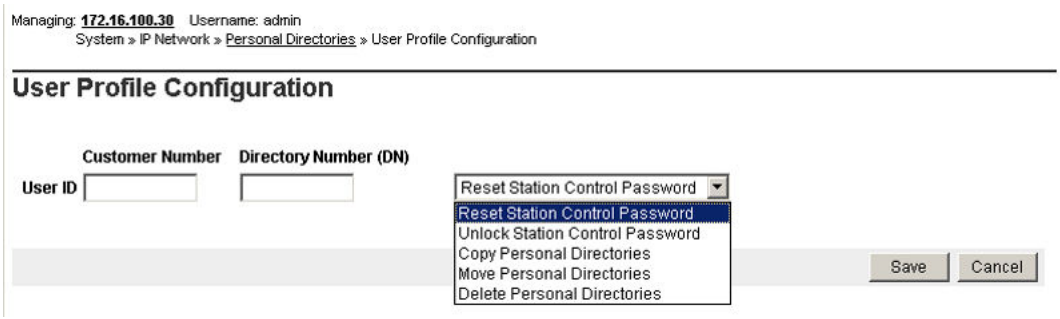


Figure 102: Personal Directories Web page

For more information about Personal Directories, Redial List, and Callers List, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

User Profile Configuration

To configure a particular user's profile in the database, click the **User Profile Configuration** link of the Personal Directories Web page. The User Profile Configuration Web page appears, as shown in the following figure.



You can perform the following:

- Reset Station Control Password
- Unlock Station Control Password
- Copy Personal Directories
- Move Personal Directories
- Delete Personal Directories

Resetting Station Control Password

1. To reset Station Control Password select **Reset Station Control Password** from the menu.
2. In the corresponding text boxes, type the **User ID** and **Directory Number**.
3. Click **Save** .

Unlocking Station Control Password

1. To unlock Station Control Password select **Unlock Station Control Password** from the menu.
2. In the corresponding text boxes, type the **User ID** and **Directory Number**.
3. Click **Save** .

Copying Personal Directories

1. To copy a personal directory, select **Copy Personal Directories** from the menu.
2. In the corresponding text boxes, type the **User ID** and **Directory Number** to copy.
3. In the corresponding text boxes, type the destination **User ID** and **Directory Number**.
4. Click **Save** .

Moving Personal Directories

1. To move a personal directory, select **Move Personal Directories** from the menu.
2. In the corresponding text boxes, type the **User ID** and **Directory Number** to move.

3. In the corresponding text boxes, type the destination **User ID** and **Directory Number**.
4. Click **Save** .

Deleting Personal Directories

1. To delete any or all of the following, select **Delete Personal Directories** :
   - Personal directory
   - Redial List
   - Callers List
   - User Preferences
2. In the corresponding text boxes, type the **User ID** and **Directory Number** to delete.
3. Select the items to delete.
4. Click **Save** .

Unicode Name Directory

The Unicode Name Directory feature enables the display of called or caller party name in Unicode format and use languages other than English for name display. It enhances the functionality of Unicode display capable Unistim terminals

The Unicode Name Directory System Management Solution (SMS) provides a solution to provision localized names (up to seven different languages) on subscriber base and generate subscriber telephony account's calling line IDs/URIs (CLID/URI) in network level to serve Unicode Name Directory server.

To successfully configure Unicode Name Directory on the Call Server side, enable the Name Directory Application and configure Lightweight Directory Access Protocol (LDAP) synchronization parameters. Name Directory Application is enabled in the Call Server only if Personal Directory Application Server is configured.

Management of Unicode Name Directory is an integral part of Subscriber Manager, for more information on Unicode Name Directory and the role of Subscriber Manager refer to *Avaya Subscriber Manager Fundamentals, NN43001-120*.

For information about Unicode Name Directory and its configuration, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

Interfaces

Element Manager supports the Value Added Server and Property Management System data blocks traditionally configured in LD 17.

Application Module Link

To access Application Module Link, click **Interfaces > Application Module Link** in the System branch of the Element Manager navigator. The Application Module Link Web page appears as shown below:

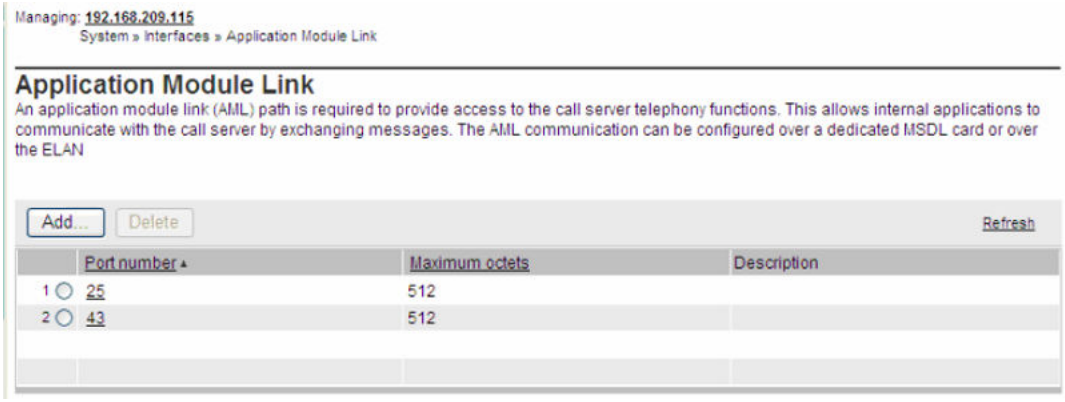


Figure 103: Application Module Link Web page

To view or edit an Application Module Link, click a port number. The Application Module Link Details Web page appears as shown below:

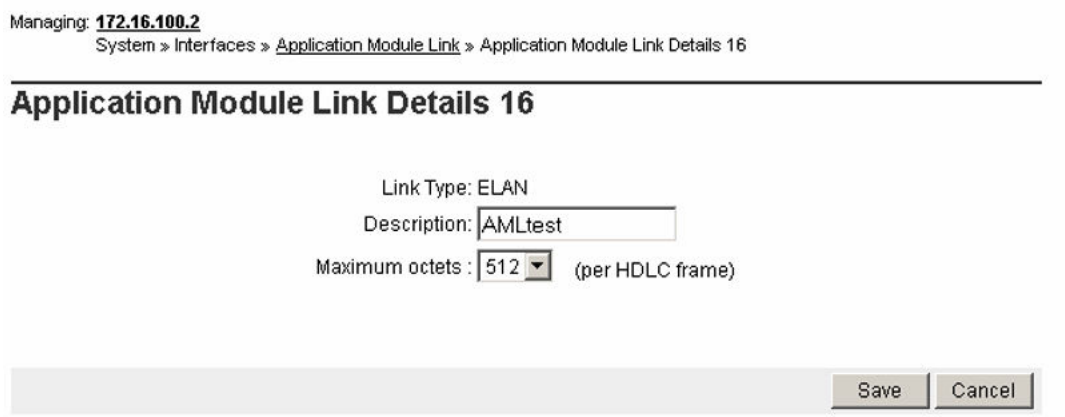


Figure 104: Application Module Link Details Web page

To edit the information, enter the appropriate values and click **Save**.

To Add a new Application Module Link click the **Add** button on the Application Module Link Web page. The New Application Module Link Web page appears as shown below:

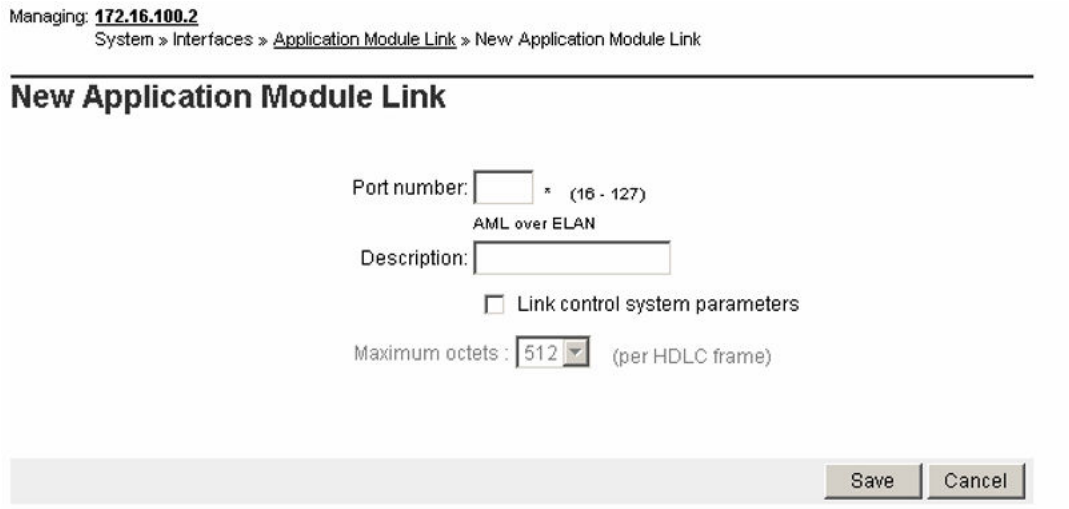


Figure 105: New Application Module Link Web page

To create a new Application Module Link, enter the appropriate information and click **Save**.

Value Added Server

Click the **Interfaces > Value Added Server** link in the **System** branch of the Element Manager navigator. The Value Added Server Web page appears as shown in Figure 106: Value Added Server Web page on page 190.

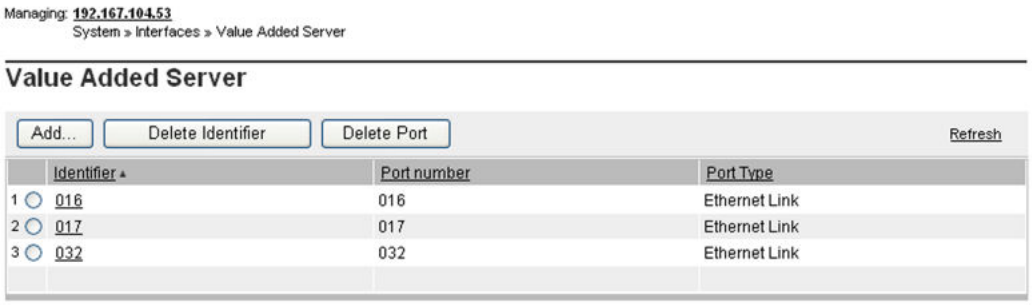


Figure 106: Value Added Server Web page

To add a Value Added Server, click **Add** . The Add Value Added Server Web page appears, as shown in Figure 107: Add Value Added Server Web page on page 190.

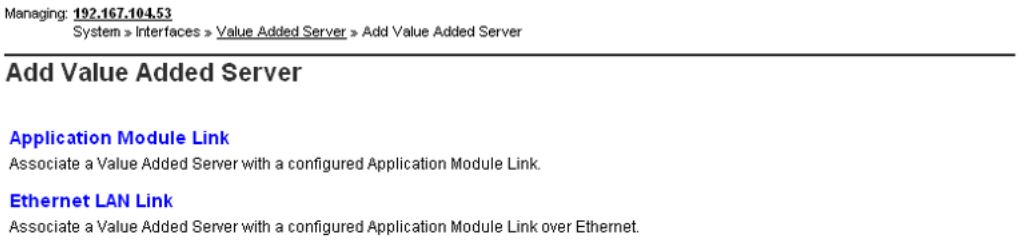


Figure 107: Add Value Added Server Web page

To associate a Value Added Server with a configured Application Module Link, click **Application Module Link** . The Application Module Link Web page appears, as shown in Figure 108: Application Module Link Web page on page 191.

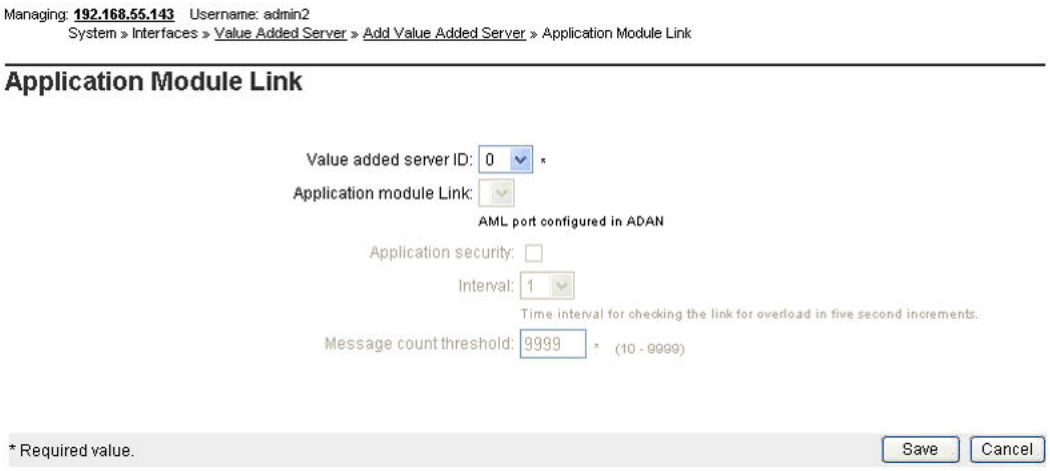


Figure 108: Application Module Link Web page

Enter the parameters for the new Value Added Server and click **Save** .

To associate a Value Added Server with a configured Application Module Link over Ethernet, on the Add Value Added Server Web page click **Ethernet LAN Link** . The Ethernet Link Web page appears, as shown in Figure 109: Ethernet Link Web page on page 191.

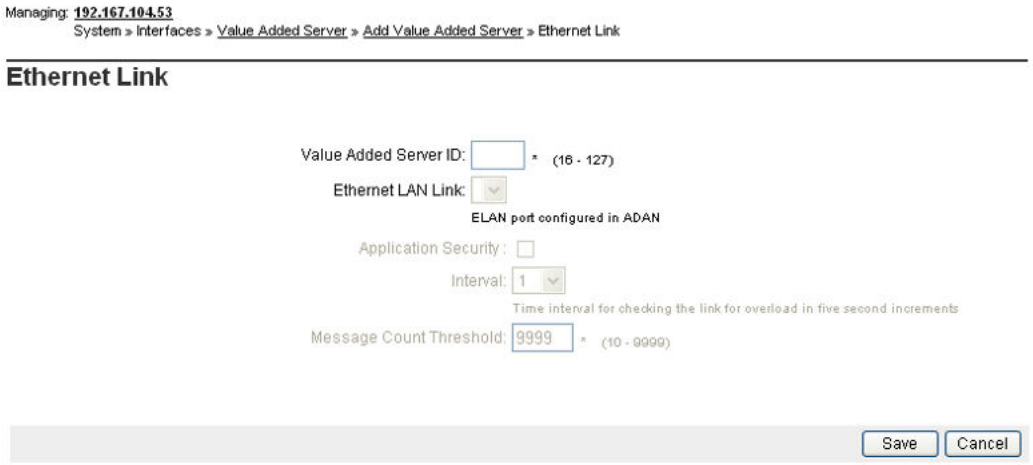


Figure 109: Ethernet Link Web page

Enter the parameters for the new Value Added Server and click **Save** .

Property Management System

Click the **Interfaces > Property Management System** link in the **System** branch of the Element Manager navigator. The Property Management System Web page appears, as shown in Figure 110: Property Management System Web page on page 192.

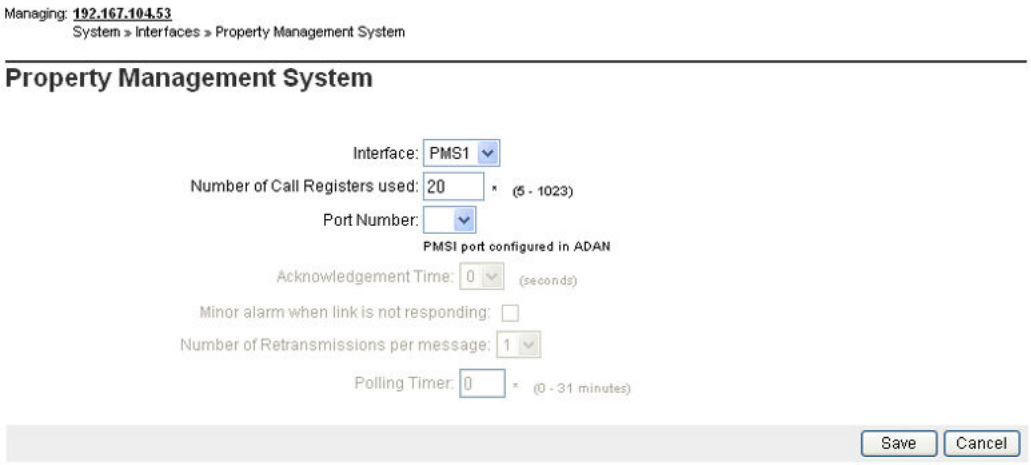


Figure 110: Property Management System Web page

Enter the parameters for the new Property Management System and click **Save** .

Engineered Values

The configuration of the system depends on the value of certain parameters. To configure and edit system parameters, click the **Engineered Values** link in the **System** branch of the Element Manager navigator. The Engineered Values Web page appears as shown in Figure 111: Engineered Values Web page on page 193.

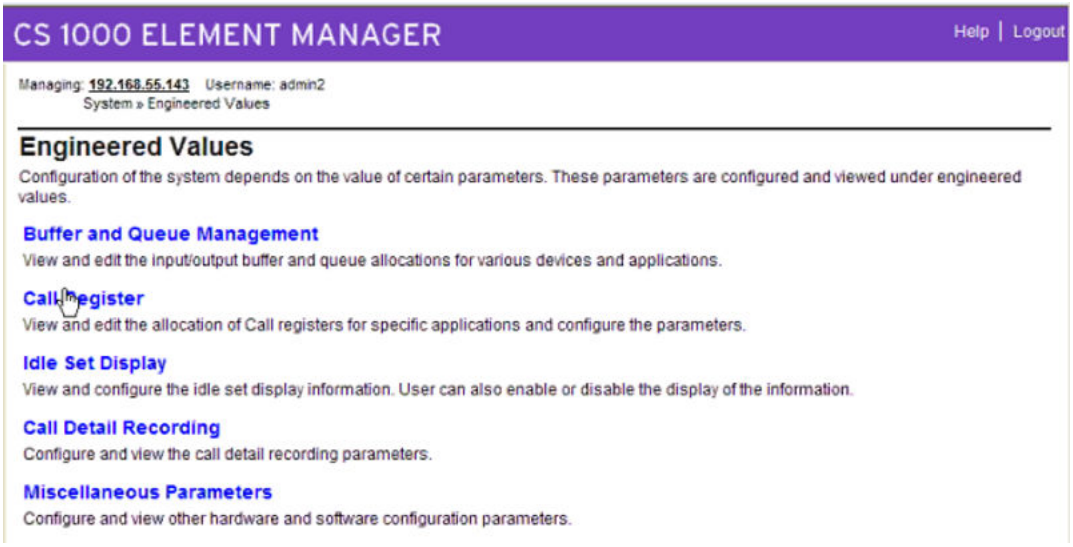


Figure 111: Engineered Values Web page

To configure the input/output buffer and queue allocations for various devices and applications, click **Buffer and Queue Management** . The Buffer and Queue Management Web page appears as shown in Figure 112: Buffer and Queue Management Web page on page 193.

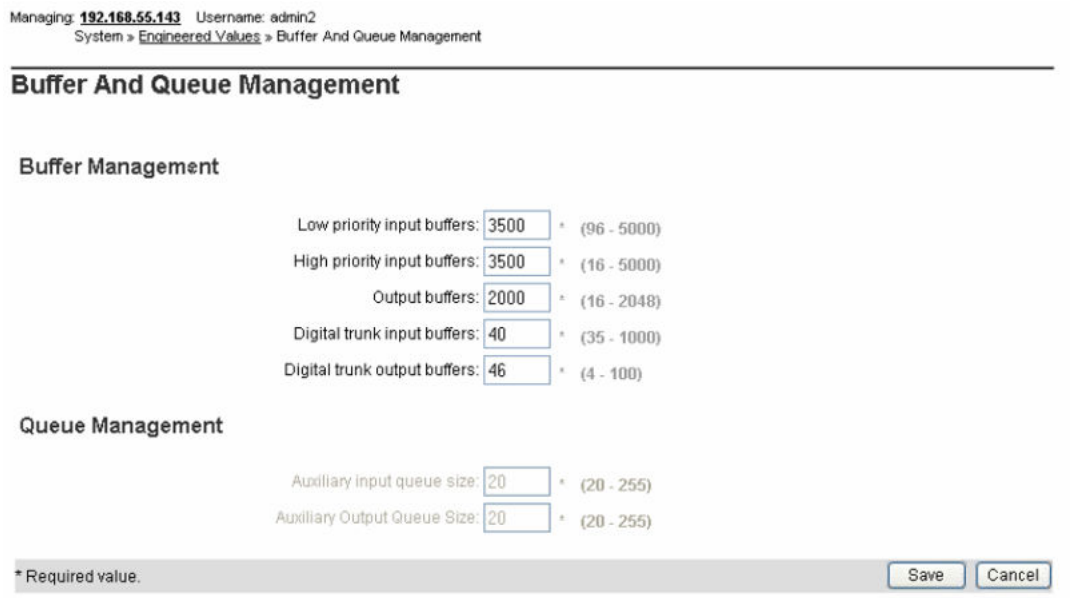


Figure 112: Buffer and Queue Management Web page

Type the desired parameters within the ranges indicated and click Save.

To configure the allocation of Call Registers for specific applications, on the Engineered Values Web page click **Call Registers** . The Call Registers Web page appears as shown in Figure 113: Call Register Web page on page 194.

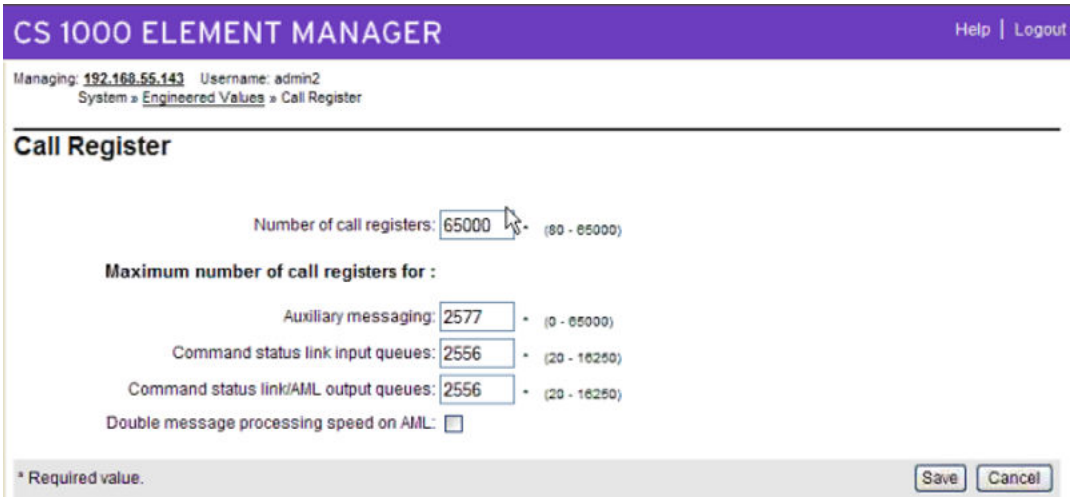


Figure 113: Call Register Web page

Enter the desired parameters within the ranges indicated and click **Save** .

To configure idle set display information, on the Engineered Values Web page click **Idle Set Display** . The Idle Set Display Web Page appears as shown in Figure 114: Idle Set Display Web page on page 194.

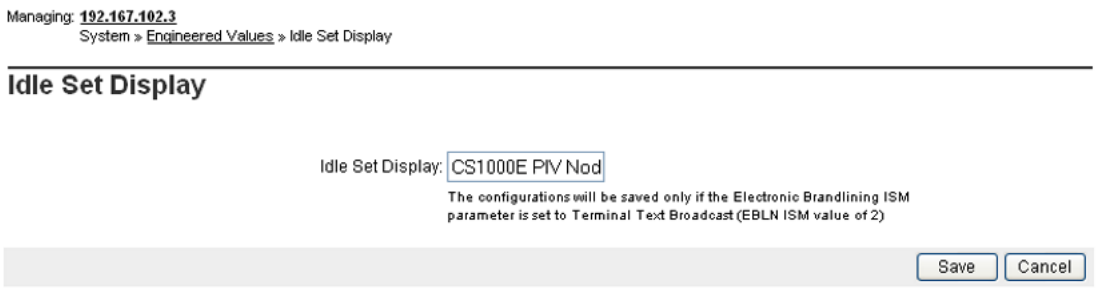


Figure 114: Idle Set Display Web page

Enter the desired display information and click **Save** .

To configure Call Detail Recording parameters, on the Engineered Values Web page click **Call Detail Recording** . The Call Detail Recording Web page appears as shown in Figure 115: Call Detail Recording Web page on page 195.

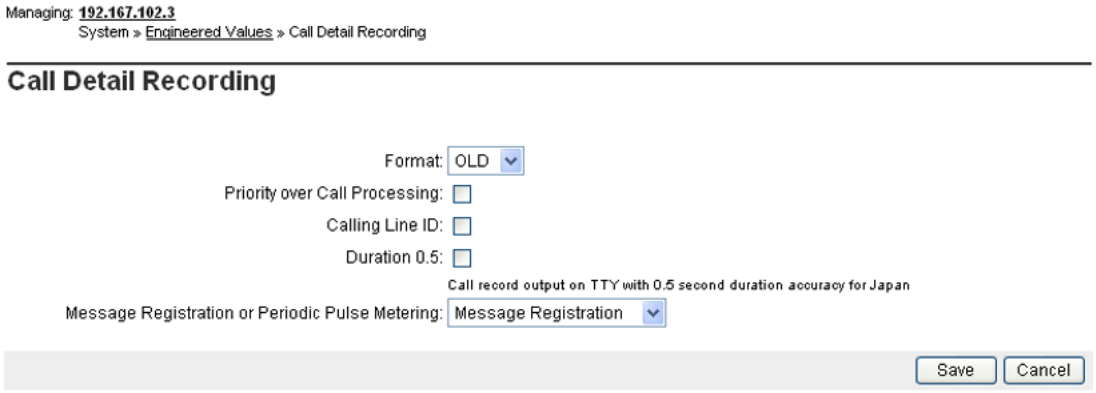


Figure 115: Call Detail Recording Web page

Type the desired parameters and click **Save** .

To configure other hardware and software parameters, on the Engineered Values Web page click **Miscellaneous Parameters** . The Miscellaneous Parameters Web page appears as shown in Figure 116: Miscellaneous Parameters Web page on page 196.

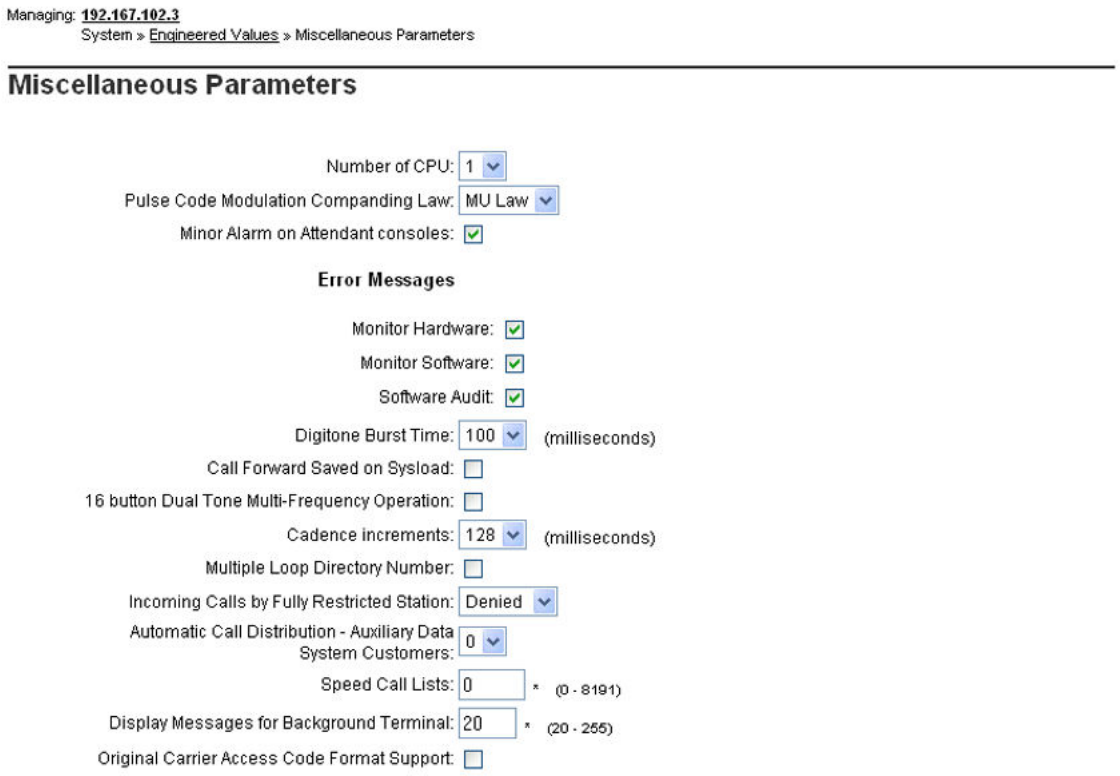


Figure 116: Miscellaneous Parameters Web page

Type the desired parameters and click **Save** .

Emergency Services

Element Manager supports the Emergency Services Client Mobility feature, which allows users to manage the location of phones, and to process emergency calls according to the caller's current data.

Service Parameters

The Service Parameters Web page allows users to modify system-wide configuration settings.

Click the **Emergency Services > Service Parameters** link in the **System** branch of the Element Manager navigator to open the Service Parameters Web page, as shown in Figure 117: Service Parameters Web page on page 197.

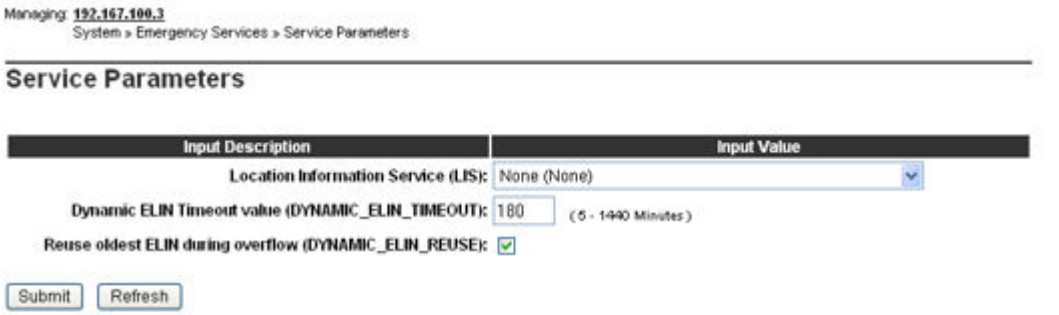


Figure 117: Service Parameters Web page

- Choose a **Location Information Service** from the first drop-down list.
  - If **Internal Subnet Location Information Service** is selected, the **Lookup Private Address for Subnet** check box appears.
  - If **External Discovery Manager** is selected, the **External Location Update Timeout** text box appears.
- Enter a **Dynamic ELIN Timeout value** .
- Check **Reuse oldest ELIN during overflow** , if necessary.
- Click **Submit** .

Access Numbers and Routing

The Access Numbers and Routing Web page allows users to process Emergency Service information, which is specific to each Customer.

Click the **Emergency Services > Access Numbers and Routing** link in the **System** branch of the Element Manager navigator to open the Access Numbers and Routing Web page, as shown in Figure 118: Access Numbers and Routing Web page on page 198.

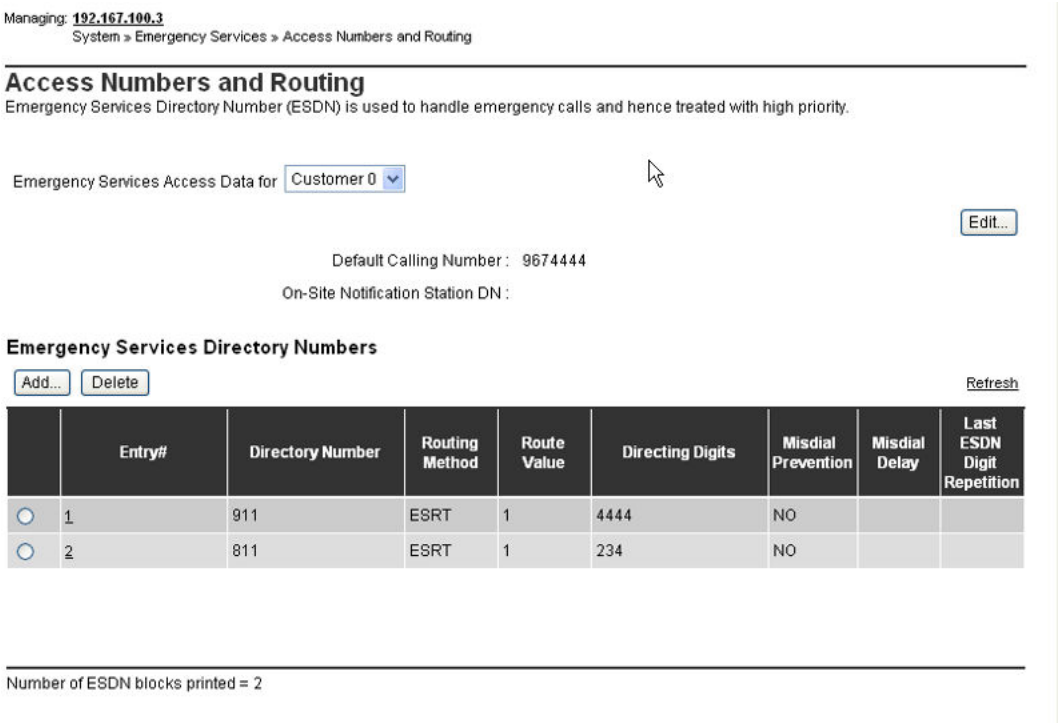


Figure 118: Access Numbers and Routing Web page

To add an Emergency Services Directory Number, click **Add** . The Add Emergency Services Directory Number Web page appears, as shown in Figure 119: Add Emergency Services Directory Number Web page on page 199.

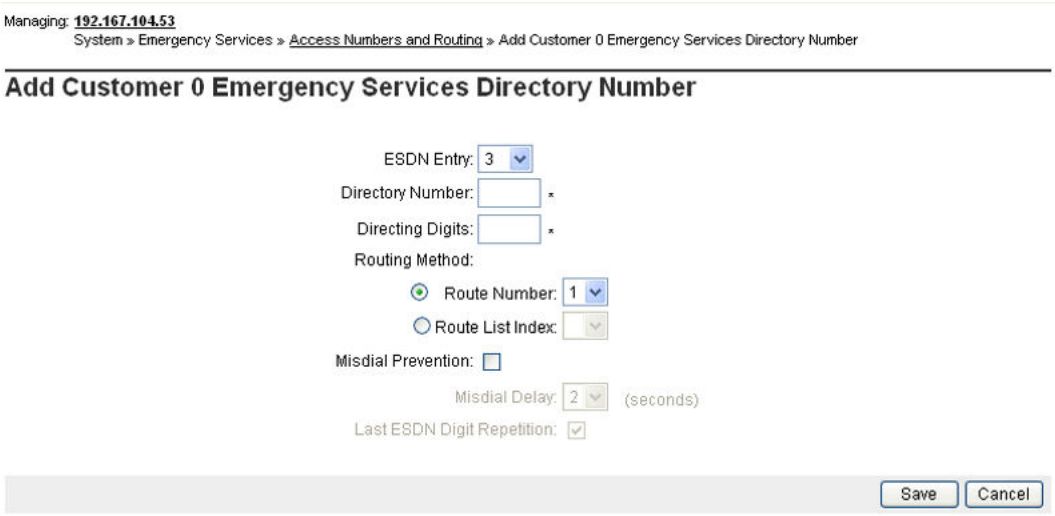


Figure 119: Add Emergency Services Directory Number Web page

To edit an existing Emergency Services Directory Number, from the Access Numbers and Routing Web page click the **Entry#** . The Edit Emergency Services Directory Number Web page appears, as shown in Figure 120: Edit Emergency Services Directory Number Web page on page 199.

Figure 120: Edit Emergency Services Directory Number Web page

To edit the CLID configuration for a Customer, select a Customer from the **Choose a customer** drop-down list and click **Edit** . The Edit Access Numbers and Routing Web page

appears, as shown in Figure 121: Edit Access Numbers and Routing Web page on page 200.

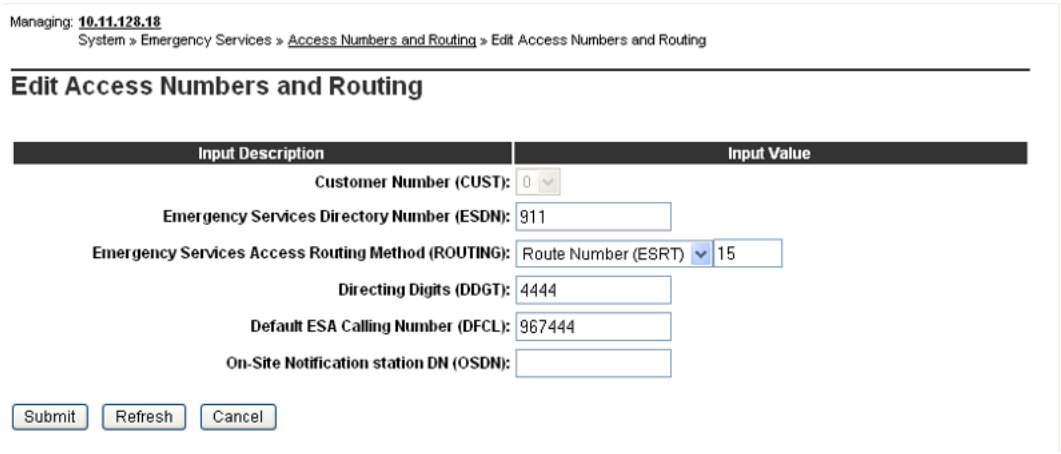


Figure 121: Edit Access Numbers and Routing Web page

To add a new CLID configuration for a Customer, on the Access Numbers and Routing Web page click **Add** . The Add Access Numbers and Routing Web page appears, as shown in Figure 122: Add Access Numbers and Routing Web page on page 200.

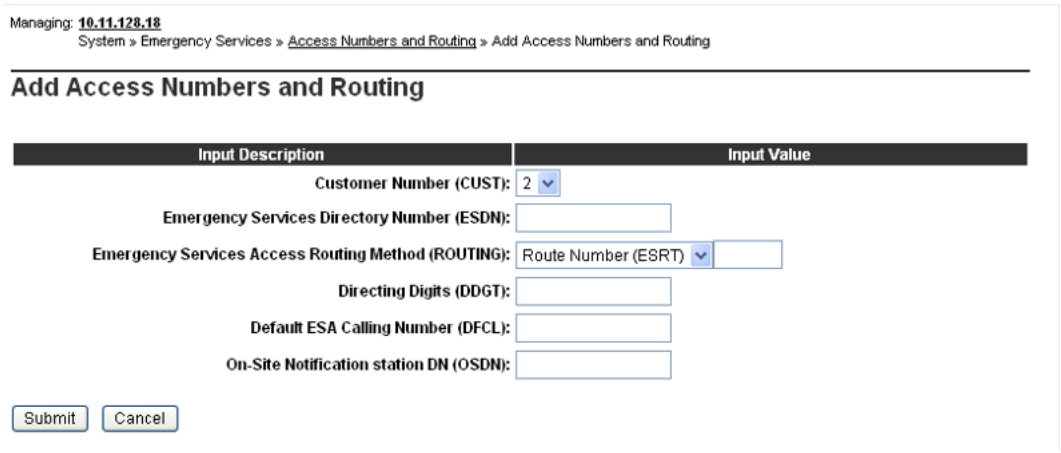


Figure 122: Add Access Numbers and Routing Web page

Choose a Customer from the **Customer Number** drop-down list. Complete the information in the remaining fields and click **Submit** .

To delete the CLID configuration for a customer, on the Access Numbers and Routing Web page click **Delete** .

Response Locations

Click the **Emergency Services > Emergency Response Locations** link in the **System** branch of the Element Manager navigator to open the Emergency Response Location Web page, as shown in Figure 123: Emergency Response Location Web page on page 201.

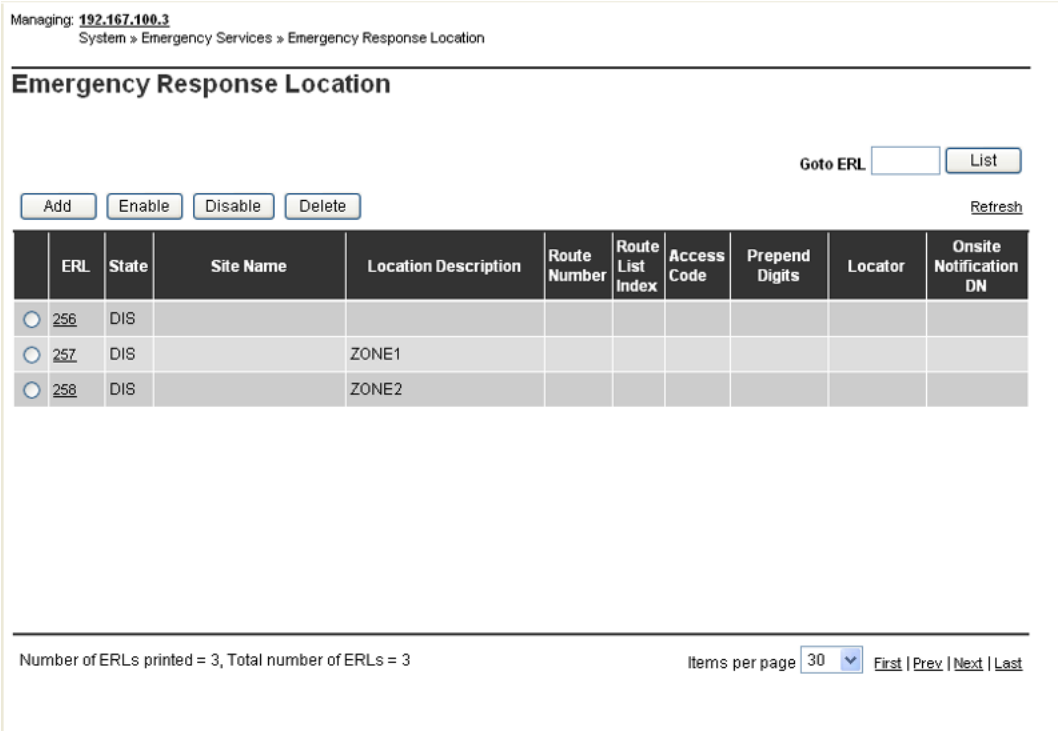


Figure 123: Emergency Response Location Web page

This Web page allows users to add, enable, disable, or delete Emergency Response Locations (ERLs).

To add an ERL, click the radio button for the ERL and click **Add** .

To enable an ERL, click the radio button for the ERL and click **Enable** .

To disable an ERL, click the radio button for the ERL and click **Disable** .

To delete an ERL, click the radio button for the ERL and click **Delete** .

To edit an ERL, click the ERL number. The Edit Emergency Response Location Web page appears, as shown in Figure 124: Edit Emergency Response Location Web page on page 202.

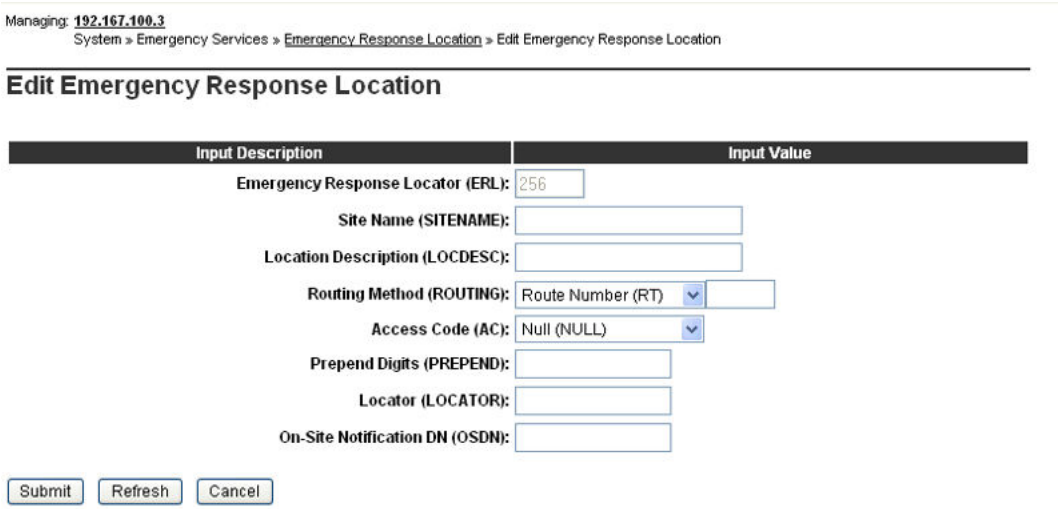


Figure 124: Edit Emergency Response Location Web page

To add an ERL, on the Emergency Response Location Web page, click **Add** . The Add Emergency Response Location Web page appears, as shown in Figure 125: Add Emergency Response Location Web page on page 203.

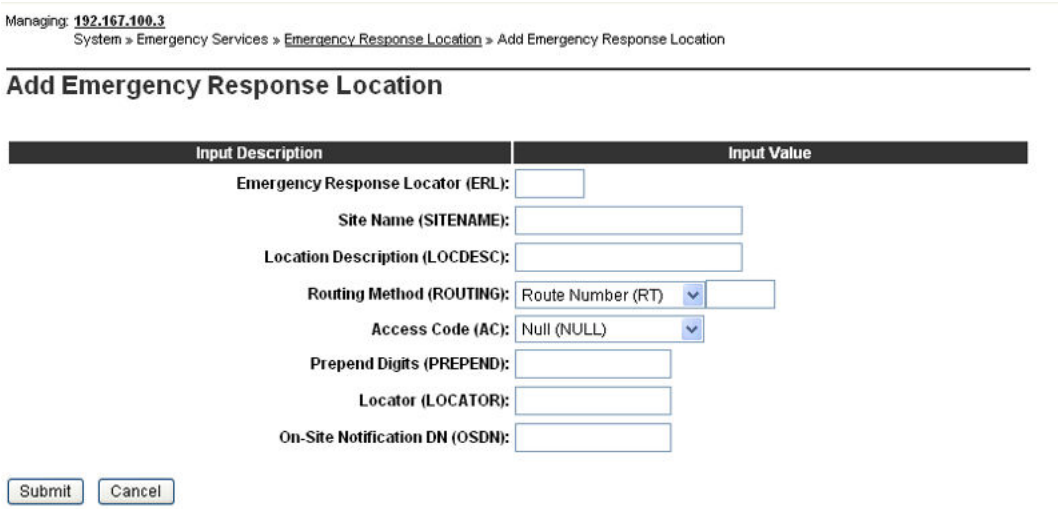


Figure 125: Add Emergency Response Location Web page

Enter the information for the new ERL and click **Submit** .

Subnet Information

The Subnet Location Information Web pages allow users to modify subnet information.

Click the **Emergency Services > Subnet Information** link in the **System** branch of the Element Manager navigator to open the Subnet Location Information Service Web page, as shown in Figure 126: Subnet Location Information Service Web page on page 204.

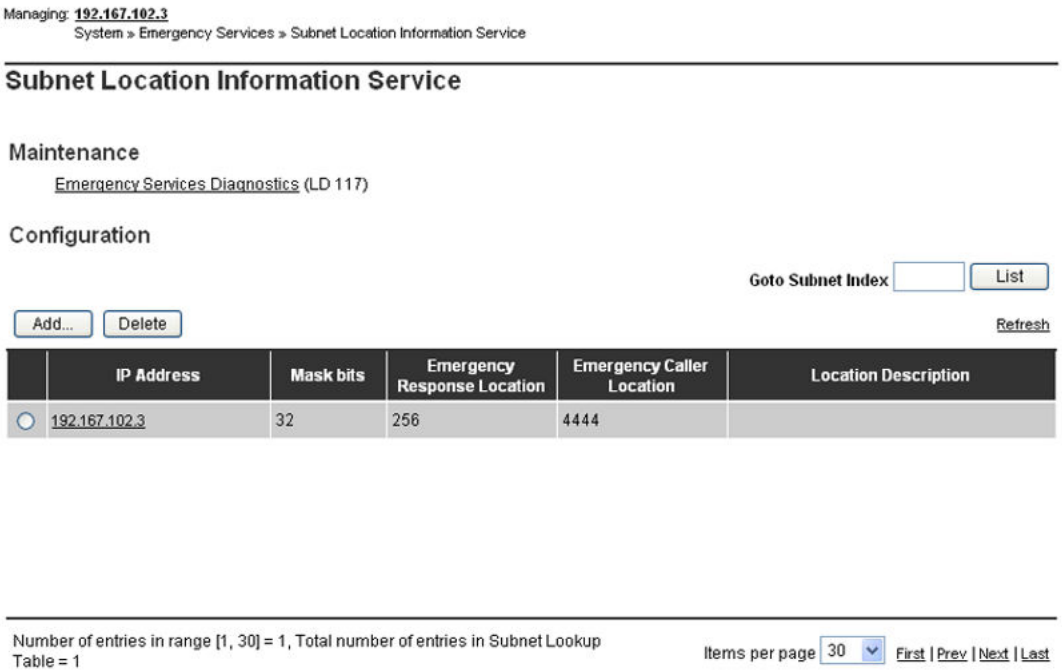


Figure 126: Subnet Location Information Service Web page

The Maintenance section contains a link to the Emergency Services Diagnostics Web page. See Emergency Services Diagnostics on page 77.

The Configuration section lists the configured subnet entries. To delete a configured Subnet Location, select the appropriate radio button beside an IP Address and click **Delete** .

To edit a configured Subnet Location, click the Subnet Location **IP Address** . The Edit Subnet Location Information Web page appears, as shown in Figure 127: Edit Subnet Location Information Web page on page 205.

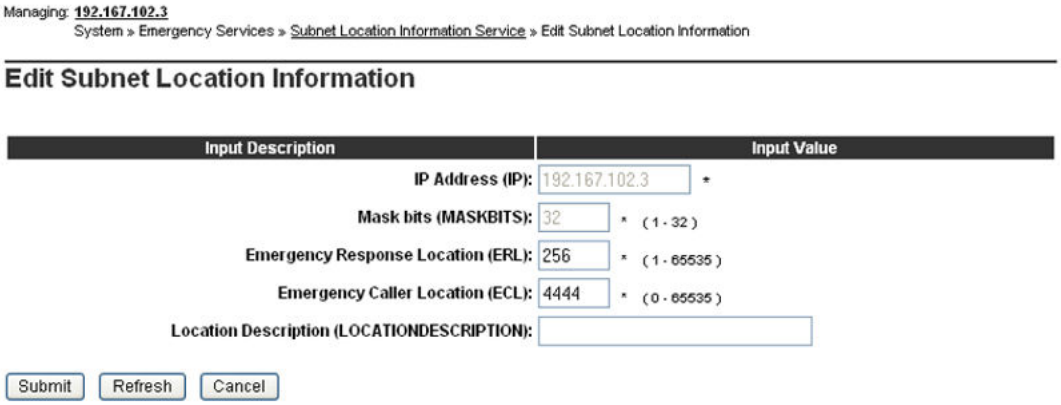


Figure 127: Edit Subnet Location Information Web page

To add a Subnet Location, from the Subnet Location Information Service Web page click **Add** . The Add Subnet Location Information Web page appears, as shown in Figure 128: Add Subnet Location Information Web page on page 205.

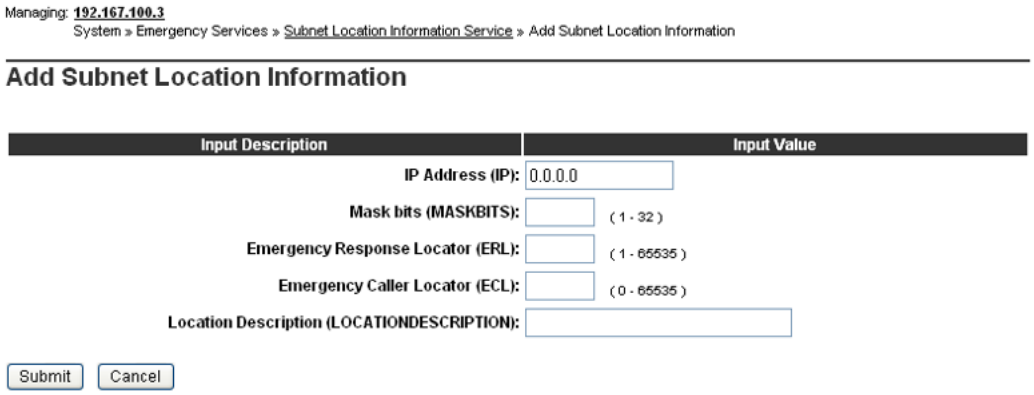


Figure 128: Add Subnet Location Information Web page

Enter the information for the new Subnet Location and click **Submit** .

Dynamic ELIN

The Dynamic Identification Web pages allow users to modify Dynamic Emergency Location information.

Click the **Emergency Services > Dynamic ELIN** link in the **System** branch of the Element Manager navigator to open the Dynamic ELIN Web page, as shown in Figure 129: Dynamic ELIN Web page on page 206.

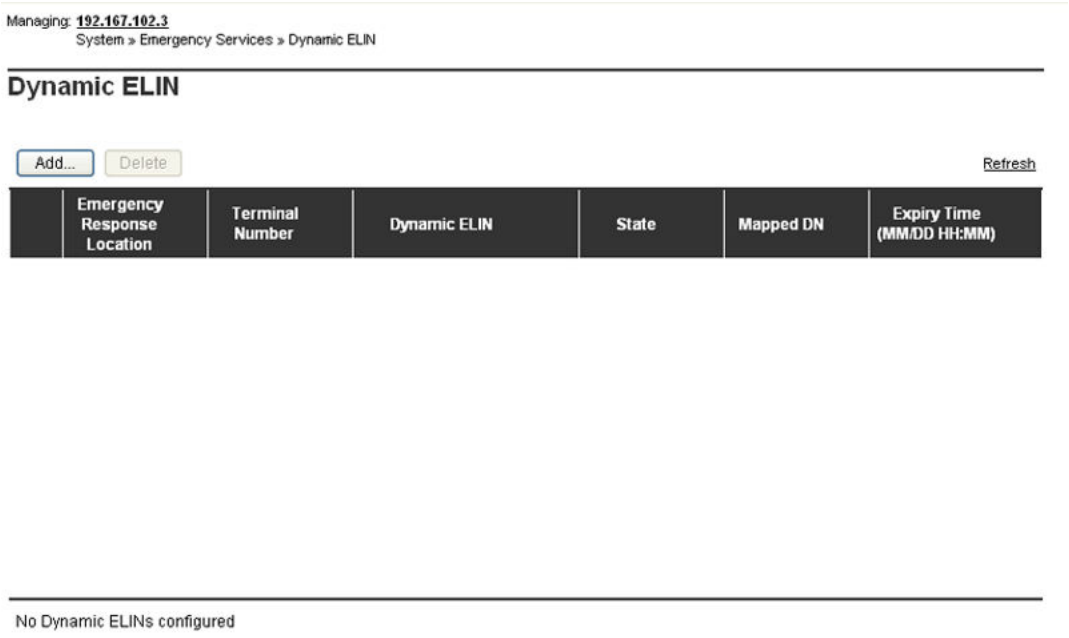


Figure 129: Dynamic ELIN Web page

This Web page lists the configured Dynamic ELINs.

To delete an ELIN, click the radio button for the ELIN and click **Delete** .

To add an ELIN, click **Add** . The Add Dynamic Location Identification Number Web page appears, as shown in Figure 130: Add Dynamic Location Identification Number Web page on page 206.

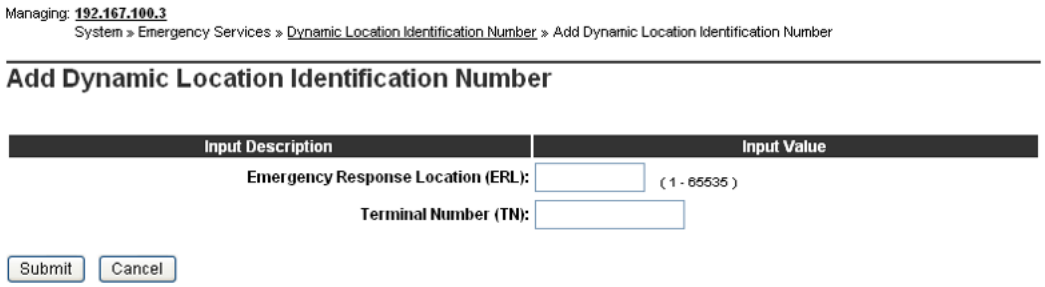


Figure 130: Add Dynamic Location Identification Number Web page

Enter the information for the new ELIN and click **Submit** .

Virtual Office Phone

The Virtual Office Phone Web pages allow users to maintain lists of mapped and unused Virtual Office TNs.

Click the **Emergency Services > Virtual Office Phone** link in the **System** branch of the Element Manager navigator to open the Virtual Office Phone Web page, as shown in Figure 131: Virtual Office Phone Web page on page 207.

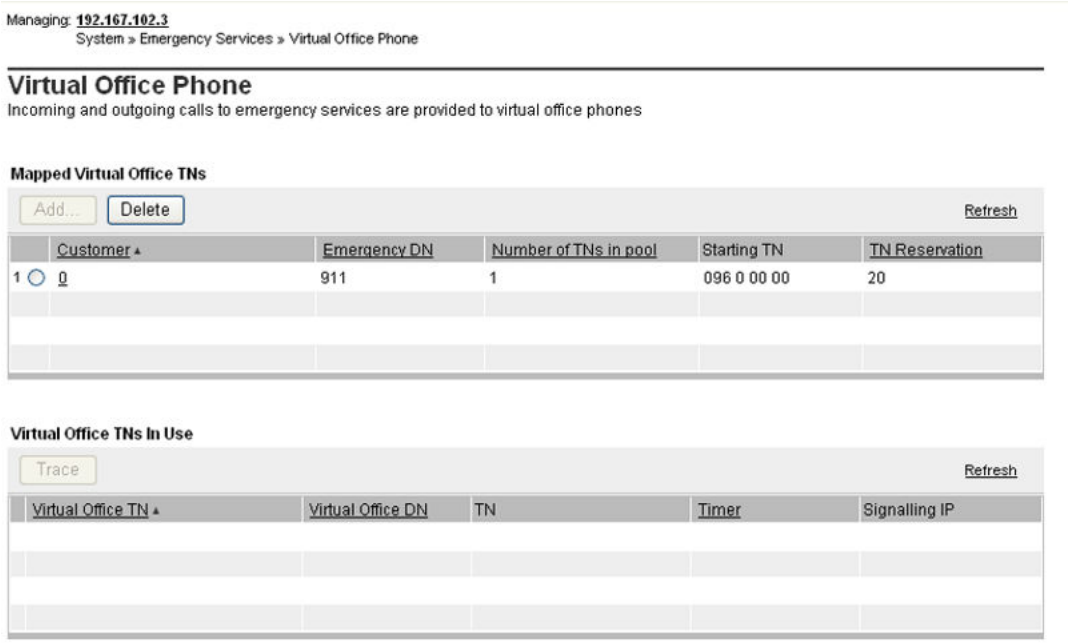


Figure 131: Virtual Office Phone Web page

To delete a Mapped Virtual Office TN, click the radio button for the Customer and click **Delete** .

To Add a Mapped Virtual Office TN, click **Add** , enter the information for the new Virtual Office TN, and click **Save** .

This Web page includes two sections listing **Mapped Virtual Office TN Pools** and Virtual Office TNs in Use.

Geographic Redundancy

Geographic Redundancy is available only on CPP IV and CP PM systems.

Database Replication Control

To configure or edit Database Replication information, click the **Geographic Redundancy > Database Replication Control** link in the **System** branch of the Element Manager navigator. The Database Replication Control Web page appears as shown in Figure 132: Database Replication Control Web page on page 208.

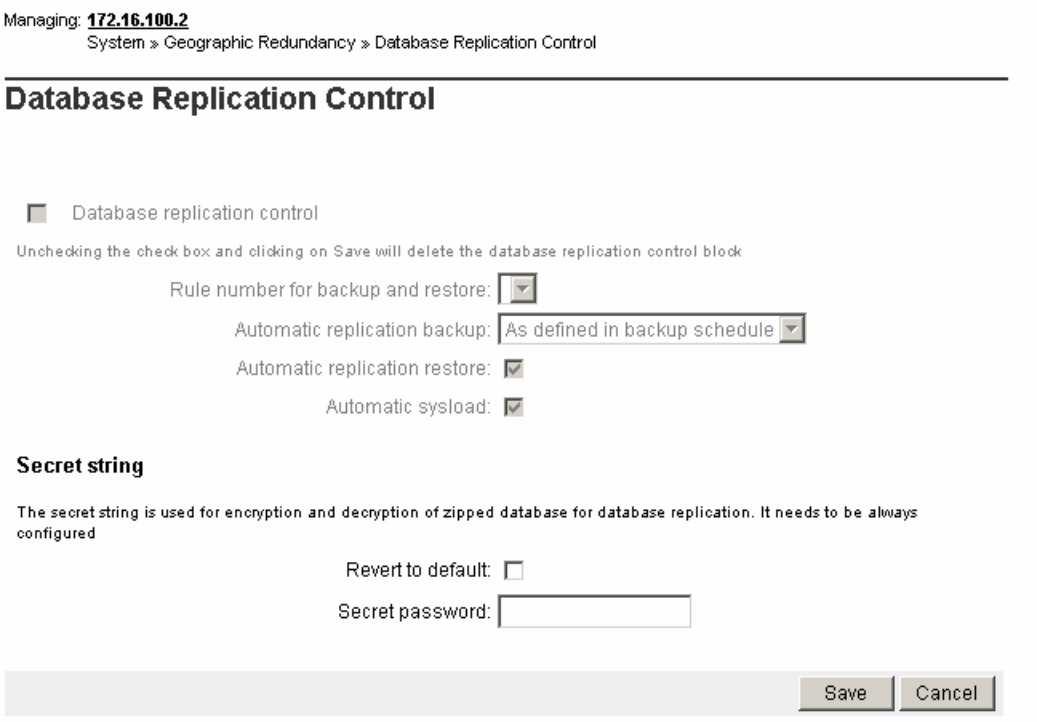


Figure 132: Database Replication Control Web page

On the Database Replication Control Web page, you can configure the following information:

- **Rule number for backup and restore**
- **Automatic replication backup** (ABKUP)
- **Automatic replication restore**
- **Automatic sysload**

Note:

You must configure one SCS backup rule before Database Replication Control Web page can be configured.

You can also create a Secret string. You create a mandatory Secret string for encryption and decryption of a zipped database and database replication.

State Control

To configure State Control information, click the **Geographic Redundancy > State Control** link in the **System** branch of the Element Manager navigator. The State Control Web page appears as shown in Figure 133: State Control Web page on page 209.

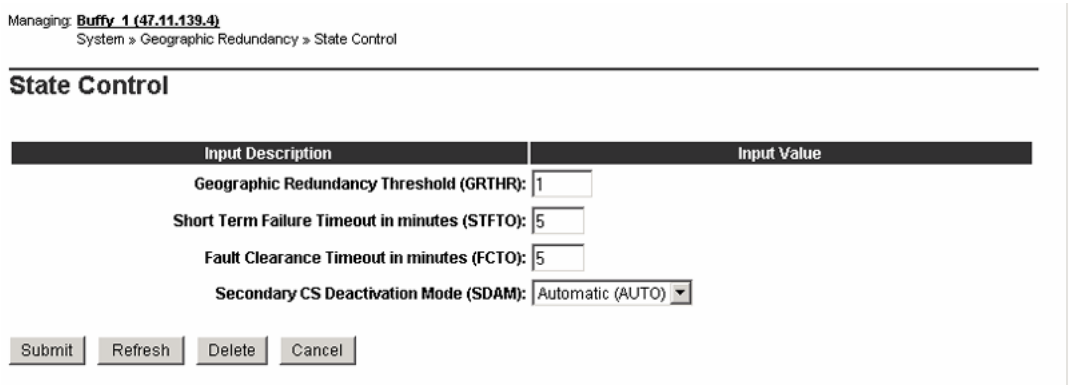


Figure 133: State Control Web page

On the State Control Web page, users can configure:

- Associated Secondary Call Server
- Threshold1 (Number Of IP phones registered)
- Threshold2 (Number of Media Gateways registered)
- Short Term Failure Timeout in minutes
- Fault Clearance Timeout in minutes
- Secondary CS Deactivation Mode

The information entered on this Web page corresponds to the commands available in LD 117.

For more information about Geographic Redundancy, see *Avaya System Redundancy Fundamentals, NN43001-507* .

Software

The **Software** link of the **System** branch of the Element Manager navigator can be used to perform patching of the Call Server or the Media Gateway.

To use the patching feature, you must enter the administrator password configured in LD 17 and have PDT access. You can use any browser to download patches from the Avaya ESPL Web site. Go to www.support.avaya.com. In the navigation tree, expand **Tools**, and then select **Enterprise Solutions PEP Library (Restricted Access)**. If you do not have an existing profile

for the ESPL site, you can register. Users, who already have profiles, can go to www.support.avaya.com/espl and log on to the ESPL site using their existing credentials.

For MGC and VGMC loadware distribution and functionality instructions, see *Enterprise Voice Solutions* and *Best Practice Guidelines*, which you can download from the ESPL Web site.

Loadware PEPs

Perform Loadware PEPs patching by clicking **Software > Loadware PEPs** link in the **System** branch of the Element Manager navigator as shown in figure Figure 134: Loadware PEPs on page 210.

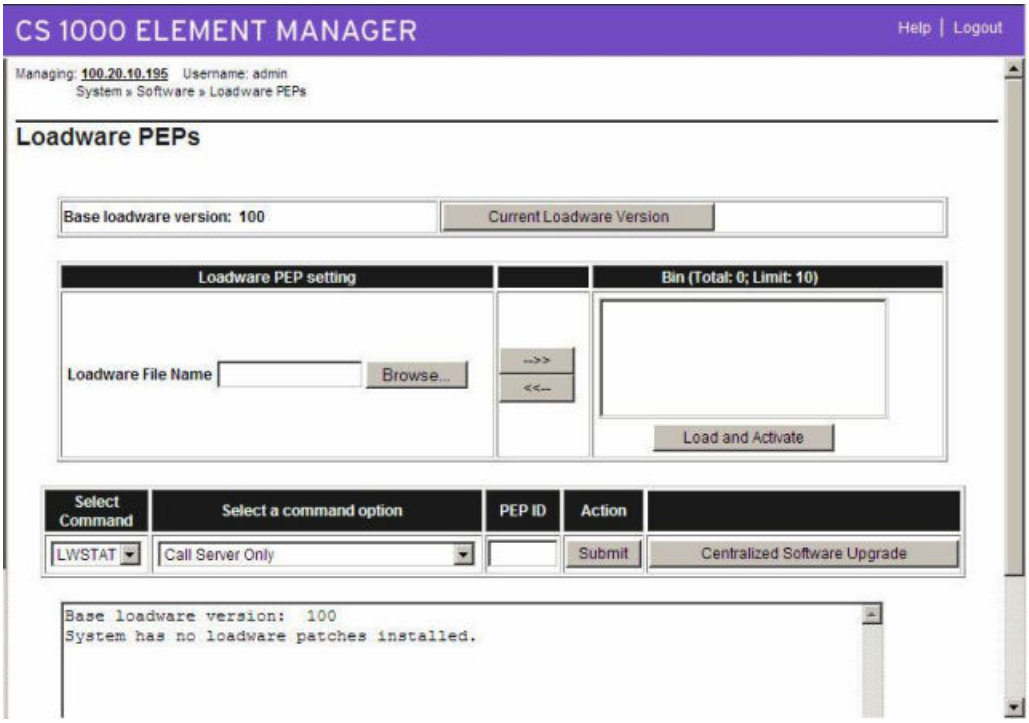


Figure 134: Loadware PEPs

From the Loadware PEPs Web page, user can

- load and activate a new Product Enhancement Package (PEP)
- get the status of a single PEP or all PEPs (PSTAT)
- view the details of Loadware on a PEP

Call Server PEPs

Perform Call Server patching by clicking the **Software > Call Server PEPs** link in the **System** branch of the Element Manager navigator. The Call Server Web page appears, as shown in Figure 135: Call Server Web page on page 211.

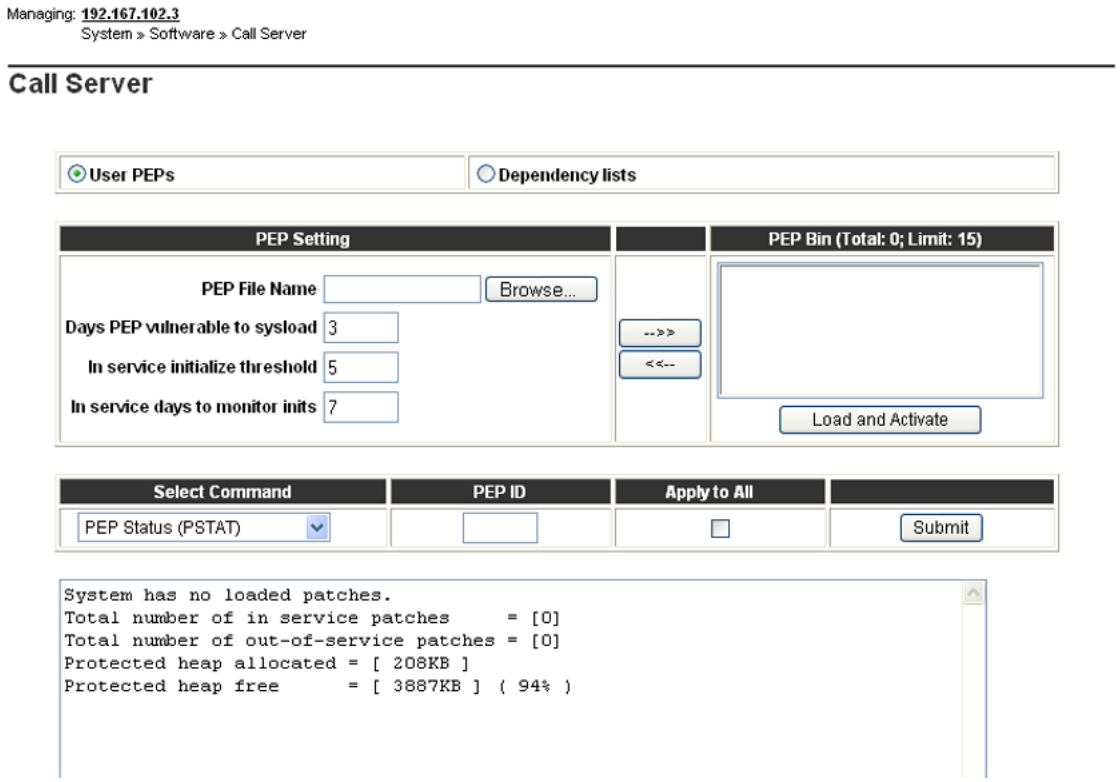


Figure 135: Call Server Web page

From the Call Server Web page, the user can:

- load and activate a new Product Enhancement Package (PEP)
- get the status of a single PEP or all PEPs (PSTAT)
- activate a single PEP or all PEPs (PINS)
- deactivate a single PEP or all PEPs (POOS)
- remove a single PEP or all PEPs (POUT)
- view the details on a PEP (PLIS)

The **PEP Setting** section at the top left of the Web page enables the user to select files and choose settings. Clicking the right arrow (**->>**) button moves PEP files into the **PEP Bin** section. Clicking the left arrow (**<<-**) button moves PEP files out of the **PEP Bin** section. Click **Load**

and Activate to submit the selected PEP to the call server. Results are displayed at the bottom of the screen.

Note:

The user can download only 15 PEP files at a time. To install more than 15 PEPs on a single entity, the user must run the utility again.

All PEP commands require the PEP ID. After selecting the PEP command from the drop-down list, enter the **PEP ID** in the text box.

The **Apply to All** check box is enabled for all commands with the exception of the PLIS command. Clicking the **Submit** button executes the command. Results are displayed at the bottom of the screen.

PEP Management can be applied to Call Servers. Element Manager enables users to load Matrix DepLists (MDP) to the Call Server and manage the MDPs by using the Management DepList commands. Click the **Dependency lists** radio button. See Figure 136: Call Server Web page - Dependency Lists on page 212.

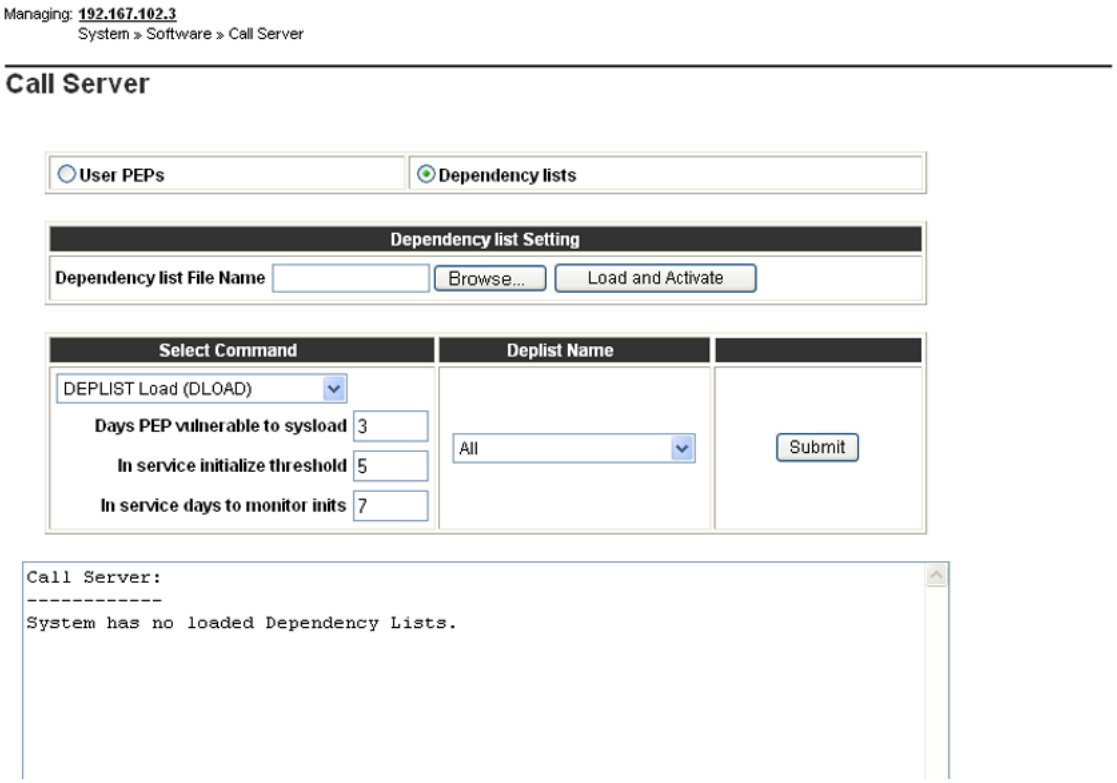


Figure 136: Call Server Web page - Dependency Lists

PEP lists are populated with individual PEPs contained in an update when a Matrix DepList is opened. The **Refresh** command refreshes the contents of an MDP on a target system and enables the user to load MDPs properly.

PEP Management supports the following commands:

- load and activate a new PEP (DLOAD)
- get the status of a single PEP or all PEPs (DSTAT)
- activate a single PEP or all PEPs (DINS)
- deactivate a single PEP or all PEPs (DOOS)
- remove a single PEP or all PEPs (DOUT)
- view the details on a PEP (DLIS)

Each PEP in the Matrix DepList has its own PEP handle and can be uninstalled, similar to current multipatch functionality.

Loading and Activating PEP Settings on the Call Server

1. Select the **User PEPs** radio button on the Call Server page.
2. Click **Browse** .

   The Choose file window appears.
3. Choose a file to be downloaded and click **Open** .
4. Enter the number of **Days PEP vulnerable to sysload** .
5. Enter the **In service initialize threshold** .
6. Enter the **In service days to monitor inits** .
7. Click the **-->>** (right arrow) button to move the PEP files into the PEP Bin section.
8. Click **Load and Activate** to submit the selected PEPs to the call server.

   Results appear at the bottom of the screen.

Additional Commands

From the Select Command list select one of the following:

- **PEP Status (PSTAT)** - Shows the status of the PEP
- **PEP In-Service (PINS)** - Places the PEP in service
- **PEP Out-Of-Service (POOS)** - Takes the PEP out of service
- **PEP Out (POUT)** - Unloads the PEP
- **PEP List (PLIS)** - Lists information about the PEP

After you select the appropriate command, select either **PEP ID** and type the **PEP ID**, on which you want to run the command, or select **Apply to All** to run the selected command on all of the PEPs. Then select **Submit** .

Loading and Activating Dependency lists on the Call Server

1. Select the **Dependency lists** radio button on the Call Server page.
2. Click **Browse** .

The Choose file window appears.

3. Choose a file to be downloaded and click **Open** .
4. Click **Load and Activate** to submit the selected Deplist to the call server.

Additional Commands

From the **Select Command** box select one of the following:

- **DEPLIST Load (DLOAD)** - Loads the Deplist
- **DEPLIST Status (DSTAT)** - Shows the status of the Deplist
- **DEPLIST In-Service (DINS)** - Places the Deplist in service
- **DEPLIST Out-Of-Service (DOOS)** - Takes the Deplist out of service
- **DEPLIST Out (DOUT)** - Unloads the Deplist
- **DEPLIST List (DLIS)** - Lists information about the Deplist

After you select the appropriate command, select the **Deplist Name** , on which to run the command. Then click **Submit** .

You can also configure the following parameters when you load a Deplist:

- the number of **Days PEP vulnerable to sysload**
- the **In service initialize threshold**
- the **In service days to monitor inits**

Warning:

Service updates that contain many PEPs can take time to install.

Software

The **Software** link of the **System** branch of the Element Manager navigator can also be used to upload and store files, upgrade firmware, and perform patching activities.

Centralized File Upload

The file upload function enables users to upload and store loadware and firmware files on the Signaling Server. These files can then be downloaded to network elements, using the functions available under the **Software > File Upload** link in the **System** branch of the navigator.

For more information about the file upload function, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

IP Phone Firmware

The **Software > IP Phone Firmware** link in the **System** branch of the Element Manager navigator allows users to upgrade IP Phone firmware. For more information, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

TPS Firmware

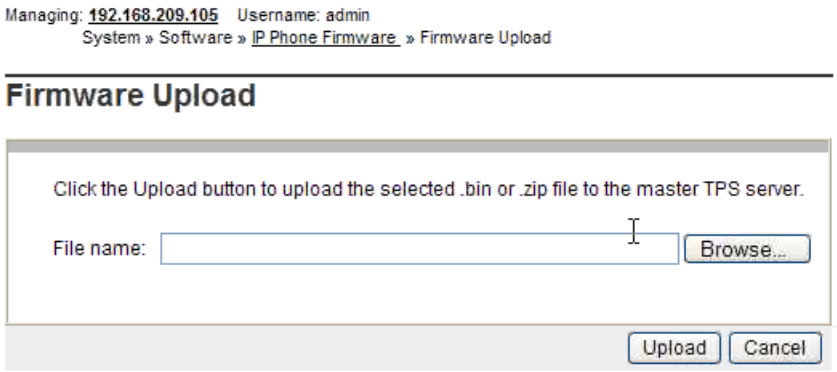
The TPS firmware feature enables the users to view, add, and delete firmware files present in the master TPS (Terminal Proxy Server). You can navigate to the feature from **Software > IP Phone Firmware > TPS Firmware**. TPS Firmware is presented as a link in the IP Phone Firmware web page. When you click the link, the Firmware Maintenance Web page opens.

To add a new firmware file to the master TPS, perform the following procedure

Adding new TPS firmware file

1. On the Firmware Maintenance Web page, click **Add**.

   The Firmware Upload Web page appears.



2. Click **Browse** to select the file to upload.

   The Choose File dialog box appears.
3. Select the file to upload.
4. Click **Open**.

   The path where the file is stored appears in the **File name** field.
5. Click **Upload**.

   A dialog box asks for confirmation on uploading the file.
6. Click **OK**.

   The page refreshes to display the TPS Firmware Web page with the new file.

To delete a firmware file from the master TPS, perform the following procedure.

Deleting a firmware file

1. Select the check box corresponding to the firmware file to be deleted.

   If you want to delete multiple files, select the check boxes corresponding to the required files. To delete all the files, select the check box corresponding to the **File Name** field.

2. Click **Delete** to delete the files.

   The system asks for a confirmation on deleting the files.

3. Click **Delete** to confirm the deletion.

   The Firmware Maintenance Web page refreshes.

Voice gateway media card loadware

The **Software >Voice Gateway Media Card** link in the **System** branch of the Element Manager navigator allows users to upgrade VGMC loadware as shown in the following figure. For more information, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

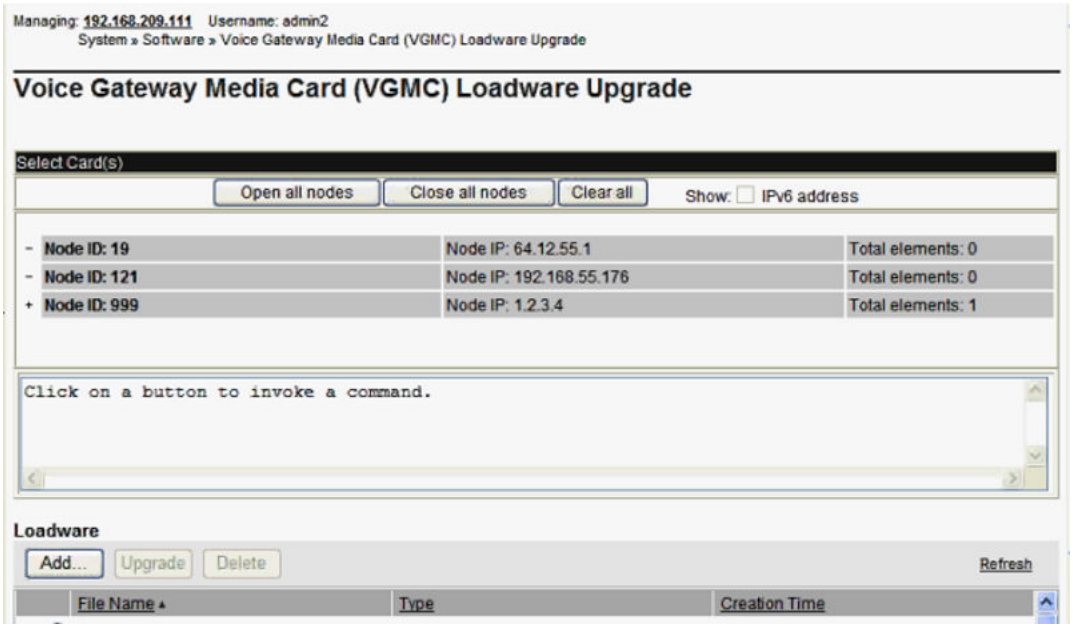


Figure 137: VGMC Loadware Upgrade

Media Cards

Click the **Software > Media Cards PEPs** link in the **System** branch of the Element Manager navigator to open the Media Cards Web page as shown in Figure 138: Media Cards Web page on page 217.

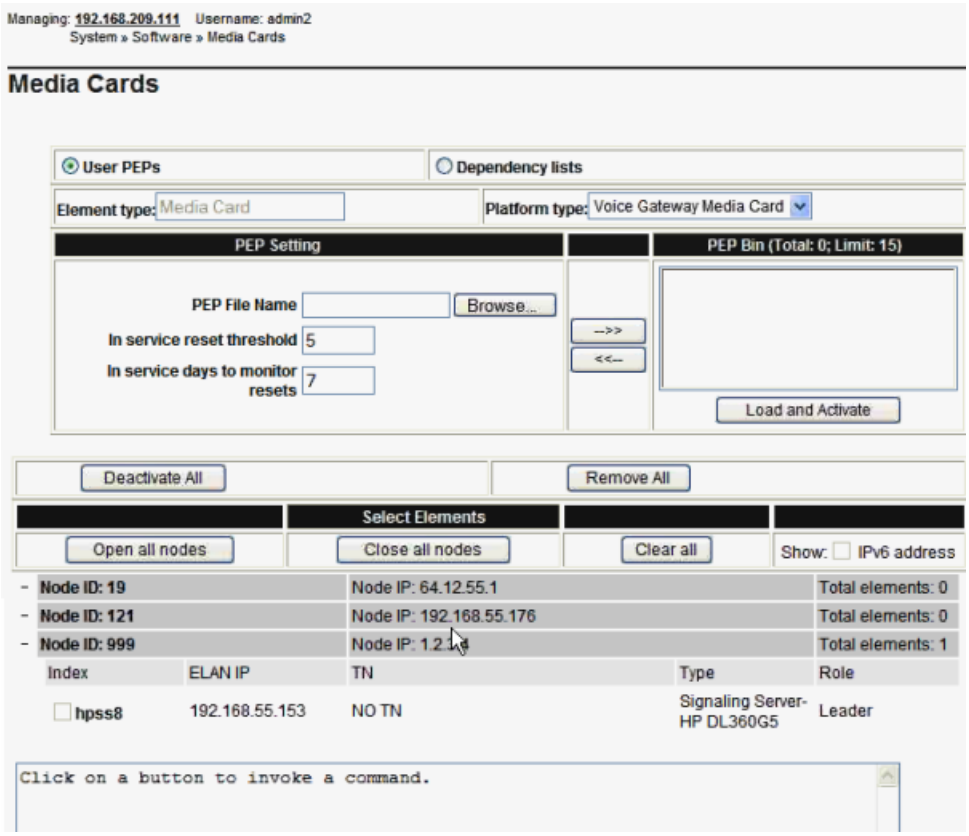


Figure 138: Media Cards Web page

From this Web page the following functions can be performed:

- load and activate a new PEP
- view the status of a single PEP or all PEPs (PSTAT)
- activate a single PEP or all PEPs (PINS)
- deactivate a single PEP or all PEPs (POOS)
- remove a single PEP or all PEPs (POUT)
- view the details on a PEP (PLIS)

The **PEP Setting** section at the top left of the Web page enables users to select files and choose settings.

Loading and Activating PEP Settings to the Signaling Server

1. Select the correct **Element type** and then **Platform type**.
2. Click **Browse**.

   The **Choose file** window appears.
3. Choose a file to be downloaded and click **Open**.
4. Enter the number of **Days PEP vulnerable to sysload**.
5. Enter the **In service initialize threshold**.
6. Enter the **In service days to monitor inits**.
7. Click the **-->>** (right arrow) button to move the PEP files into the PEP Bin section.
8. Click **Load and Activate** to submit the selected PEPs to the call server.

   Results are displayed at the bottom of the screen.

Clicking the **-->>** (right arrow) button moves PEP files into the **PEP Bin** section. Likewise, clicking the **<<--** (left arrow) button moves PEP files out of the **PEP Bin** section. Click **Load and Activate** to submit the selected PEPs to the call server. Results are displayed at the bottom of the screen.

Note:

A maximum of 15 PEP files can be downloaded at a time. If more than 15 PEPs must be installed on a single entity, the utility must be run again.

Click the **PSTAT** button to open the Type Web page for the selected element.

All PEP commands require the PEP ID. After selecting the PEP **Command** from the drop-down list, enter the **PEP ID** in the text box.

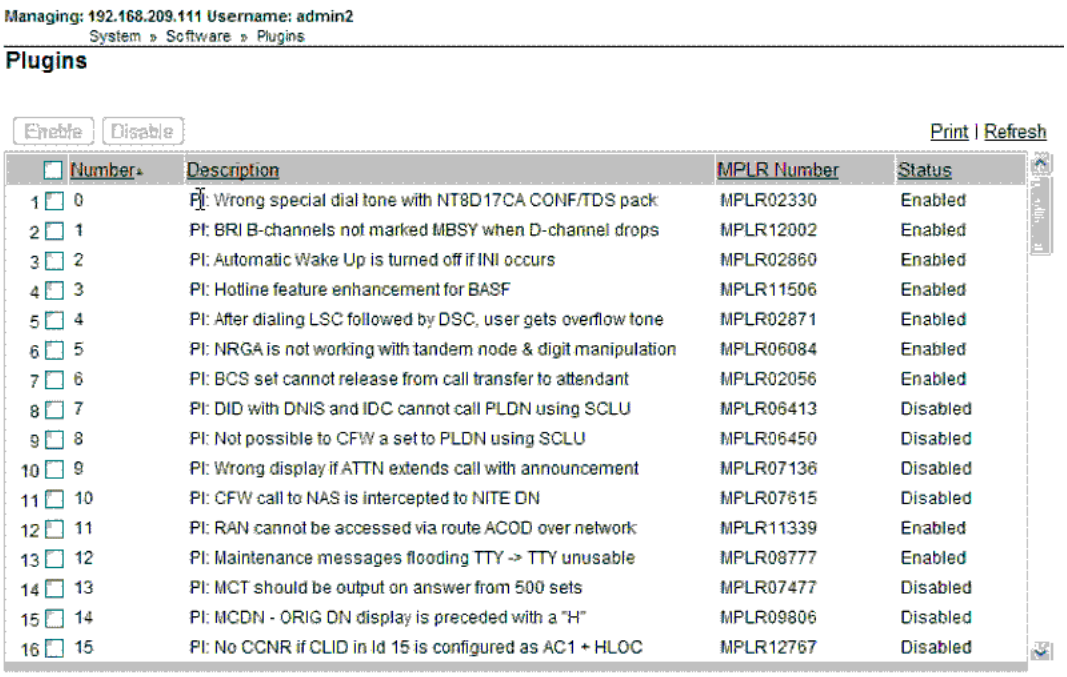
The **Apply to All** check box is enabled for all commands with the exception of the PLIS command. Clicking the **Submit** button executes the command. Results are displayed at the bottom of the screen.

Plug-ins

The Plug-ins feature displays the status and details of all the plug-ins in the Call Server. Using this feature you can enable or disable a particular plug-in or set of plug-ins. You can view this link only if you have PDT2 user rights.

To access the Plugins Web page, select **Software > Plug-ins** from the **System** branch of the Element Manager.

The following figure displays the Plugins Web page.



	Number	Description	MPLR Number	Status
1	0	PI: Wrong special dial tone with NT8D17CA CONF/TDS pack	MPLR02330	Enabled
2	1	PI: BRI B-channels not marked MBSY when D-channel drops	MPLR12002	Enabled
3	2	PI: Automatic Wake Up is turned off if INI occurs	MPLR02860	Enabled
4	3	PI: Hotline feature enhancement for BASF	MPLR11506	Enabled
5	4	PI: After dialing LSC followed by DSC, user gets overflow tone	MPLR02871	Enabled
6	5	PI: NRGA is not working with tandem node & digit manipulation	MPLR06084	Enabled
7	6	PI: BCS set cannot release from call transfer to attendant	MPLR02056	Enabled
8	7	PI: DID with DNIS and IDC cannot call PLDN using SCLU	MPLR06413	Disabled
9	8	PI: Not possible to CFW a set to PLDN using SCLU	MPLR06450	Disabled
10	9	PI: Wrong display if ATTN extends call with announcement	MPLR07136	Disabled
11	10	PI: CFW call to NAS is intercepted to NITE DN	MPLR07615	Disabled
12	11	PI: RAN cannot be accessed via route ACOD over network	MPLR11339	Enabled
13	12	PI: Maintenance messages flooding TTY -> TTY unusable	MPLR08777	Enabled
14	13	PI: MCT should be output on answer from 500 sets	MPLR07477	Disabled
15	14	PI: MCDN - ORIG DN display is preceded with a "H"	MPLR09806	Disabled
16	15	PI: No CCNR if CLID in Id 15 is configured as AC1 + HLOC	MPLR12767	Disabled

From the Plugins Web page you can perform the following actions:

- Enable a plug-in or set of plug-ins
- Disable a plug-in or set of plug-ins
- Print the details of the page
- Refresh the page to map all plug-ins with the Call Server

Use the following procedure to enable plug-ins on the Call Server.

Enabling plug-ins on the Call Server

1. Select the check box corresponding to the plug-in that you want to enable.

   To enable multiple plug-ins simultaneously, select the check boxes corresponding to the required plug-ins.
2. Click **Enable** .

   The page refreshes and displays the status of the plug-in as **Enabled** .

Use the following procedure to disable plug-ins on the Call Server.

Disabling plugi-ns on the Call Server

1. Select the check box corresponding to the plug-in you want to disable.

   To disable multiple plug-ins simultaneously, select the check boxes corresponding to the required plug-ins.
2. Click **Disable** .

   The page refreshes and displays the status of the plug-in as Disabled.

Chapter 9: Customers, Routes and Trunks

Contents

This chapter contains information about the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Introduction

The **Customers** and **Routes and Trunks** branches of the Element Manager navigator are used to launch Web pages that enable the user to configure and edit data relating to customers and their equipment.

Customers

When the user clicks the **Customers** branch of the Element Manager navigator, the Customers Web page appears, as shown in Figure 139: Customers Web page on page 222. To configure customer data, click the **Customer Number**.

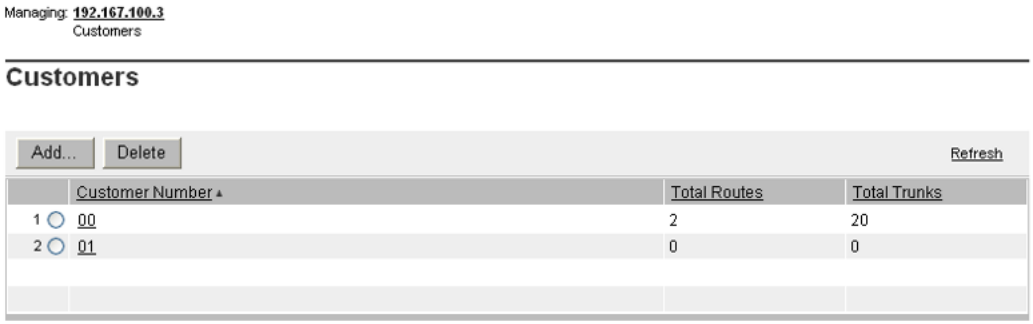


Figure 139: Customers Web page

Note:

To create a new customer, you must create a new role in Unified Communications Management (UCM) and modify the permissions for that role so that Customer Tenant Mappings reflect permissions for all customers to be added.

For information about creating a new roll in UCM, refer to *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

To add a new customer, click Add.

The Basic Configuration Web page appears, as shown in Figure 140: Basic Configuration Web page on page 223.

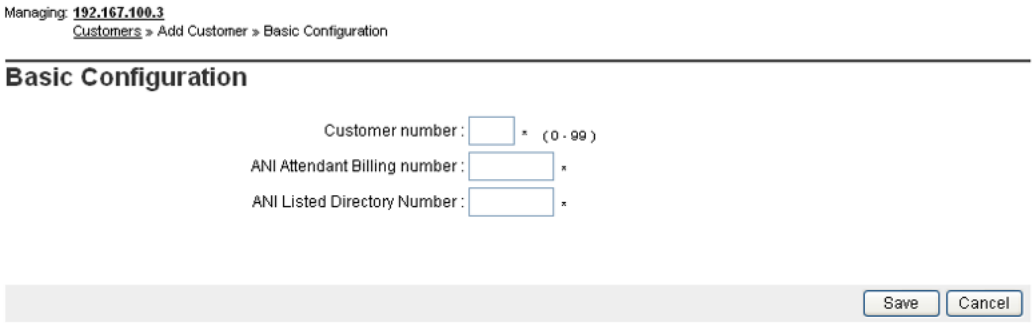


Figure 140: Basic Configuration Web page

The information entered in this Web page corresponds to Default Customer Data Block information traditionally configured using LD 15 - Customer Data Block.

Enter the required information in the three fields and click Save.

The Customer Details Web page appears, as shown in Figure 141: Customer Details Web page on page 224.

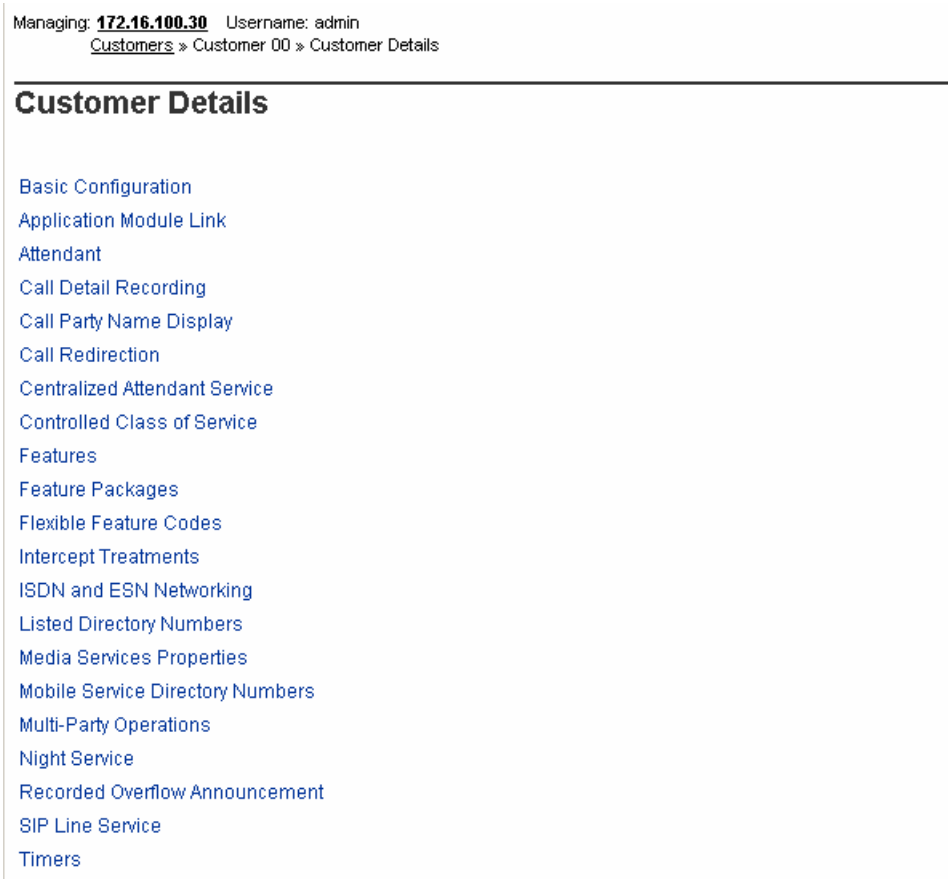


Figure 141: Customer Details Web page

This Web page contains links to web pages where users can configure additional parameters for each route data block.

Application Module Link

The Application Module Link Web page allows users to configure the Application Module Link data block for a customer. Click Application Module Link to open this Web page, as shown in Figure 142: Application Module Link Web page on page 225.

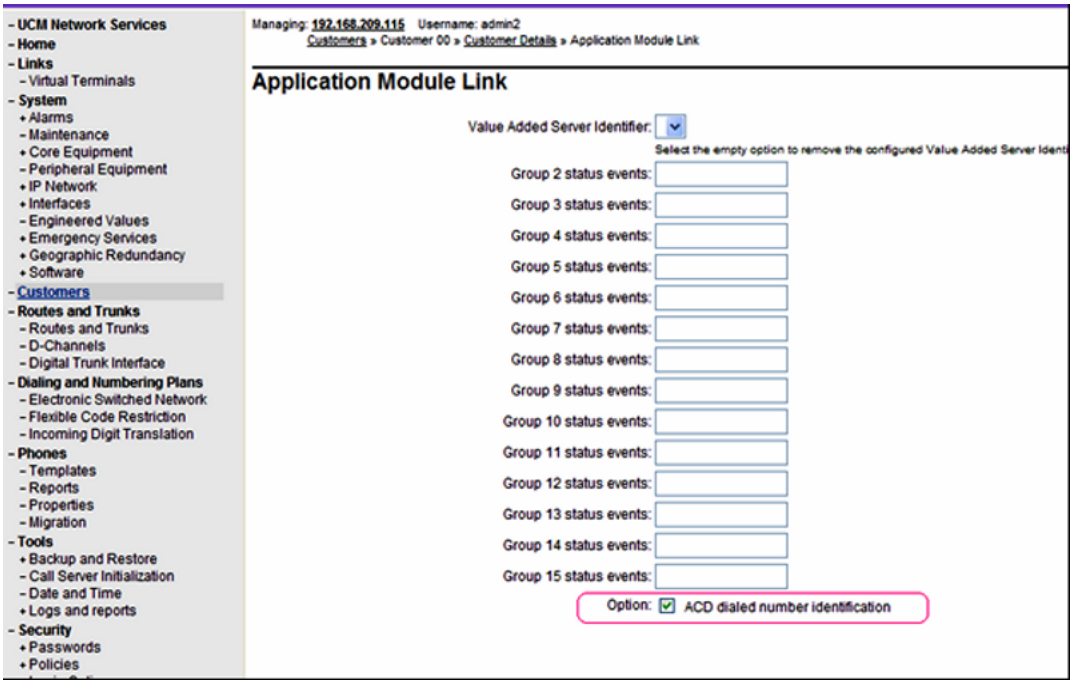


Figure 142: Application Module Link Web page

Enter the Value Added Service Identifier and Group status events information and click Save.

Attendant

The Attendant web page allows users to enable different options for a customer. Click **Attendant** on the Customers web page.

Select the appropriate check boxes in the Attendant Web page and click **Save**.

Call Detail Recording

Use the Call Detail Recording Web page to configure the Call Detail Recording data block for a customer. Click **Call Detail Recording** to open this Web page, as shown in Figure 143: Call Detail Recording Web page on page 226.

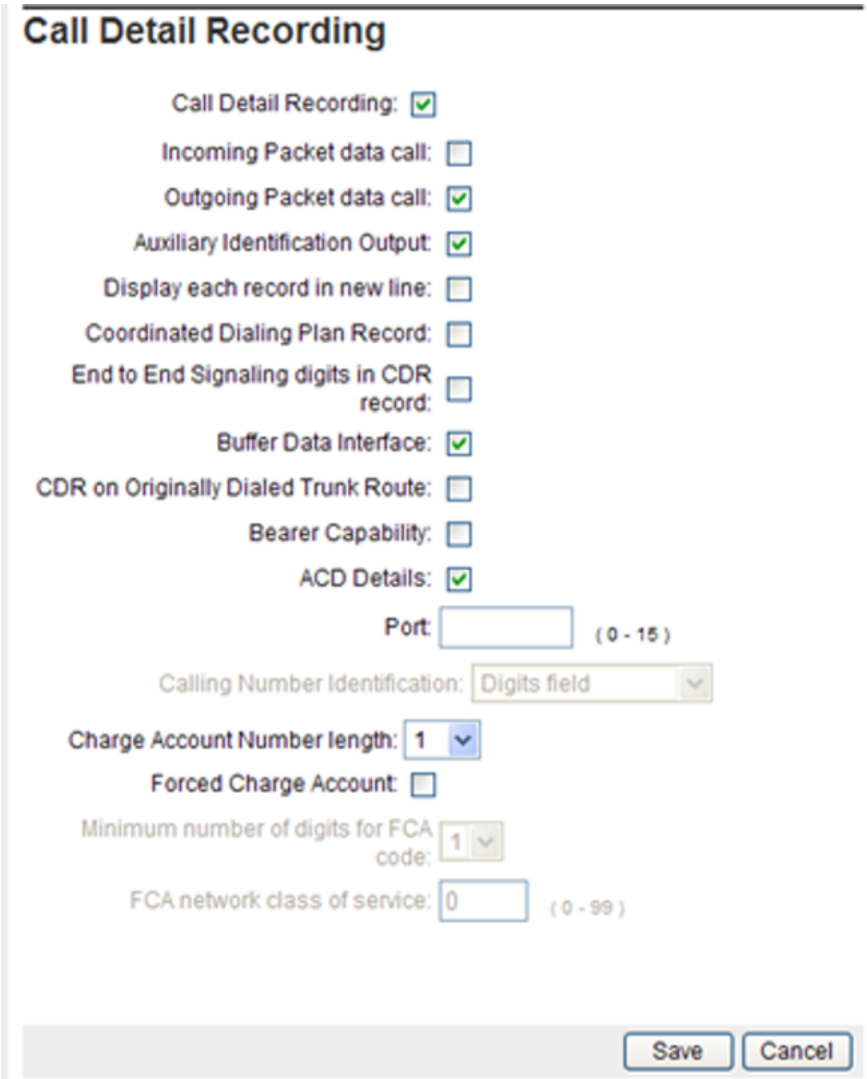


Figure 143: Call Detail Recording Web page

Enter the appropriate information and click **Save**.

Call Party Name Display

Use the Call Party Name Display Web page to configure the Call Party Name Display data block for a customer. Call Party Name Display names for Incoming Digit Conversion (IDC) are supported on this Web page. Click **Call Party Name Display** to open this Web page, as shown in Figure 144: Call Party Name Display Web page on page 227.

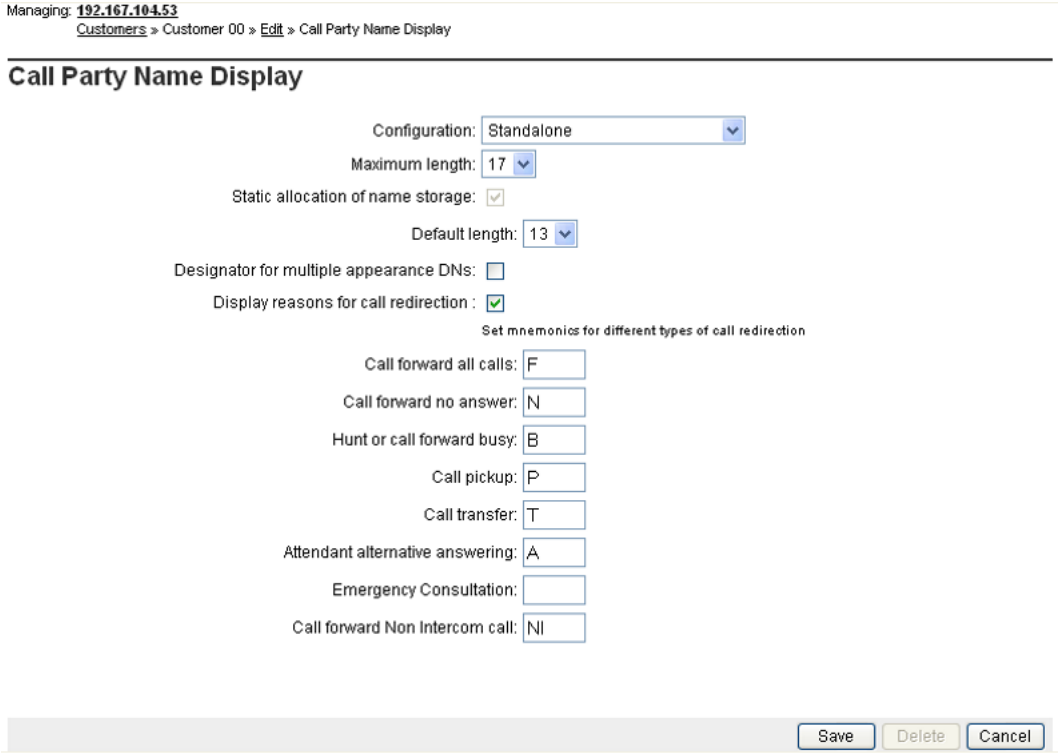


Figure 144: Call Party Name Display Web page

Enter the appropriate information and click **Save**.

Note:

The **Static Allocation of name storage** check box is selected and not editable if the BGD package is enabled.

Call Redirection

Use the Call Redirection Web page to configure the Call Redirection data block for a customer. Click **Call Redirection** to open this Web page, as shown in Figure 145: Call Redirection Web page on page 228.

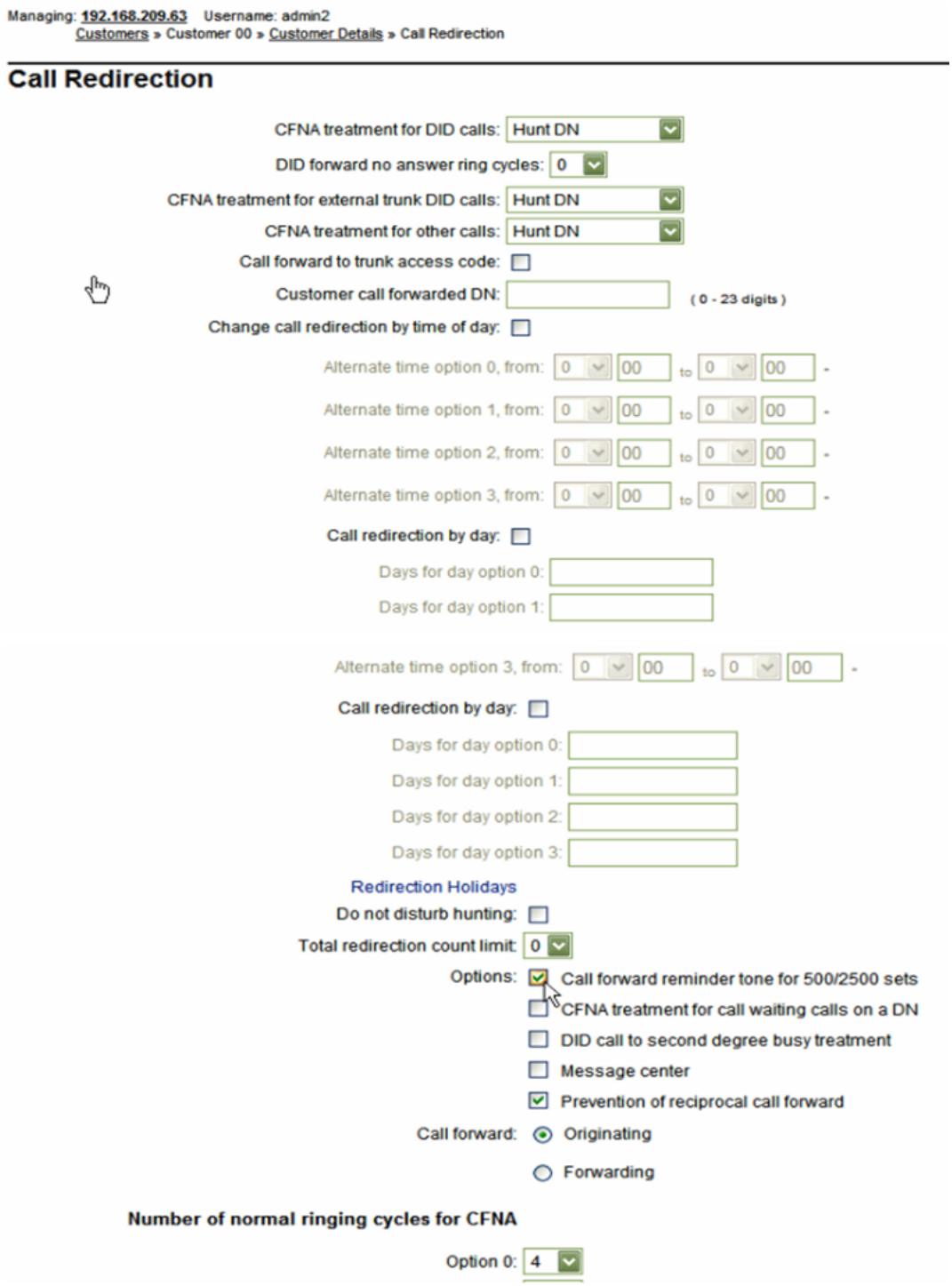


Figure 145: Call Redirection Web page

Enter the appropriate information, select appropriate options and click **Save**.

Click **Redirection Holidays** to open the Redirection Holidays Web page, as shown in Figure 146: Redirection Holidays Web page on page 229.

This Web page displays holiday redirections for existing dates and allows users to add, edit, or delete holidays.

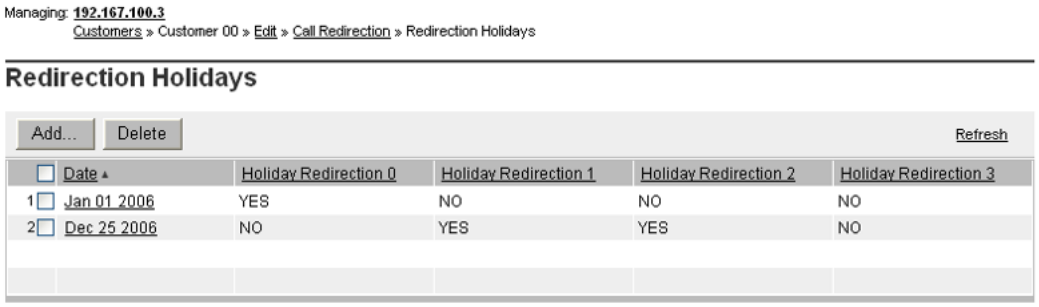


Figure 146: Redirection Holidays Web page

To add a holiday, click **Add**. The Add Date of Holiday Web page appears, as shown in Figure 147: Add Date of Holiday Web page on page 229.

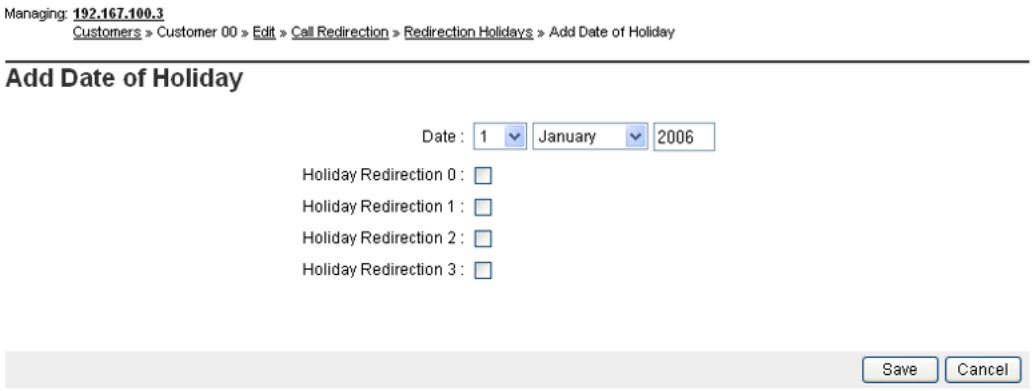


Figure 147: Add Date of Holiday Web page

Use this Web page to configure holiday redirections for a customer. Enter the holiday information and click **Save**.

Centralized Attendant Service

Use the Centralized Attendant Service Web page to centralize attendant services at a single location. To open this Web page, as shown in Figure 148: Centralized Attendant Service Web page on page 230, on the Edit Web page, click **Centralized Attendant Service**.

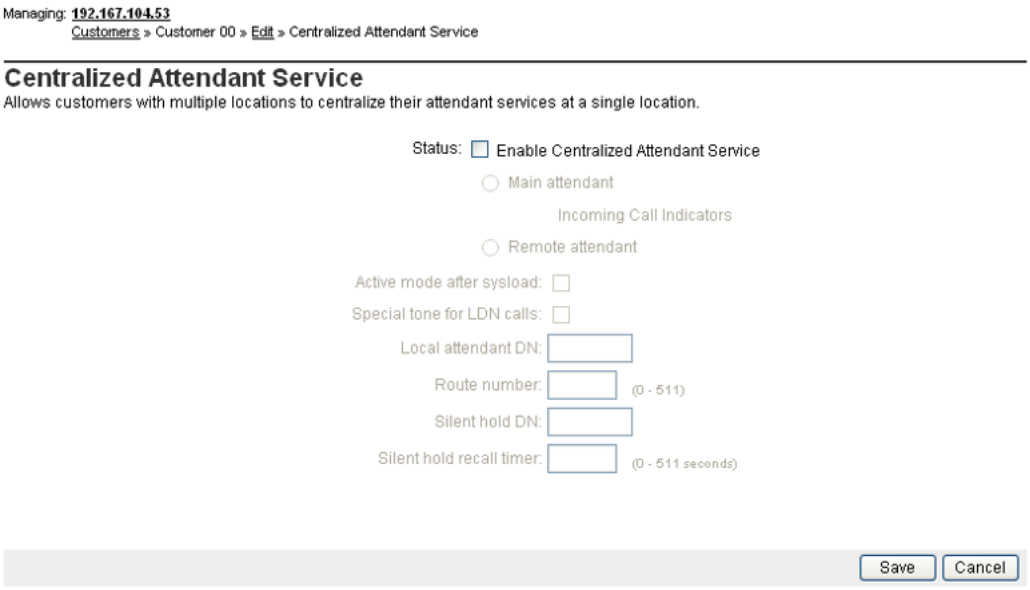


Figure 148: Centralized Attendant Service Web page

Enter the appropriate information and click **Save**.

To edit the Attendant Incoming Call Indicators, select the **Main attendant** radio button, and then click **Incoming Call Indicators**. The Edit Attendant ICI Web page appears, as shown in Figure 149: Edit Attendant ICI Web page on page 231.

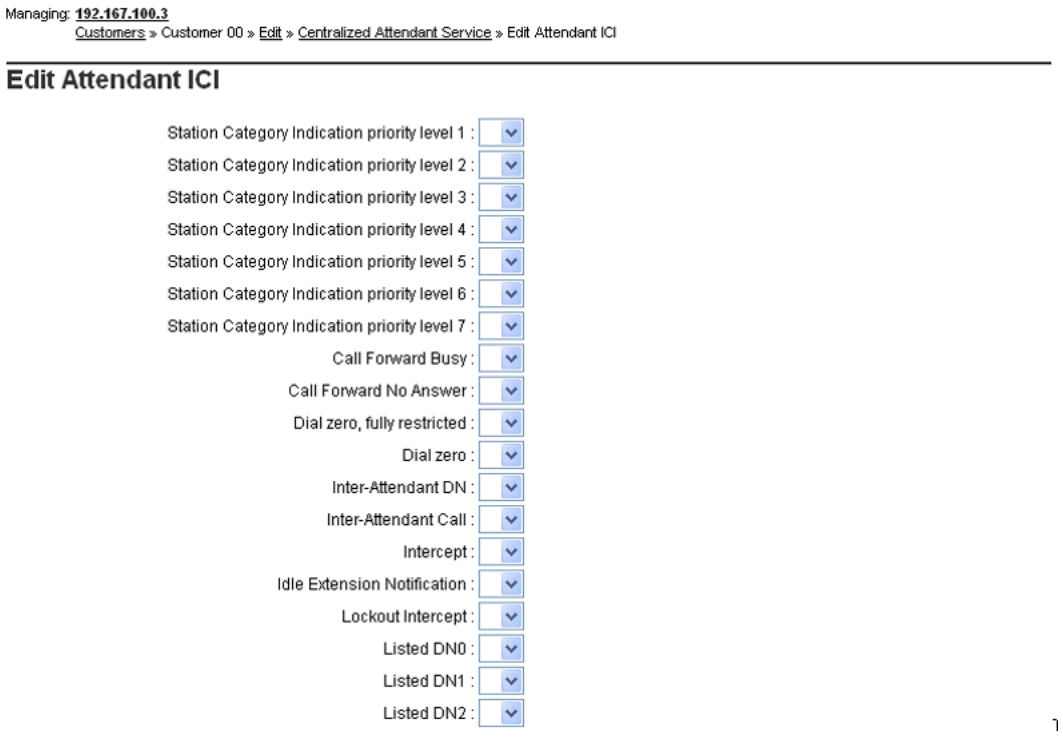


Figure 149: Edit Attendant ICI Web page

Enter the appropriate information and click **Save**.

Controlled Class of Service

Use the Controlled Class of Service Web page to configure the Controlled Class of Service data block for a customer. Click **Controlled Class of Service** to open this Web page, as shown in Figure 150: Controlled Class of Service Web page on page 232.

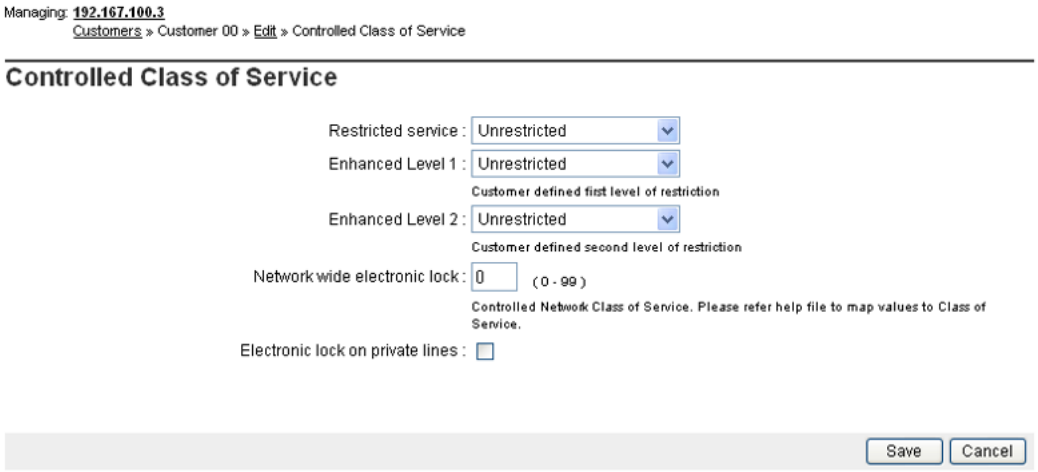


Figure 150: Controlled Class of Service Web page

Enter the appropriate information and click **Save**.

Flexible Feature Codes

Use the Flexible Feature Codes Web page to configure the Flexible Feature Codes (FFC) data block for a customer. To access the Flexible Feature Codes Web page, as shown in Figure 151: Flexible Feature Codes Web page on page 233, on the Edit Web page, click the **Flexible Feature Codes** link.

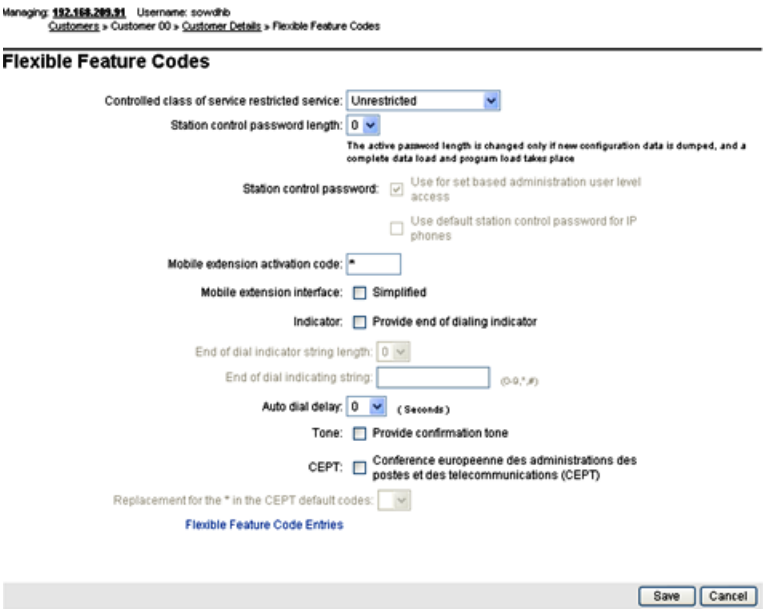


Figure 151: Flexible Feature Codes Web page

To configure Change Flexible Feature Code end-of-dialing indicator, select the **Change Flexible Feature Code end-of-dialing indicator** checkbox.

Enter the appropriate information and click **Save**.

Flexible Feature Code Entries

To access Flexible Feature Code Entries click the **Flexible Feature Code Entries** hyperlink. The Search for Flexible Feature Code Entries Web page appears as shown in Figure 152: Search for Flexible Feature Code Entries Web page on page 234.

Note:

To access Flexible Feature Code Entries Web page for a Customer the FCC data block must be configured, see Configuring Flexible Feature Codes on page 235. If you click the **Flexible Feature Code Entries** hyperlink before you configure the FCC data block, the message *"FCC Block is not configured. Click on [OK] to configure the FCC block for the customer."* appears. Click **OK** to automatically configure the FCC data block and open the Flexible Feature Code Entries Web page.

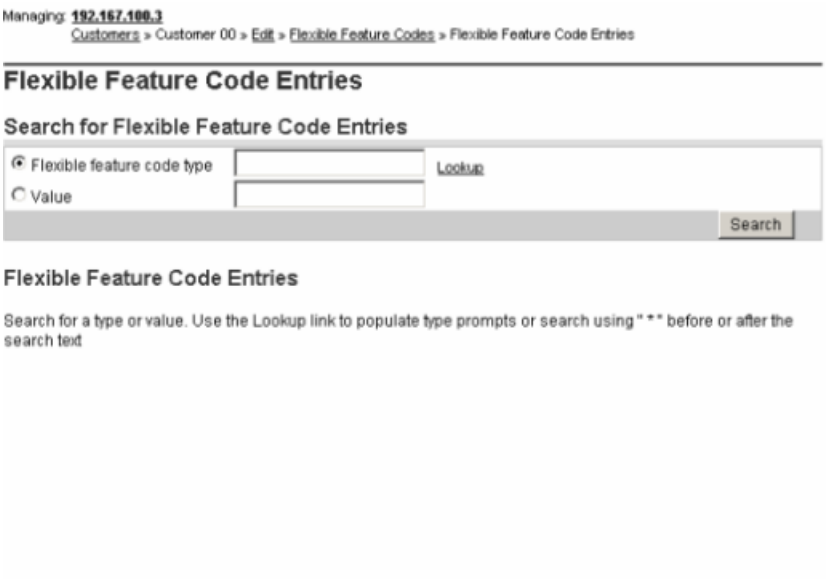


Figure 152: Search for Flexible Feature Code Entries Web page

To search for specific Flexible Feature Codes, follow the steps in Searching for Flexible Feature Codes on page 234.

Searching for Flexible Feature Codes

1. Click the **Flexible feature code type** radio button to activate search for Flexible Feature Codes.
2. Click the **Look up** hyperlink.

   The Flexible Feature Code Lookup pop up window appears.
3. Click the corresponding check boxes for the required features, and then click **Assign**.

   The selected feature prompt names appear in the **Specific Feature Code type** input box.
4. Click **Search** . The datagrid lists only the codes for the selected feature.

To search for Flexible Feature Codes by Value, follow the steps in Searching for Flexible Feature Codes by Value on page 234.

Searching for Flexible Feature Codes by Value

1. Enter the configured Flexible Feature Code value in the **Value** input box.
2. Check the **Value** radio button, to enable the **Search** button.
3. Click the **Search** button.

   The flexible feature code, type, and the value appear in the datagrid.

To search for Flexible Feature Codes using Advanced Search, follow the steps in Searching for Flexible Feature Codes (Advanced) on page 235.

Searching for Flexible Feature Codes (Advanced)

1. Enter the wildcard character * before or after the search text in the **Flexible feature code type** input box.
2. Check the **Flexible feature code type** radio button to enable the **Search** button.
3. Click the **Search** button.

   All the flexible feature code types with the configured values that match the given search text appear in the datagrid.

To configure Flexible Feature Codes for a customer, follow the steps in Configuring Flexible Feature Codes on page 235.

Configuring Flexible Feature Codes

1. In the Flexible Feature Codes Web page, select **Flexible Feature Confirmation Tone** and **Conference European Des Postes Tel (CEPT) defaults**.

   The **Replacement for * in CEPT default codes** appears as a sub prompt for **Conference European Des Postes Tel (CEPT) defaults** prompt. Enable only if **Conference European Des Postes Tel (CEPT) defaults** prompt is selected.
2. To complete the configuration, click **Save** .
3. Click **Cancel** to cancel the action. The Edit Web page appears.

To add Flexible Feature Codes to the Customer, follow the steps in Adding Flexible Feature Codes on page 235.

Adding Flexible Feature Codes

1. Click the **Flexible Feature Code Entries** hyperlink on the Flexible Feature Code Web page.

   The Flexible Feature Code Entries Web page appears.
2. Click **Add** on the Flexible Feature Code Entries Web page.

   The Add Flexible Feature Code Web page appears.
3. Click the **Look up** hyperlink adjacent to the **Flexible feature code type** input box.

   The Flexible Feature Code Lookup popup window appears and lists all of the Flexible Feature Codes.
4. Click a **Flexible Feature Code** to add it to the **Flexible feature code type** input box.
5. Enter a value in the **Value** box.
6. Click **Save** .

   The new Flexible Feature Code appears on the Flexible Feature Code Entries Web page.

Features web page

Use the **Features** Web page to configure the Features data block for a customer. Click **Features** to open this Web page, as shown in Figure 153: Features Web page on page 237.

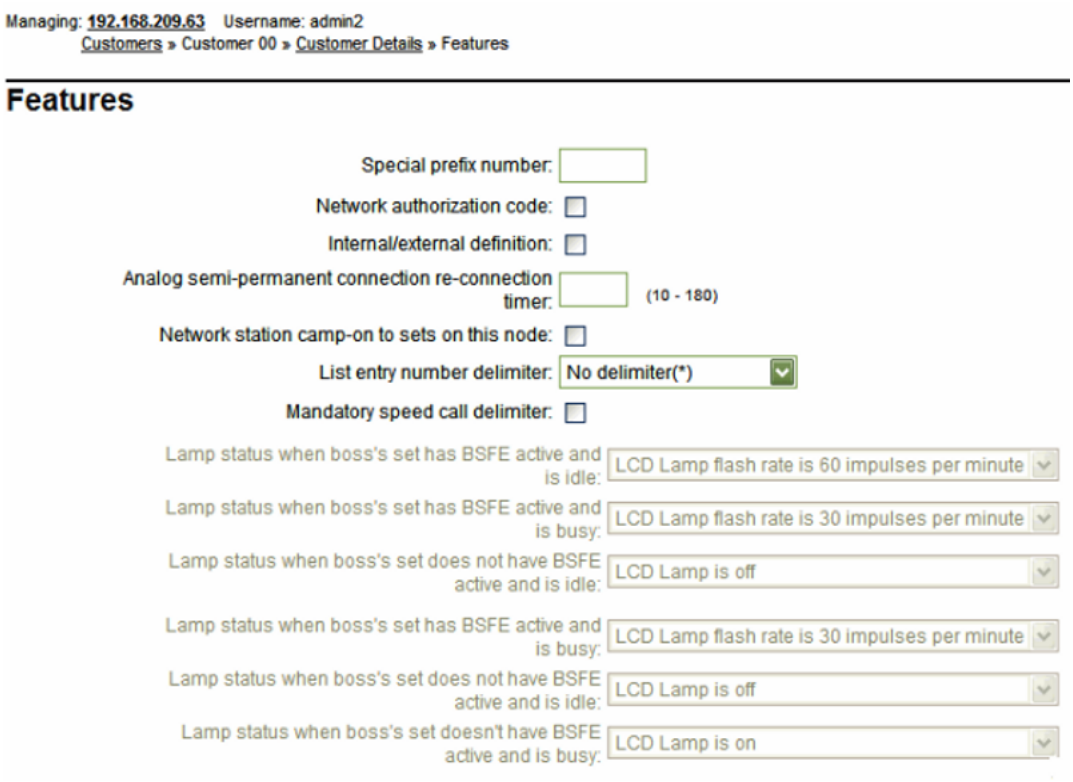


Figure 153: Features Web page

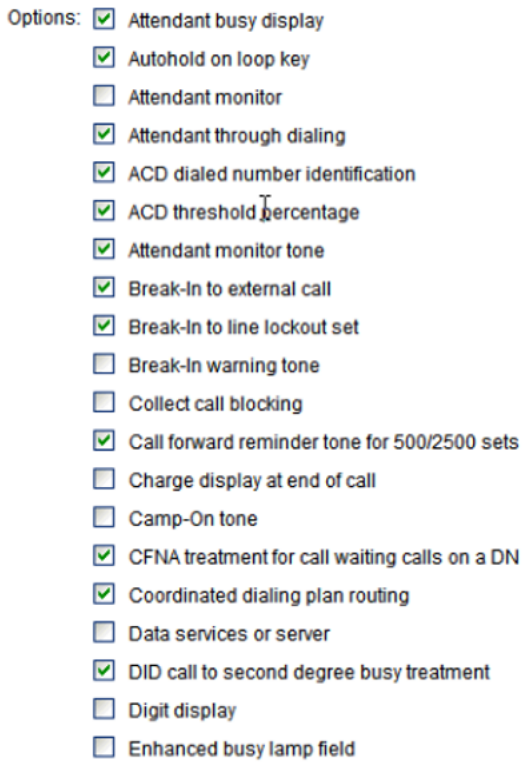


Figure 154: Feature options

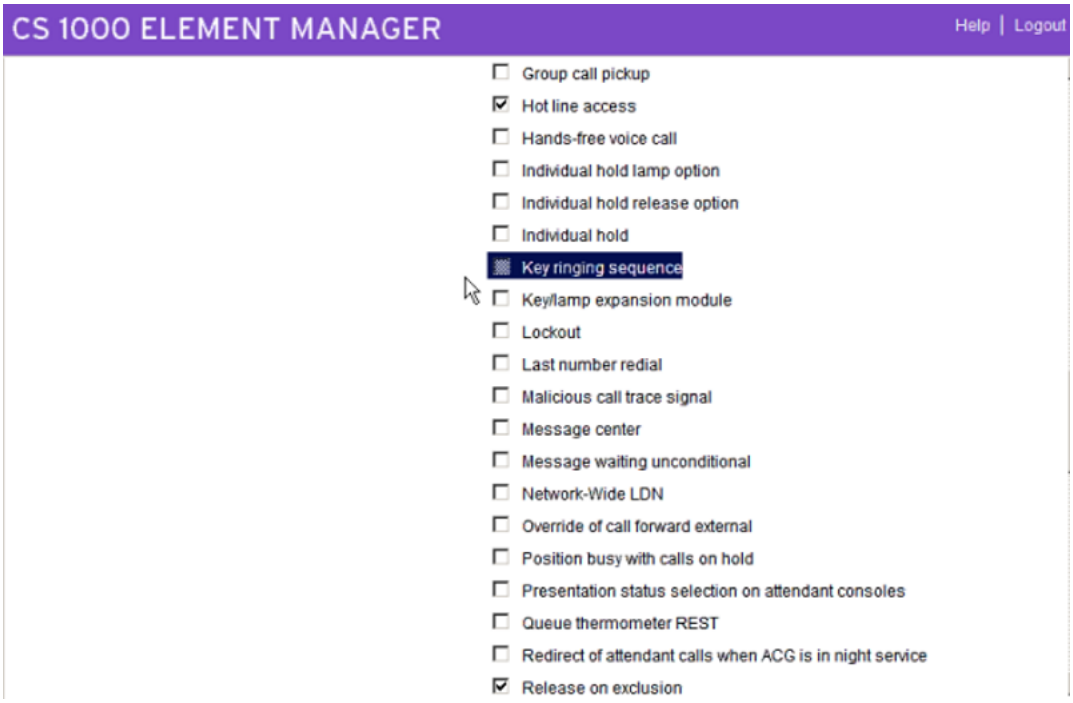


Figure 155: Feature options (Cont'd)

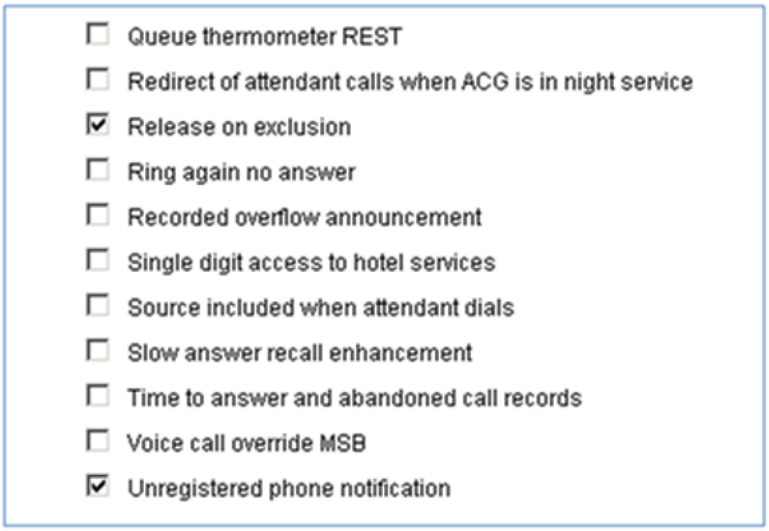
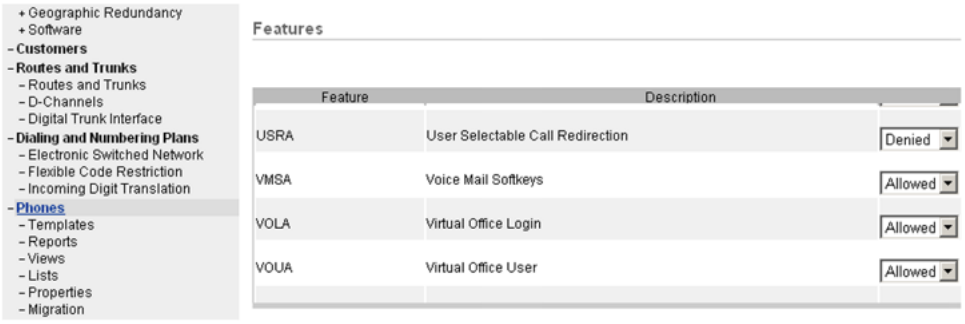


Figure 156: Feature options (Cont'd)



Enter the appropriate information, select the appropriate options, and then click **Save**.

Media Services Properties

Use the Media Services Properties Web page to view the Media Services Properties for a customer.

Figure 157: Media Services Properties Web page

Listed Directory Numbers

Use the Listed Directory Numbers Web page to configure the Listed Directory Numbers data block for a customer. Click **Listed Directory Numbers** to open this Web page, as shown in Figure 158: Listed Directory Numbers Web page on page 240.

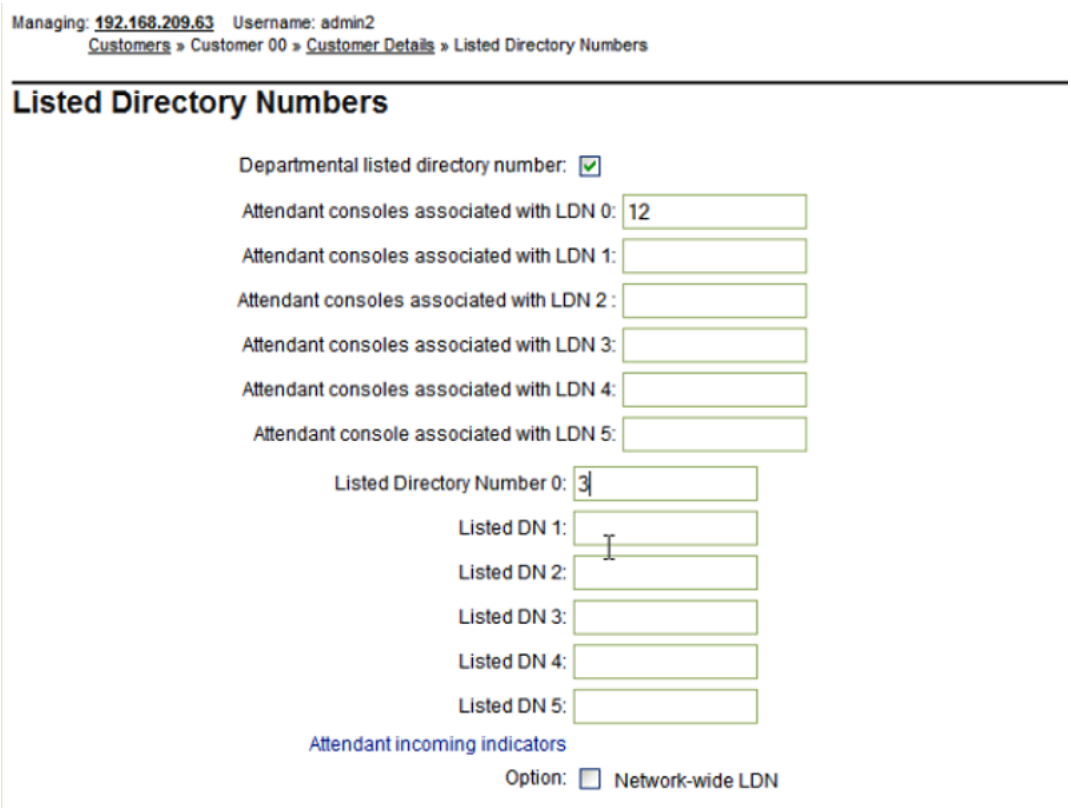


Figure 158: Listed Directory Numbers Web page

To configure attendant consoles associated with Listed Directory Numbers, select the **Departmental listed directory number** checkbox.

Enter the appropriate information and click **Save**.

Mobile Service Directory Number

Use the Mobile Service Directory Numbers Web page to view, edit, add, and delete Mobile Service Directory Numbers. Click **Mobile Service Directory Numbers** to open this Web page, as shown in Figure 159: Mobile Service Directory Numbers Web page on page 241. For more information about Mobile Directory Service Numbers and Mobile Extension, refer to *Avaya Features and Services Fundamentals - Book 4 of 6, NN43001-106-B4*.

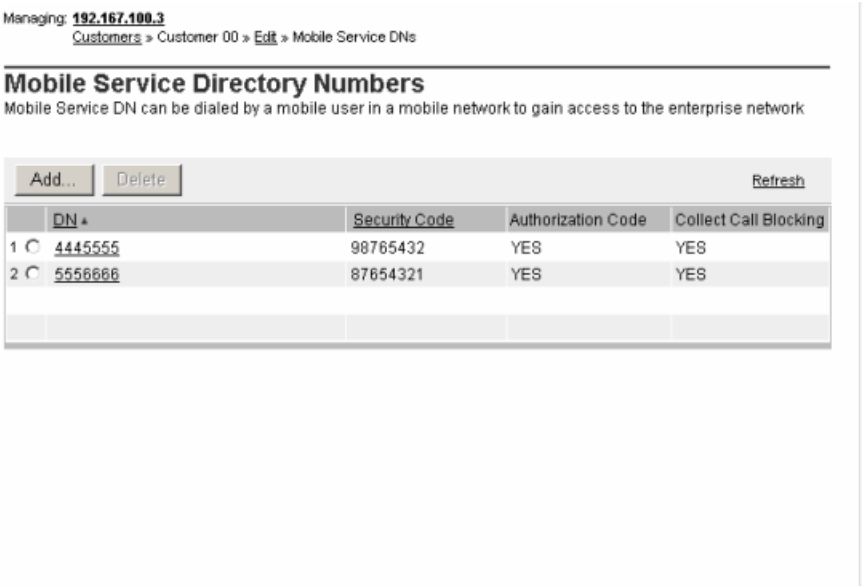


Figure 159: Mobile Service Directory Numbers Web page

ISDN and ESN Networking

Use the ISDN and ESN Networking Web page to configure the Integrated Services Digital Network (ISDN) and ESN Networking data block for a customer. To access the ISDN and ESN Networking Web page, click **Customers , Customer 00 , Customer Details , ISDN and ESN Networking**. The page appears as shown in Figure 160: ISDN and ESDN Networking Web page on page 241.

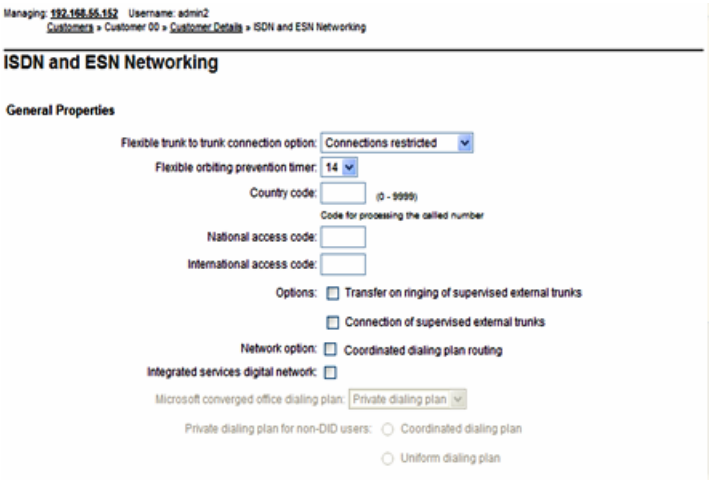


Figure 160: ISDN and ESDN Networking Web page

Enter the appropriate information and click **Save**.

When ISDN is enabled in ISDN and ESN Networking page, the Microsoft converged office dialing plan fields become active and editable as shown in the following figure.

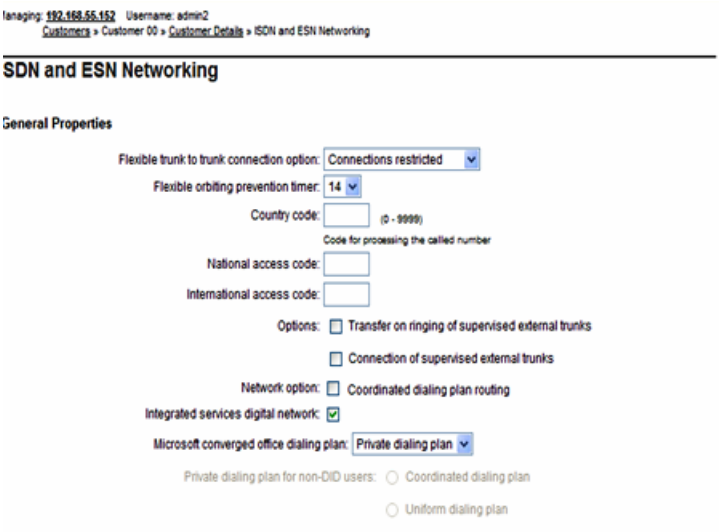


Figure 161: ISDN and ESDN Networking Web page with ISDN enabled

When ISDN is enabled and the Microsoft converged office dialing plan is in Mixed Mode, private dialing plan fields are become active and editable as shown in the following figure.

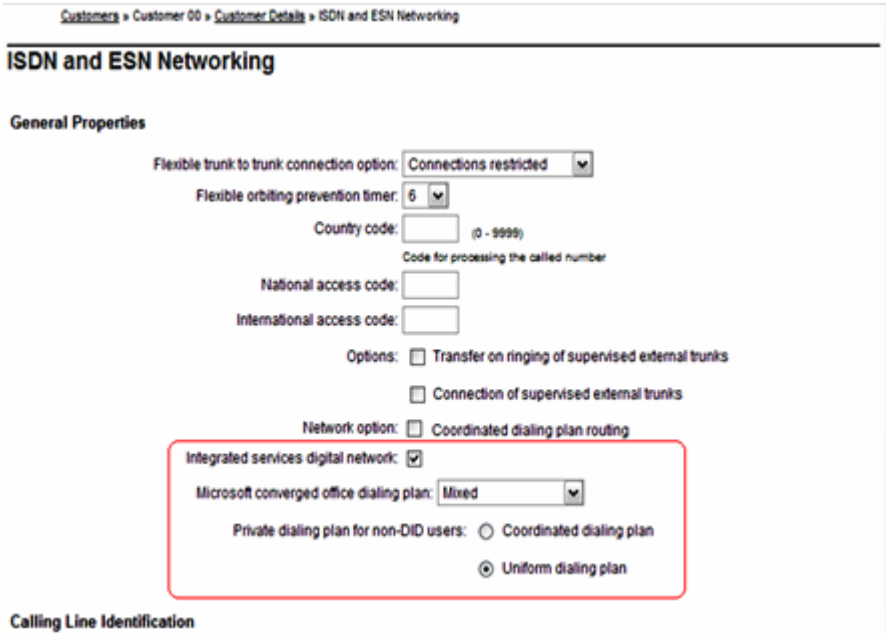


Figure 162: Private dialing plan

To configure Calling Line Identification (CLID) parameters, click **Calling Line Identification Entries**. The Calling Line Identification Entries Web page appears, as shown in Figure 163: Calling Line Identification Entries Web page on page 243.

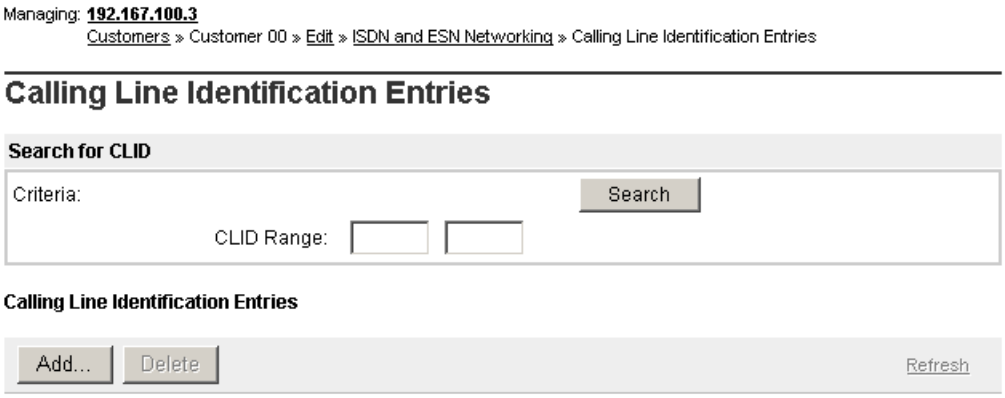


Figure 163: Calling Line Identification Entries Web page

To search for a CLID, enter the **CLID Range** and click **Search**.

To add a CLID, click **Add**. The New Calling Line Identification Web page appears, as shown in Figure 164: New Calling Line Identification Web page on page 243.

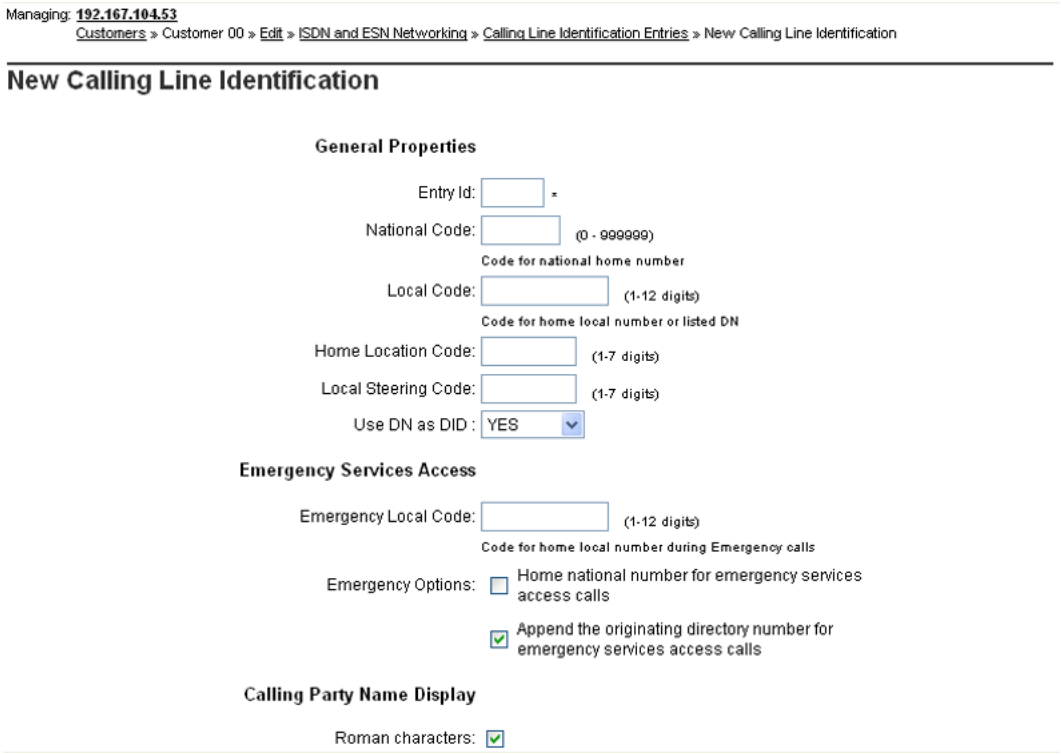


Figure 164: New Calling Line Identification Web page

Enter the parameters for the new CLID and click **Save**.

Night Service

Use the Night Service Web page to configure the Night Service data block for a customer. Click **Night Service** to open this Web page, as shown in Figure 165: Night Service Web page on page 244.

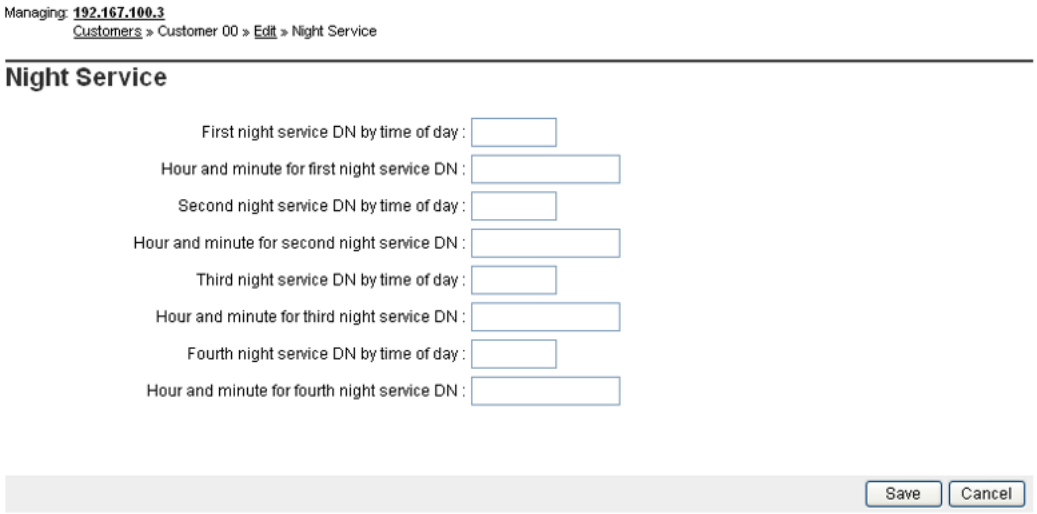


Figure 165: Night Service Web page

Enter the appropriate information and click **Save**.

Feature Packages

Use the Feature Packages Web page to view and edit the parameters associated with feature packages. Click **Feature Packages** to open this Web page.

Click the plus sign located to the left of the Feature Packages heading to expand the feature packages, as shown in Figure 166: Feature Packages Web page on page 245.

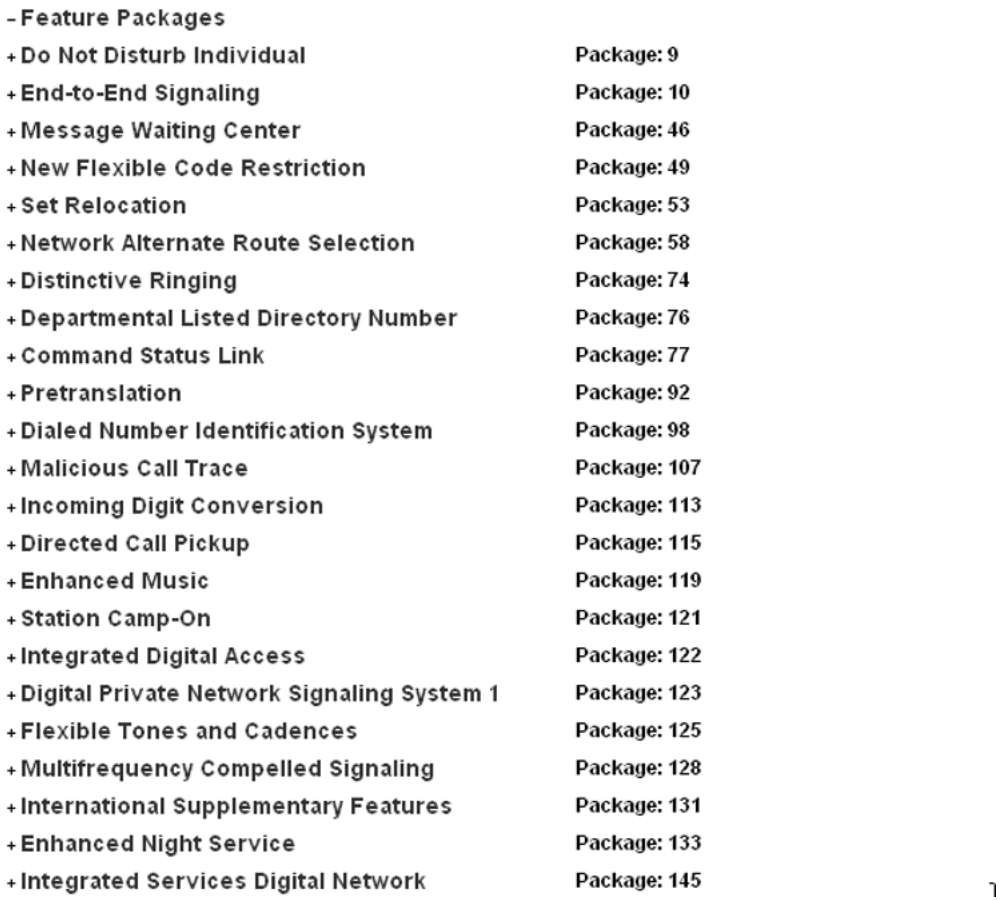


Figure 166: Feature Packages Web page

Enter the Media services routing number. Choose the Numbering plan identifier and Type of number from the respective drop-down lists and then click **Save**.

Note:

The only feature packages whose parameters can be viewed and edited are those that have been enabled on the system. Feature packages cannot be removed or added from Element Manager.

Click the plus sign located to the left of the feature package name to view and edit the parameters associated with the feature package. For feature packages that are not equipped for the customer, Element Manager includes a button labeled **To Order**. This button provides a link to information on how to order the feature package.

Enter the appropriate information and click **Save**.

Important:

When you configure M3900 System Initiated Language (Package 386) and Japanese is the default language, you must explicitly configure the set-to-set-messages (MSG 1 to MSG10). Otherwise, the customer information does not load or appear after you click **Submit**.

Intercept Treatments

Use the Intercept Treatments Web page to configure the Intercept Treatments data block for a customer. Click **Intercept Treatments** to open this Web page, as shown in Figure 167: Intercept Treatments Web page on page 246.

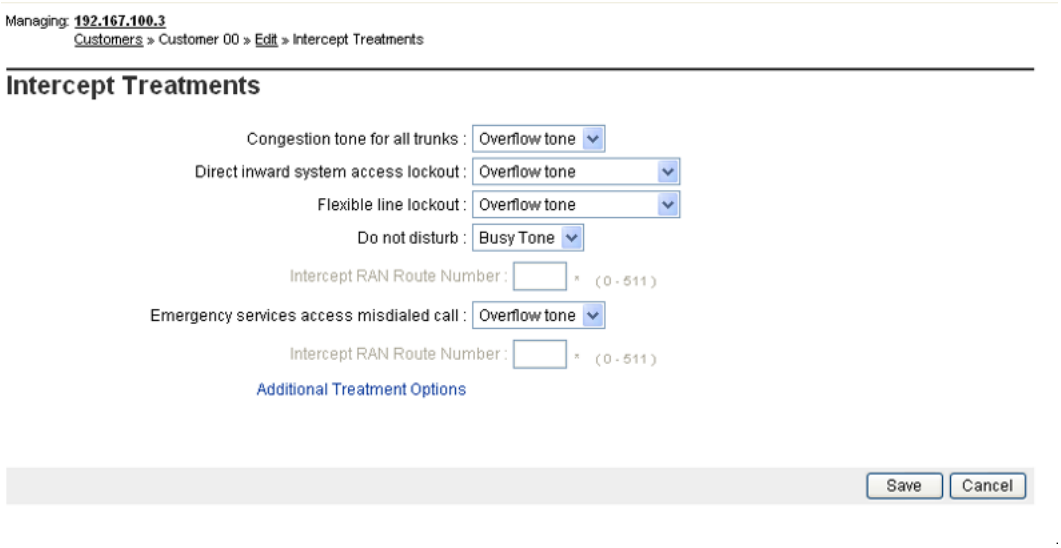


Figure 167: Intercept Treatments Web page

Enter the appropriate information and click **Save**.

To configure additional prompts for Intercept Treatments, click **Additional Treatment Options** . The Intercept Treatments Options Web page appears, as shown in Figure 168: Intercept Treatments Options Web page on page 247.

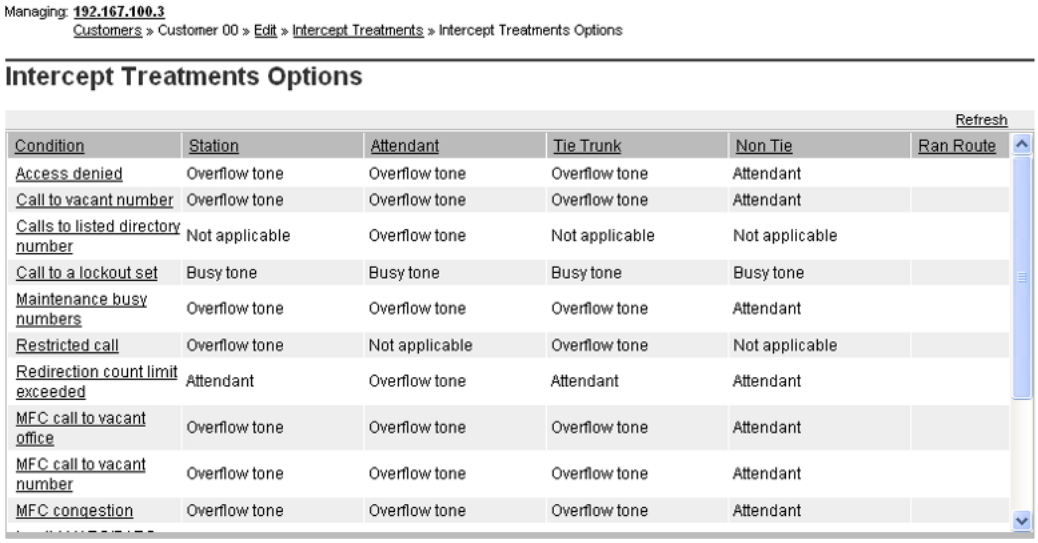


Figure 168: Intercept Treatments Options Web page

To edit an Intercept Treatment for a customer, click the **Condition**. The Edit Web page for that Condition appears, as shown in Figure 169: Edit Condition Web page on page 247.

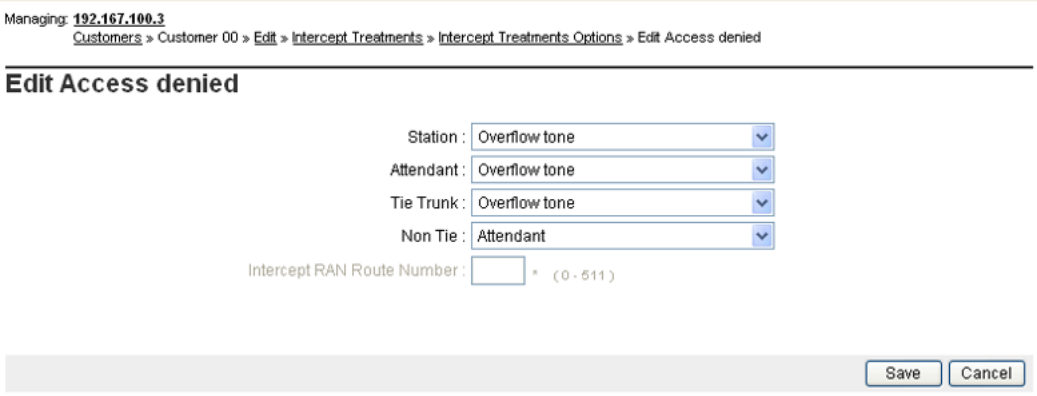


Figure 169: Edit Condition Web page

Enter the appropriate information and click **Save**.

Multi Party Operations

Use the Multi Party Operations Web page to configure the Multi Party Operations data block for a customer. Click **Multi Party Operations** to open this Web page, as shown in Figure 170: Multi Party Operations Web page on page 248.

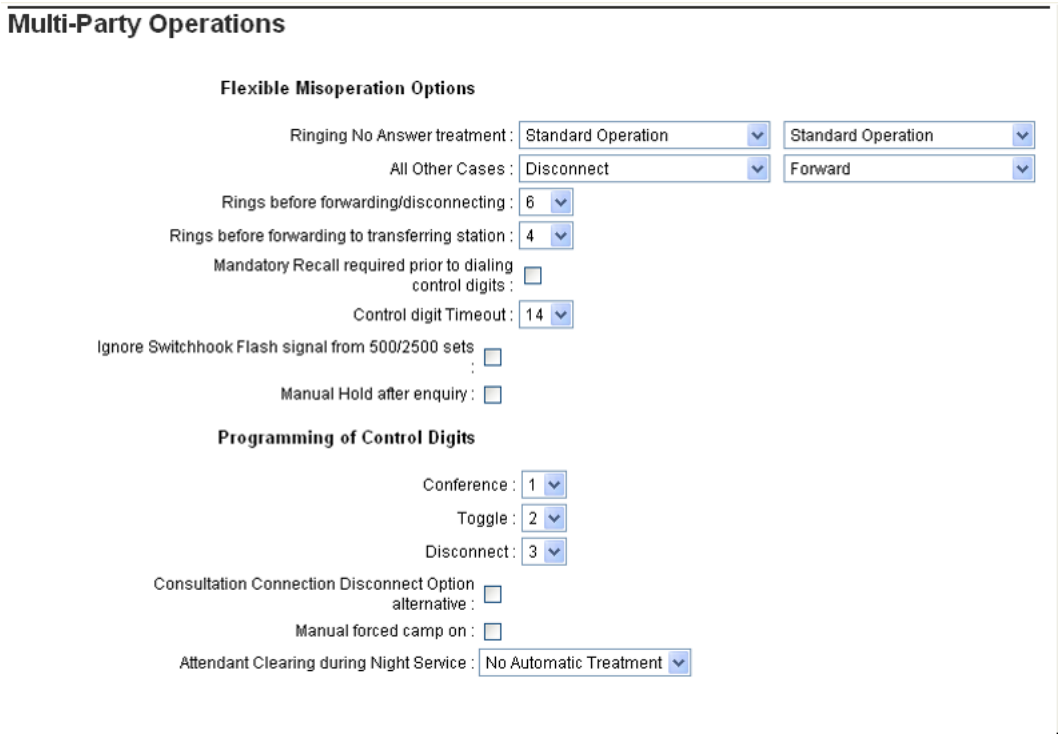


Figure 170: Multi Party Operations Web page

Enter the appropriate information and click **Save**.

Recorded Overflow Announcement

Use the Recorded Overflow Announcement Web page to configure the Recorded Overflow Announcement data block for a customer. Click **Recorded Overflow Announcement** to open this Web page, as shown in Figure 171: Recorded Overflow Announcement Web page on page 249.

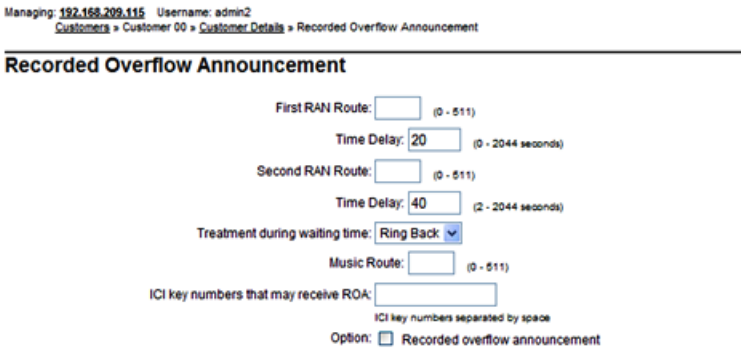


Figure 171: Recorded Overflow Announcement Web page

Enter the appropriate information and click **Save**.

SIP Line Service

The SIP Line Service package 417 must be equipped in order to enable SIP Line Service on CS 1000 system.

The SIP Service Web page allows users to configure SIP Line Service parameters.

You can enable or disable SIP Line Service by clicking the check box. Once the service is enabled, the rest of the SIP Line service parameters are displayed. The SIP root domain is a mandatory field when SIP Line service is enabled. The User Agent DN is an optional field but when this DN prefix is configured in the customer page, it is used to build the HOT U key information on the Phones Web page for SIPL Phones.

For more information, see *Avaya SIP Line Fundamentals, NN43001-508*.

Timers

Use the Timers Web page to configure the Timers data block for a customer. Click **Timers** to open this Web page, as shown in Figure 172: Timers Web page on page 250.

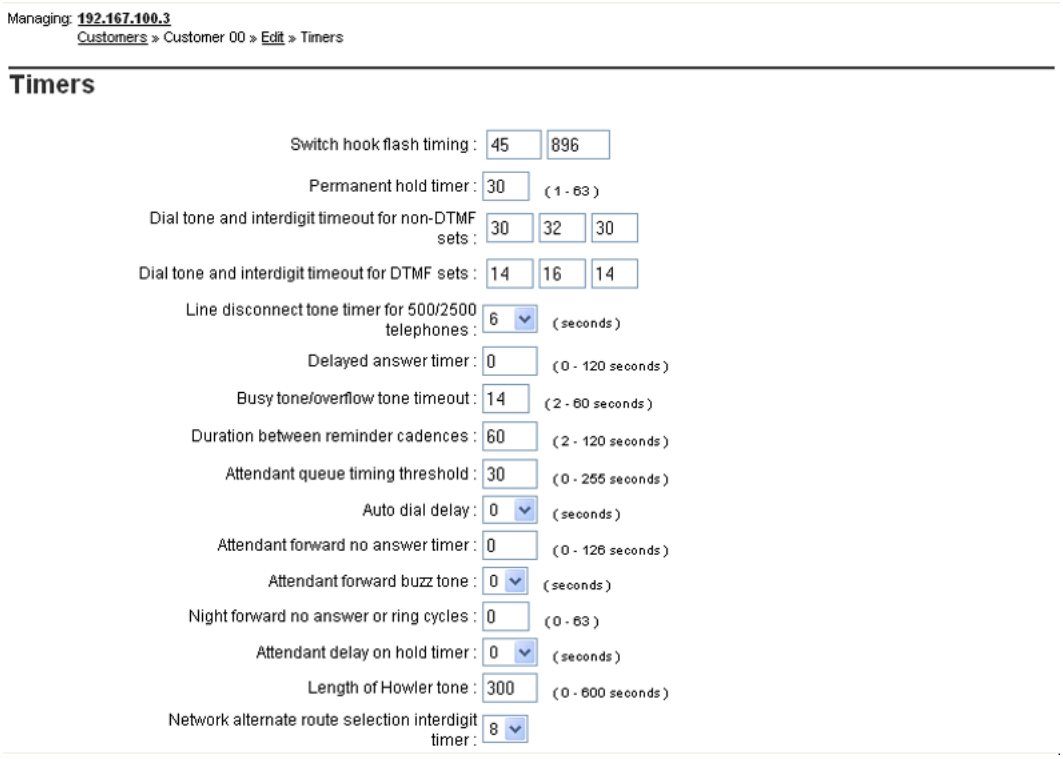


Figure 172: Timers Web page

Enter the appropriate information and click **Save**.

Note:

The **Attendant forward no answer timer** and **Attendant forward buzz tone** must be even numbers.

Route and Trunk Configuration

There are three options in the **Routes and Trunks** branch of the Element Manager navigator.

Routes and Trunks

Click the **Routes and Trunks** link on the **Routes and Trunks** branch of the Element Manager navigator to open the Routes and Trunks Web page, as shown in Figure 173: Routes and Trunks Web page on page 251. Use this Web page to view information about existing customers, routes, and trunks.

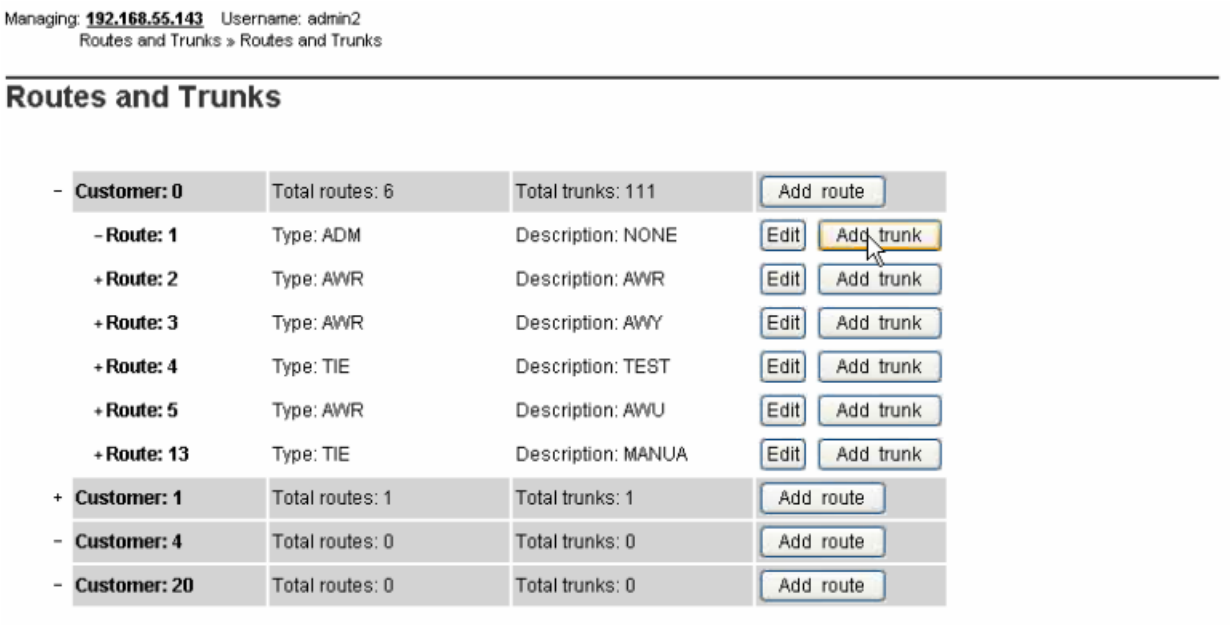


Figure 173: Routes and Trunks Web page

This Web page also contains buttons that link to additional Web pages. Follow these links to

- add a new route
- edit route data
- add a new trunk
- edit trunk data
- delete multiple trunks

Route Properties

Click the **Edit** button beside a Route row to open the Route Property Configuration Web page for the selected customer and route. See Figure 174: Route Property Configuration Web page on page 252.

Note:

If there are a large number of routes or trunks, this Web page can be slow to load.

The information entered in the **Basic Configuration** section of this Web page corresponds to Route Data Block information traditionally configured using LD 16 - Route Data Block.

Note:

H.323 and SIP must not use the same route.

For information about configuring routes, see *Avaya IP Peer Networking Installation and Commissioning, NN43001-313* .

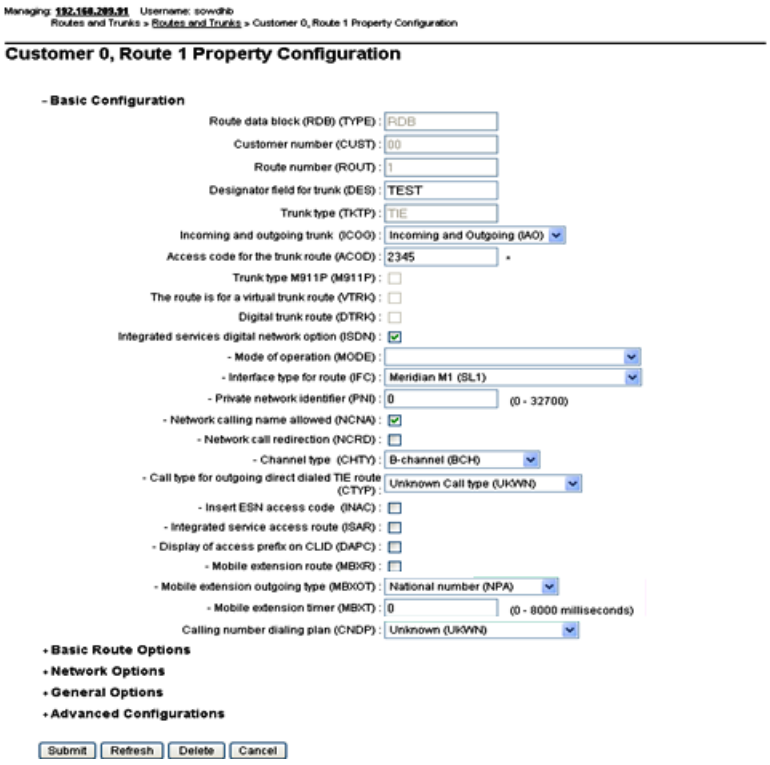


Figure 174: Route Property Configuration Web page

Basic Configuration

In the **Basic Configuration** section of this Web page (see Figure 175: Basic Configuration for routes on page 253), the following functions can be performed:

- Assign a **Route Number** (ROUT) using the drop-down list.
- Enter a **Designation** (DES) for the route.
- Select a **Trunk Type** (TKTP) from the drop-down list.
- Use the drop-down list to indicate that the trunk is **Incoming and/or Outgoing** (ICOG).
- Assign an **Access Code** (ACOD) to the trunk route.

Element Manager may request that users enter data for additional parameters, depending on what is entered in the Basic Configuration fields. Choices in the drop-down lists for every parameter in the Basic Configuration fields are determined by the data entered above that field.

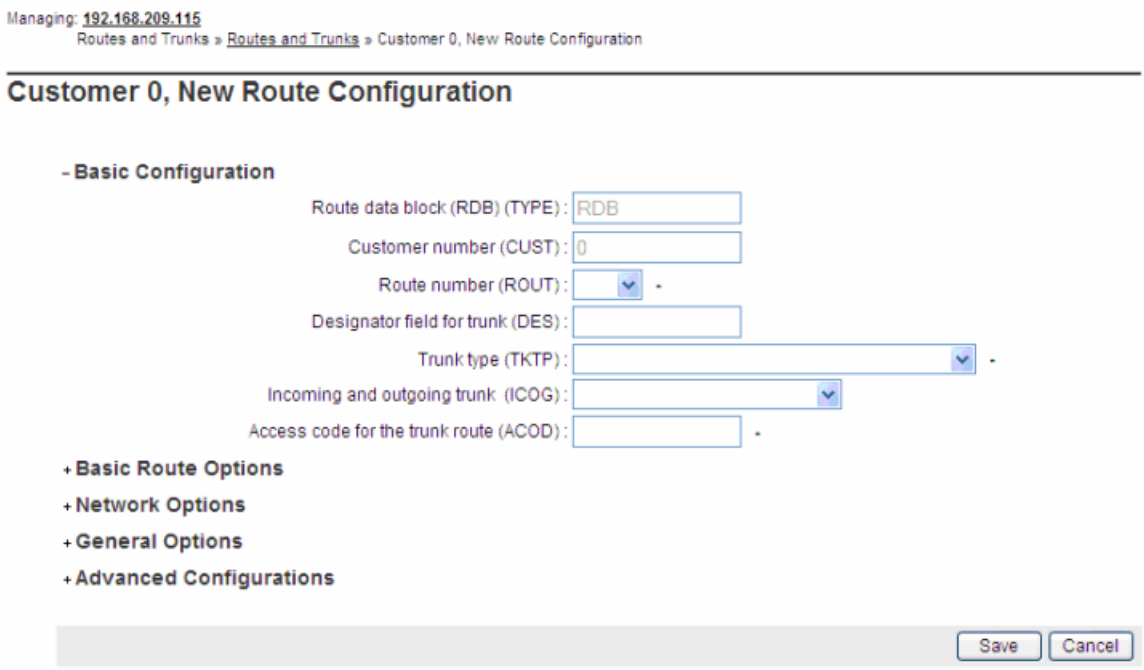


Figure 175: Basic Configuration for routes

To save changes made in this section, click **Submit** at the bottom of the Route Property Configuration Web page.

Basic Route Options

In the Basic Route Options section (see Figure 176: Basic Route Options configuration on page 254), use the check boxes to activate the following options for this route:

- Billing Number Required (BILN)
- Call Detail Recording (CDR)
- Controls or timers (CNTL)
- Conventional (TIE trunk only) (CNVT)
- Incoming DID Digit Conversion (IDC)
- Process Notification Networked Calls (PNNC)

In addition, use the drop-down list to select a Multi-frequency Compelled or MFC Signaling (MFC) type.

Note:

The route used in this example is a TIE trunk route. The inputs requested by Element Manager vary depending on the responses to earlier input requests, including Trunk Type (TKTP).

Depending on which boxes are selected in the preceding list, Element Manager requests that users enter data for additional parameters, as shown in Figure 176: Basic Route Options configuration on page 254.

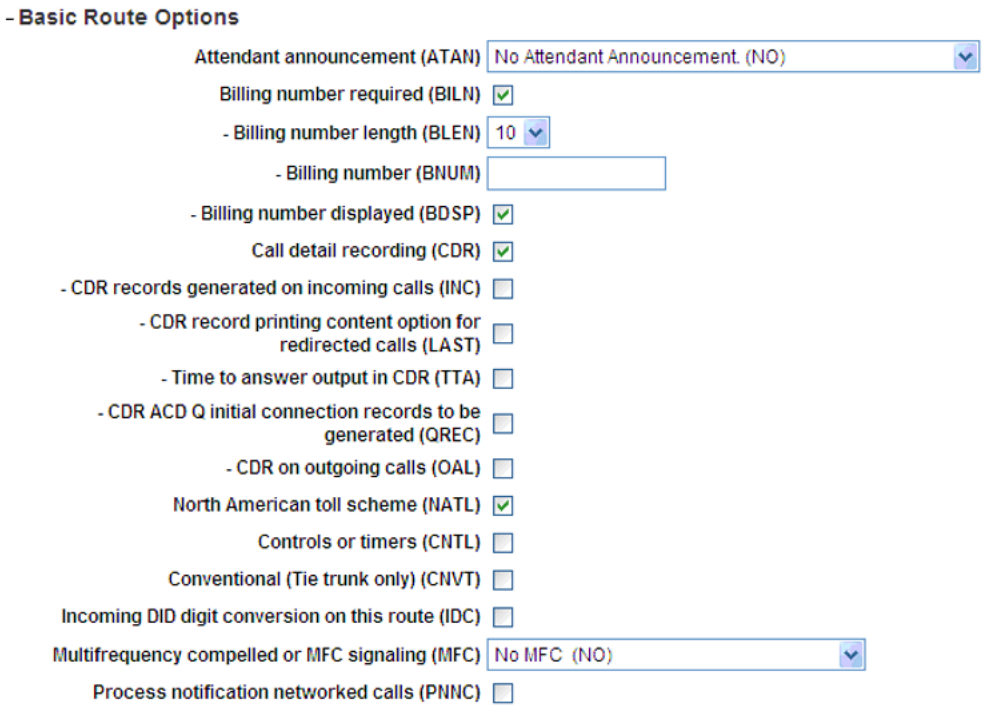


Figure 176: Basic Route Options configuration

To save changes made in this section, click **Submit** at the bottom of the Route Property Configuration Web page.

Network Options

Figure 177: Network Options for routes on page 255 provides an example of the input requested in the **Network Options** section for the route shown in Figure 174: Route Property Configuration Web page on page 252. The actual input that Element Manager requests varies depending on the type of route and the responses to earlier input requests.

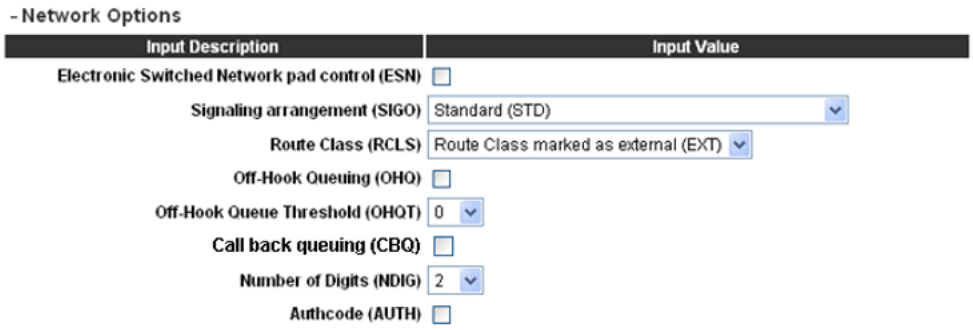


Figure 177: Network Options for routes

To save changes made in this section, click **Submit** at the bottom of the Route Property Configuration Web page.

General Options

Figure 178: General Options for routes on page 255 provides an example of the input requested in the **General Options** section for the route shown in Figure 174: Route Property Configuration Web page on page 252. The actual input that Element Manager requests varies depending on the type of route and the responses to earlier input requests.

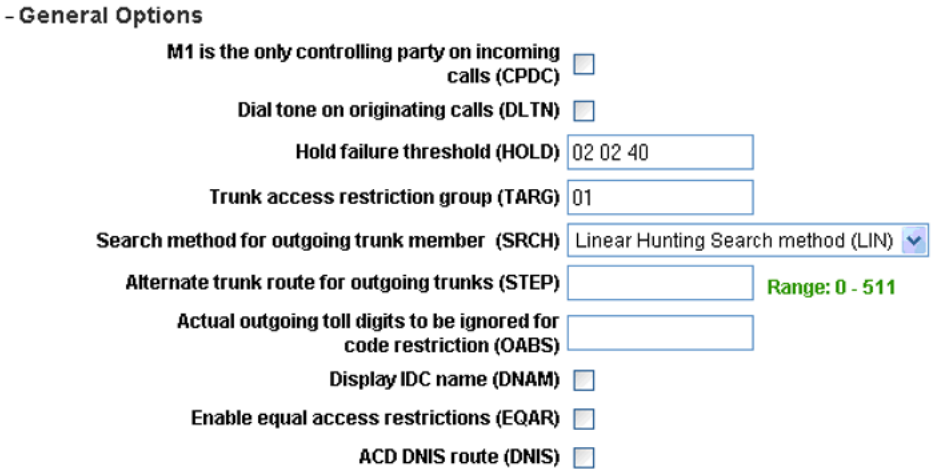


Figure 178: General Options for routes

To save changes made in this section, click **Submit** at the bottom of the Route Property Configuration Web page.

Advanced Configurations

Figure 179: Advanced Configurations for routes on page 256 provides an example of the input requested in the **Advanced Configurations** section for the route shown in Figure 174: Route

Property Configuration Web page on page 252. The actual input that Element Manager requests varies depending on the type of route and the responses to earlier input requests.

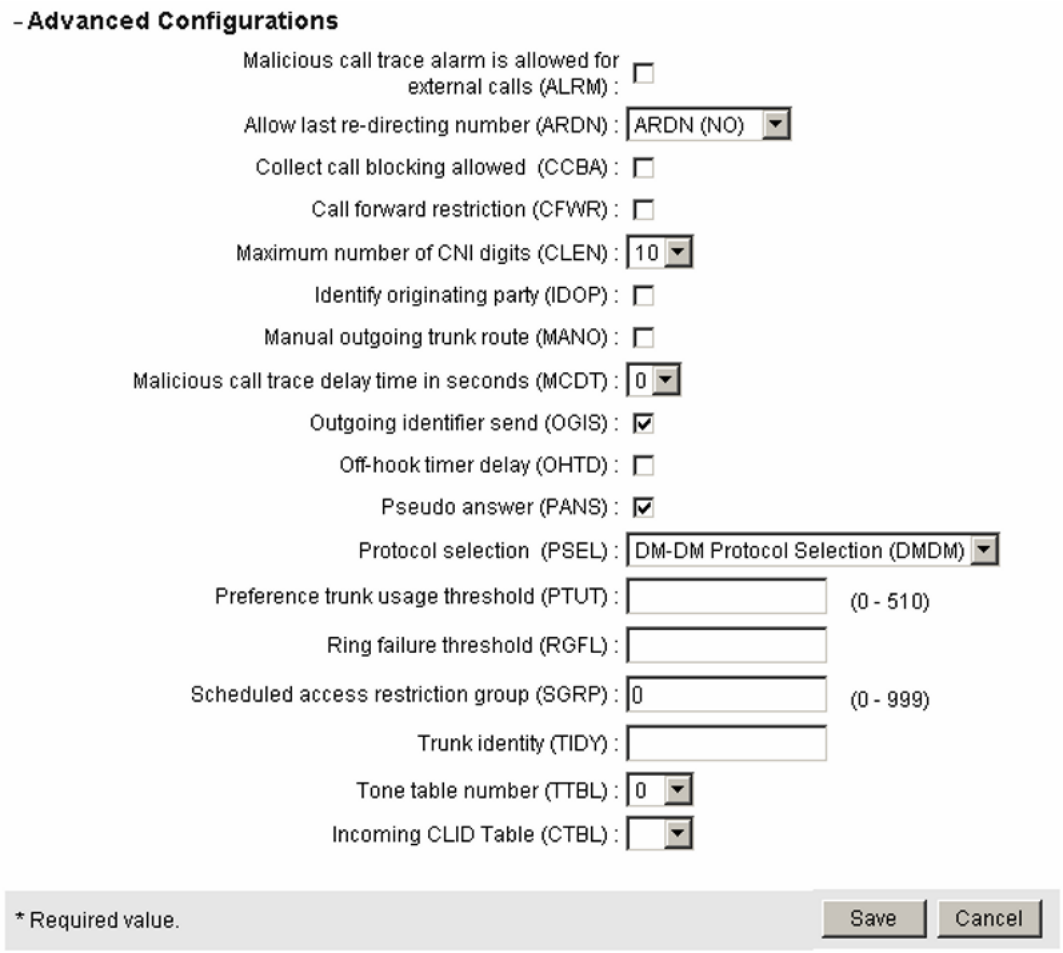


Figure 179: Advanced Configurations for routes

To save changes made in this section, click **Submit** at the bottom of the Route Property Configuration Web page.

New Trunk Configuration

Click the **Add Trunk** button beside a Customer Row or a Trunk Row to open the New Trunk Configuration Web page for the selected customer, route, and trunk, as shown in Figure 180: New Trunk Configuration Web page on page 257.

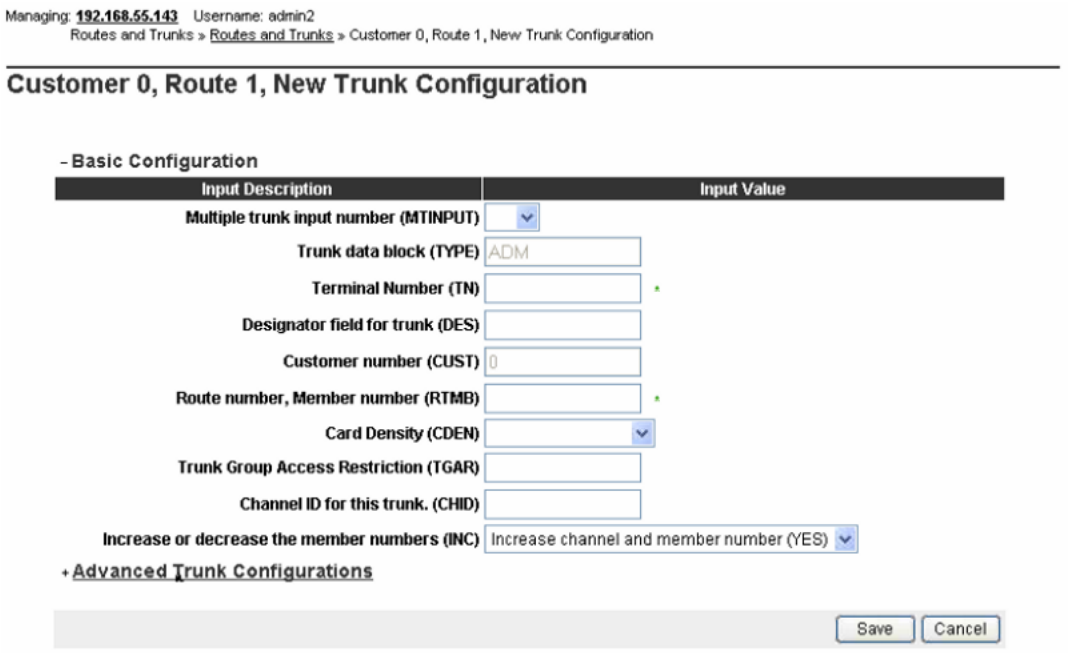


Figure 180: New Trunk Configuration Web page

The New Trunk Configuration Web pages are divided into two categories:

1. Basic Configuration
2. Advanced Trunk Configurations

Basic Configuration

In the **Basic Configuration** section of these Web pages (see Figure 180: New Trunk Configuration Web page on page 257), users can perform the following tasks:

- Enter a **Designator field (DES)** for the trunk.
- Select an **Extended Trunk (XTRK)** card type from the drop-down list.
- Edit the route or member number in the **Route number, Member number (RTMB)** text box. The range is 0-4000.
- Use the **Level 3 Signaling (SIGL)** drop-down list to select a Level 3 signaling method.
- Use the **Start arrangement Incoming (STRI)** drop-down list to select a start arrangement for incoming calls.
- Use the **Start arrangement Outgoing (STRO)** drop-down list to select a start arrangement for outgoing calls.

- Use the **Increase or decrease the member numbers (INC)** drop-down list to select either increasing channel numbers and member numbers or increasing channel numbers and decreasing member numbers.
- Click the **Class of Service (CLS) Edit** button to view Class of Service information for the trunk. See Figure 181: Class of Service Configuration Web page on page 258.

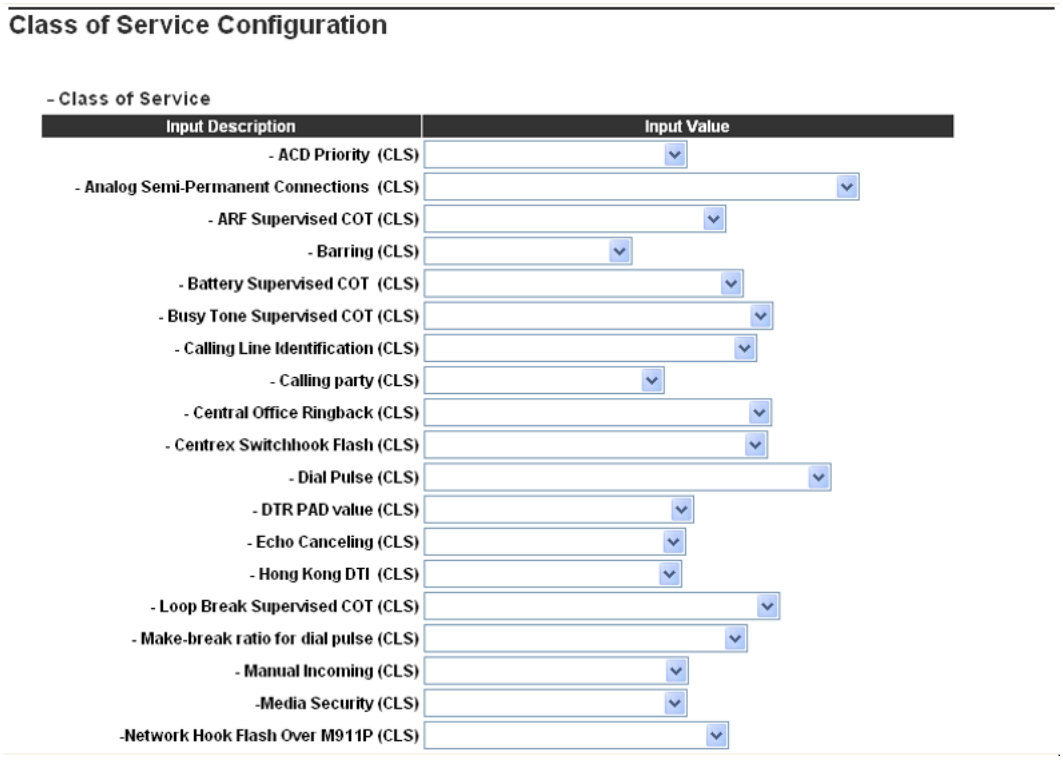


Figure 181: Class of Service Configuration Web page

Note:

The member used in this example is a TIE trunk. The inputs requested by Element Manager may vary depending on the responses to earlier input requests.

To save changes made in this section, click **Submit** at the bottom of the New Member Configuration Web page.

Advanced Trunk Configurations

Figure 182: Advanced Configurations for trunks on page 259 provides an example of the input requested in the **Advanced Trunk Configurations** section for the TIE Trunk shown in Figure 180: New Trunk Configuration Web page on page 257.

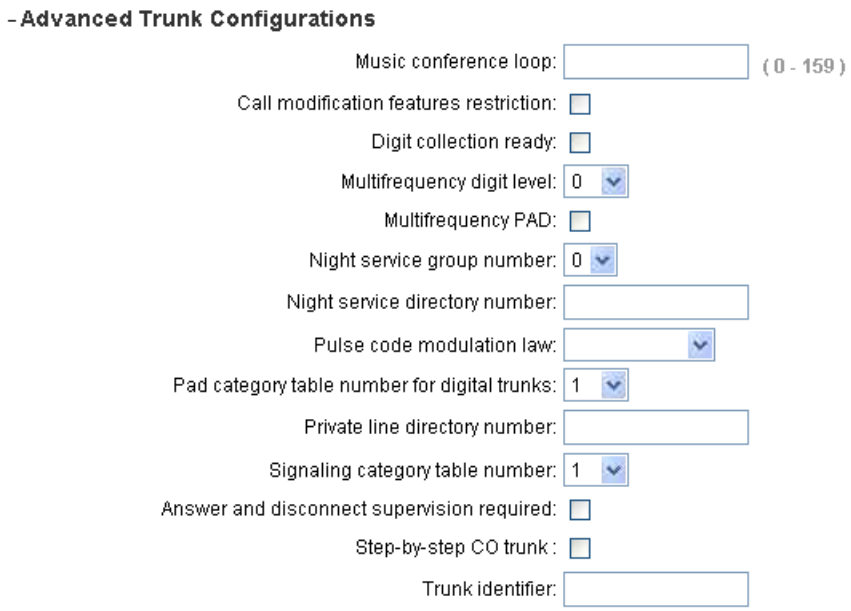


Figure 182: Advanced Configurations for trunks

Note:

The member used in this example is a TIE trunk. The inputs requested by Element Manager may vary depending on the responses to earlier input requests.

To save changes made in this section, click **Submit** at the bottom of the Web page.

Delete multiple trunk members

Click **Multi-Del** located beside a member row to open the Delete multiple trunk members Web page for the selected member, as shown in Figure 183: Delete multiple trunk members page on page 260. On this Web page, the information for the Parent Route is read-only.

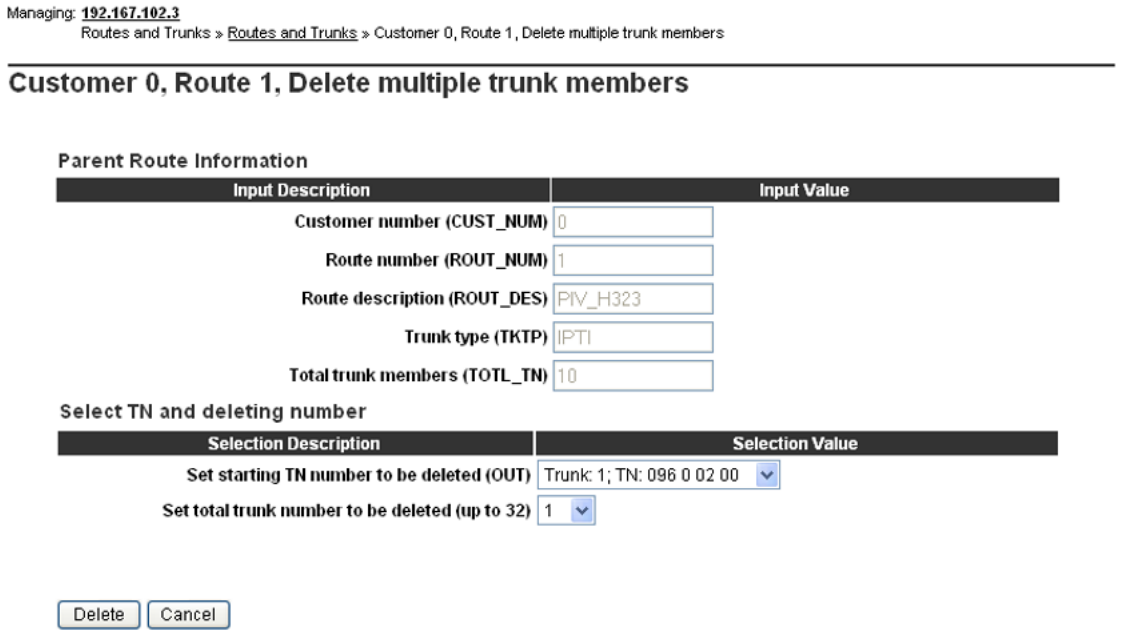


Figure 183: Delete multiple trunk members page

To delete multiple trunk members using this Web page:

1. Use the **Set starting TN to be deleted** drop-down list to determine the start of the deletion list.
2. Use the **Set total trunk number to be deleted** drop-down list to indicate the total number of trunks to be deleted (up to 32).
3. Click **Delete**.

D-channels

Click the **D-Channels** link on the **Routes and Trunks** branch of the Element Manager navigator to open the D-Channels Web page. This Web page allows users to configure or edit D-channel information, as shown in Figure 184: D-Channels Web page on page 261.

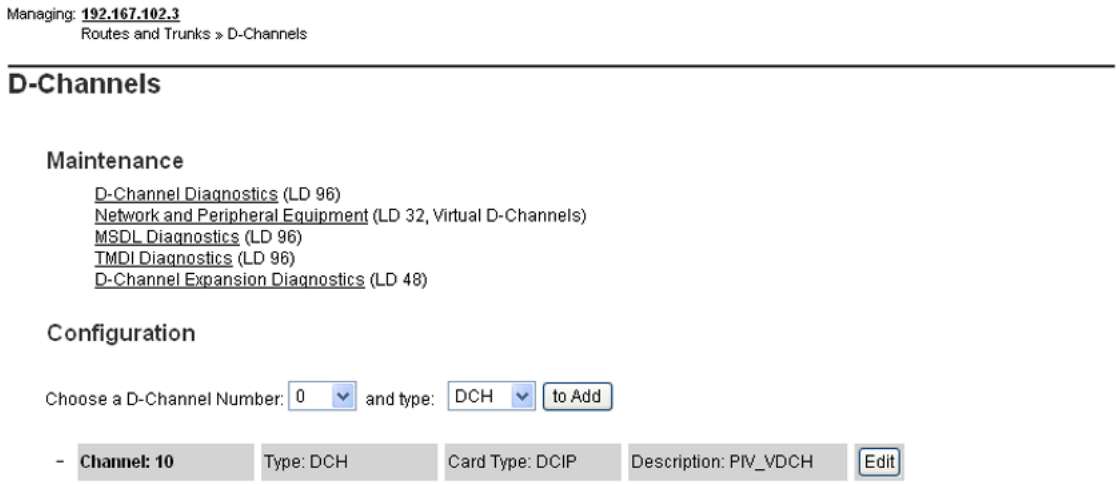


Figure 184: D-Channels Web page

Maintenance

The **Maintenance** section contains links to the following commands:

- D-Channel Diagnostics (LD 96)
- Network and Peripheral Equipment (LD 32, Virtual D-Channels)
- MSDL Diagnostics (LD 96)
- TMDI Diagnostics (LD 96)
- D-Channel Expansion Diagnostics (LD 48)

For more information about these commands, see System on page 43.

Configuration

From the D-Channels Web page users can view basic information about existing D-channels.

This Web page also contains buttons that link to additional Web pages. Follow these links to do the following:

- add a new D-channel
- edit D-channel data

To add a new D-channel, select a number from the **Choose a D-channel Number** drop-down list, select a D-channel **type** from the type drop-down list, and click **to Add**. To edit the configuration information about an existing D-channel, click the **Edit** button located to the right of the Description field.

Click the **to Add** button, or any of the **Edit** buttons, to open the D-Channels Property Configuration Web page for that channel, as shown in Figure 185: D-Channels Property Configuration Web page on page 262).

Note:

H.323 and SIP can use the same D-channel.

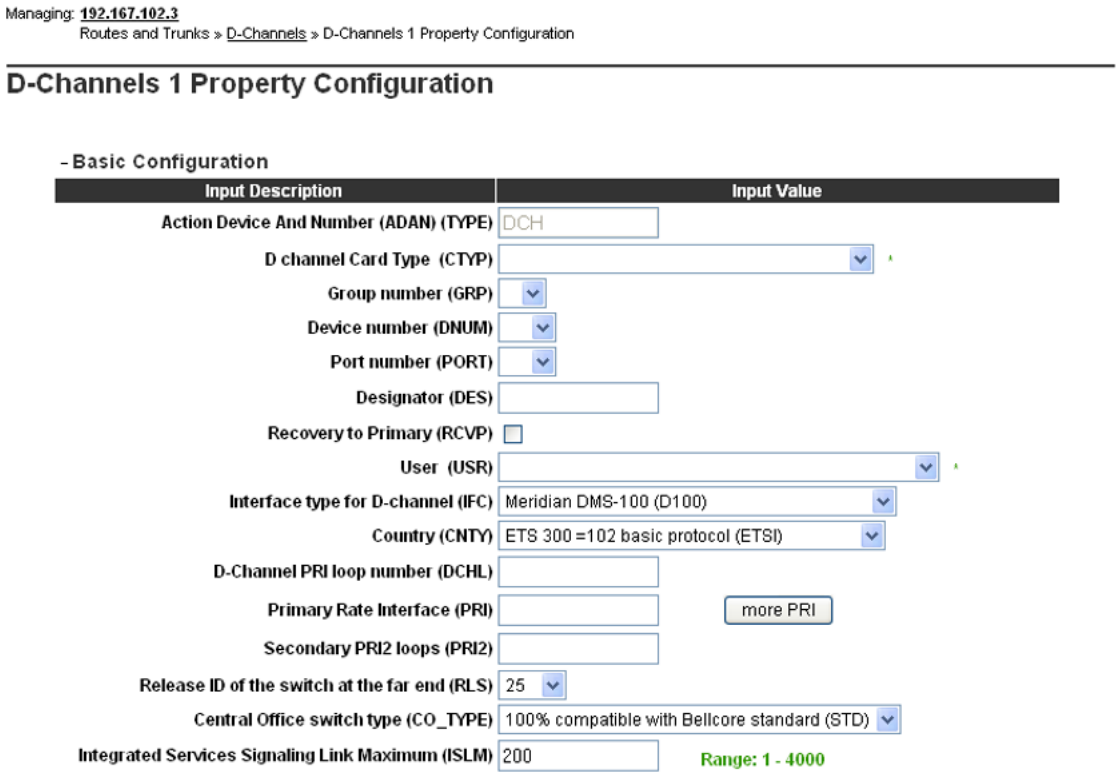


Figure 185: D-Channels Property Configuration Web page

In the D-Channels Property Configuration Web page, users can:

- Enter information about the Basic Configuration Web page.
  - The information entered in this section corresponds to ADAN and ADAN DCH (Action Device and Number, D-channel and back-up D-channels) data traditionally configured

using LD 17 - Configuration Record 1. In addition to basic D-channel configuration, additional information can be entered for optional settings in the following two categories:

- Basic D-channel options (BSCOPT)
- Advanced D-channel options (ADVOPT)

These options are shown in Figure 186: Basic and Advanced D-Channel options on page 263.

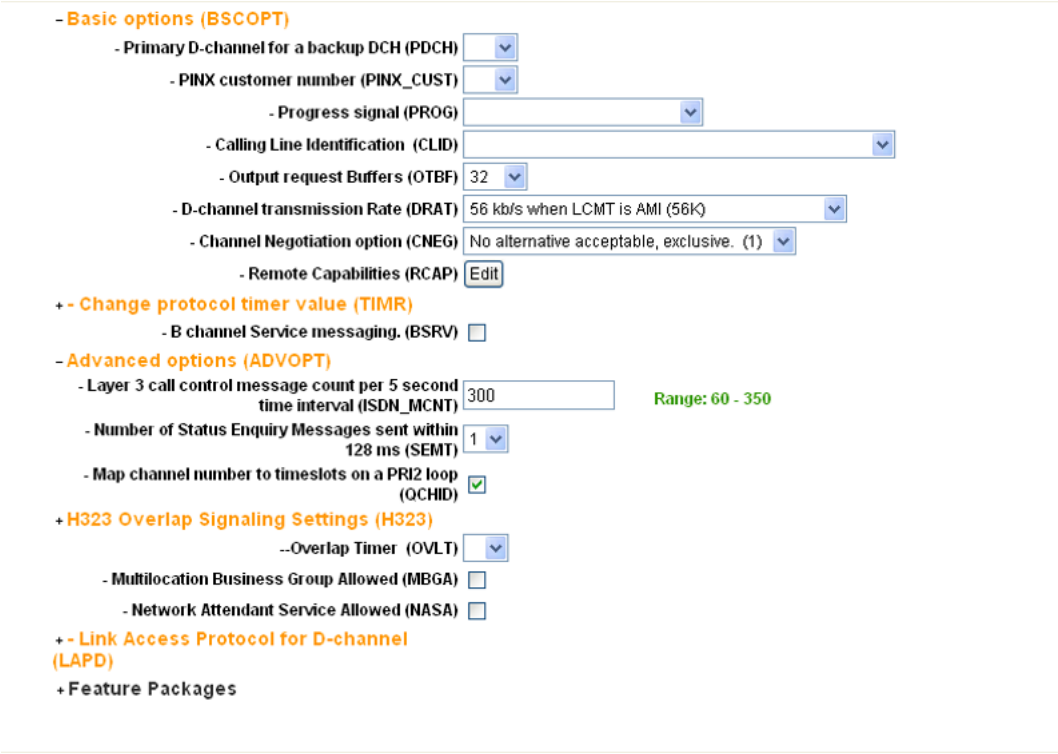


Figure 186: Basic and Advanced D-Channel options

- Configure information about the Feature Packages Web page.
  - Digital Private Networking Signaling System 1 (Package 123)
  - Virtual Network Services (Package 183)

To save changes made in this section, click **Submit** at the bottom of the D-channels Property Configuration Web page.

Digital Trunk Interface

When the user clicks the **Digital Trunk Interface** link on the **Routes and Trunks** branch of the Element Manager navigator, the Digital Trunk Interface Web page appears, as shown in

Figure 187: Digital Trunk Interface Web page on page 264. This Web page allows the user to configure or edit Digital Trunk Interface information.

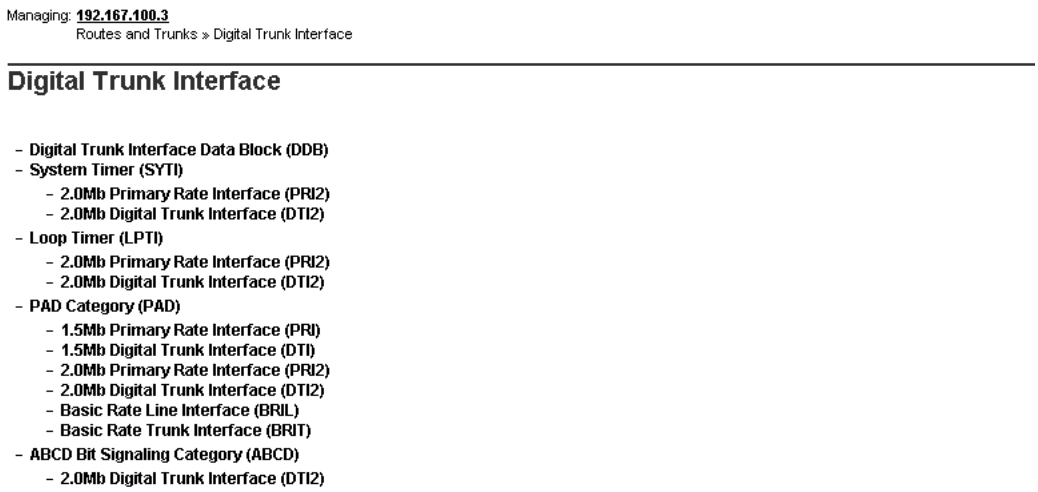


Figure 187: Digital Trunk Interface Web page

Use this Web page to access additional Web pages to perform the following functions:

- configure Digital Trunk Interface Data Block (DDB) information
- configure System Timer (SYSTI) parameters for:
  - 2.0 Mb Primary Rate Interface (PRI2)
  - 2.0 Mb Digital Trunk Interface (DTI2)
- configure Loop Timer (LPTI) parameters for:
  - 2.0 Mb Primary Rate Interface (PRI2)
  - 2.0 Mb Digital Trunk Interface (DTI2)
- configure PAD Category (PAD) parameters for:
  - 1.5 Mb Primary Rate Interface (PRI)
  - 1.5 Mb Digital Trunk Interface (DTI)
  - 2.0 Mb Primary Rate Interface (PRI2)
  - 2.0 Mb Digital Trunk Interface (DTI2)
  - Basic Rate Line Interface (BRIL)

- Basic Rate Trunk Interface (BRIT)

- configure ABCD Bit Signaling Category (ABCD) parameters for the 2.0 Mb Digital Trunk Interface (DTI2)

To configure or edit Digital Trunk Interface Data Block (DDB) information, click **Digital Trunk Interface Data Block (DDB)**. The Threshold Set List Web page appears. See Figure 188: Threshold Set List Web page on page 265.

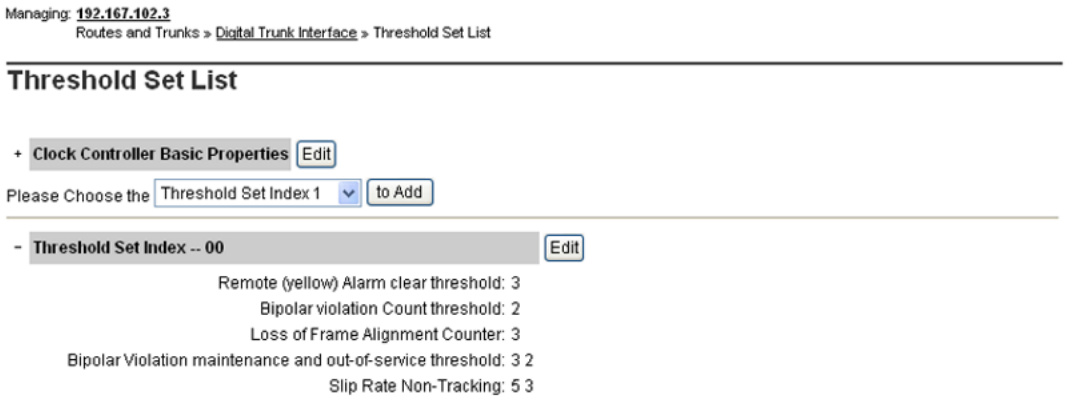


Figure 188: Threshold Set List Web page

From this Web page, users can access additional Web pages to perform the following functions:

- edit Clock Controller Basic Properties
- add a Threshold Set Index
- edit an existing Threshold Set Block

Edit Clock Controller properties by clicking the **Edit** button next to the **Clock Controller Basic Properties** button. The Clock Controller Basic Properties Web page appears, as shown in Figure 189: Clock Controller Basic Properties Web page on page 266.

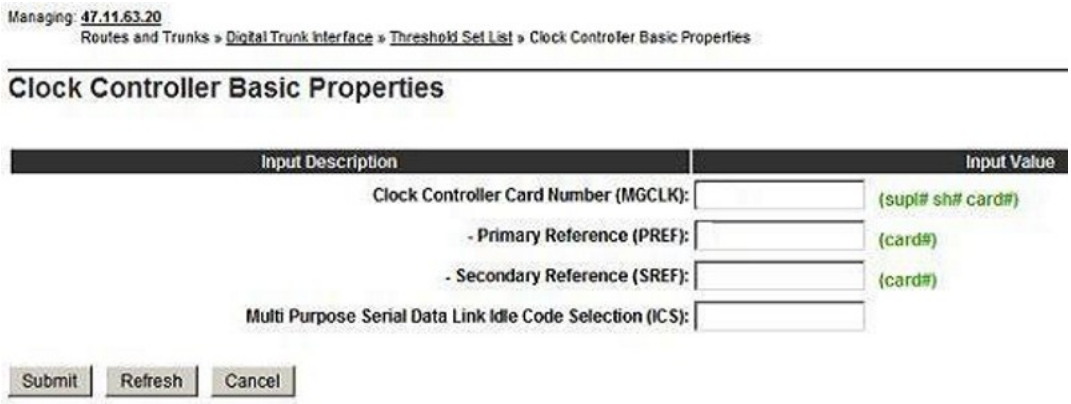


Figure 189: Clock Controller Basic Properties Web page

Next enter the required information in the text boxes.

To add or edit a Threshold Set Index, follow the steps in Adding or editing a Threshold Set Index on page 266.

Adding or editing a Threshold Set Index

To add a Threshold Set Index

1. Select a **Threshold Set Index** from the drop-down list.
2. Click **to Add**.

   To edit the configuration information in an existing Threshold Set Block, click **Edit** located to the right of the index number.

After you click the **to Add** button or a **Threshold Set Index Edit** button on Figure 188: Threshold Set List Web page on page 265, the Threshold Set Block Web page for that index appears, as shown in Figure 190: Threshold Set Block Web page on page 267.

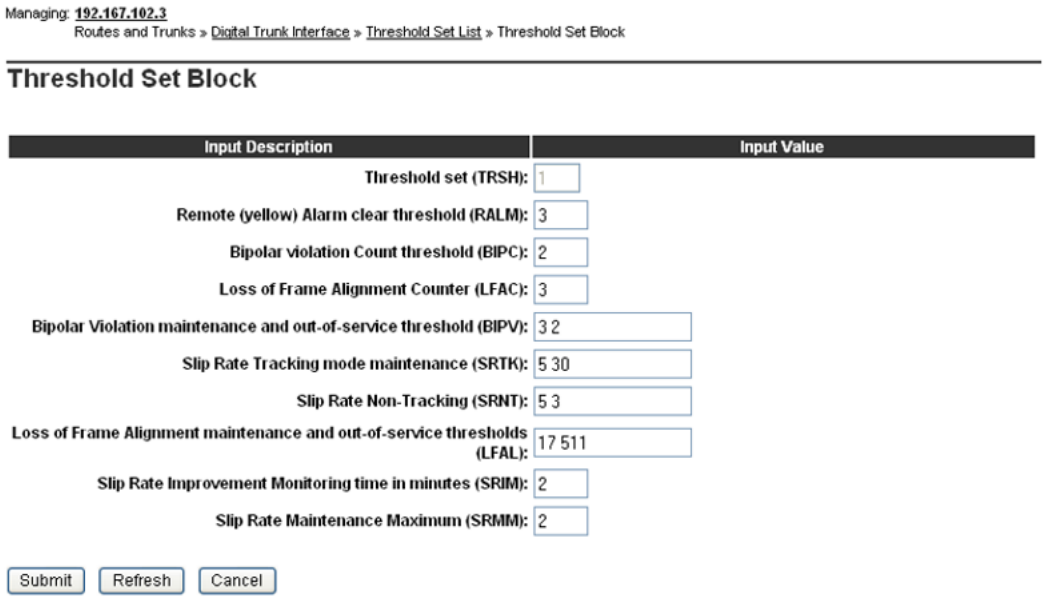


Figure 190: Threshold Set Block Web page

The information entered in this section corresponds to DDB (Digital Trunk Interface Data Block) information traditionally configured using LD 73 - Digital Trunk Interface.

To save changes made in this section, click **Submit** at the bottom of the Threshold Set Block Web page.

Chapter 10: Dialing and Numbering Plans

Contents

This chapter contains information about the following topics:

Introduction

Element Manager enables users to configure the Dialing and Numbering Plans for the Call Server and the Network Routing Service (NRS) Manager. The information configured in the Dialing and Numbering Plans corresponds to the Command Line Interface (CLI) prompts and responses for Electronic Switched Network (ESN) data traditionally configured in LD 86, LD 87, and LD 90.

For more information about the overlays referred to in this chapter, see *Avaya Software Input Output Administration, NN43001-611,* and *Avaya Software Input Output Reference - Maintenance, NN43001-711*.

Electronic Switched Network

To configure or edit the Dialing and Numbering Plan for the Electronic Switched Network, click the **Electronic Switched Network** link in the **Dialing and Numbering Plans** branch of the Element Manager navigator. The **Electronic Switched Network (ESN)** Web page appears as shown in Figure 191: Electronic Switched Network (ESN) Web page on page 270. From this Web page users can configure the Dialing and Numbering Plan for each customer on the Electronic Switched Network.

Element Manager provides access to the following Dialing and Numbering Plan parameters:

- Network Control & Services
- Coordinated Dialing Plan (CDP)
- Numbering Plan (NET)

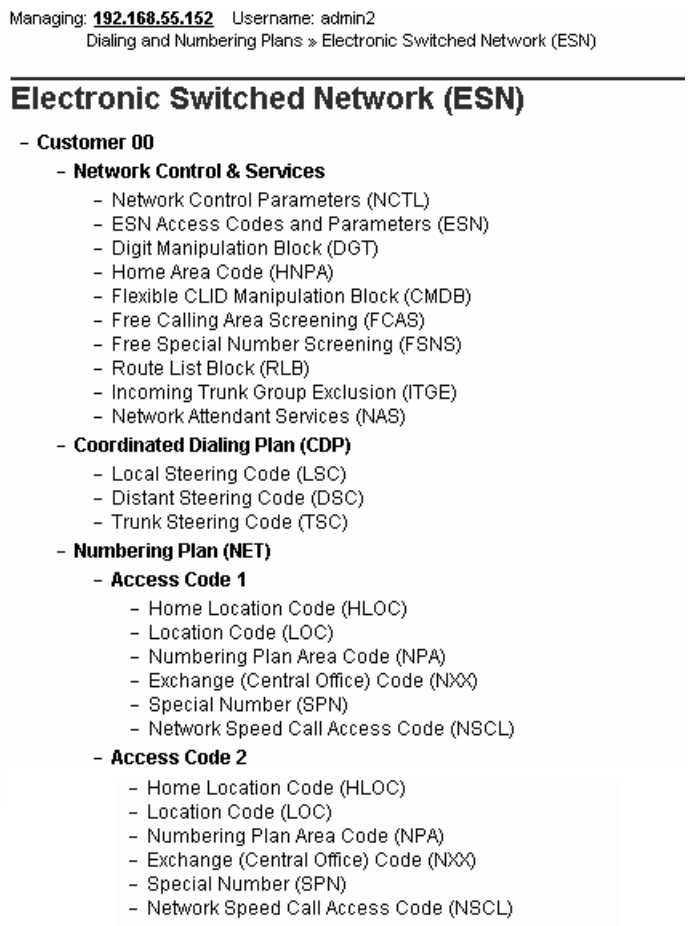


Figure 191: Electronic Switched Network (ESN) Web page

Network Control and Services

Under Network Control and Services, users can click the links to configure or modify the parameters associated with the following items:

- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Home Area Code (HNPA)

- Flexible CLID Manipulation Block (CMDB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)

The Network Control Parameters (NCTL) that are configurable using Element Manager correspond to data traditionally configured in LD 87. Free Calling Area Screening (FCAS) and Free Special Number Screening (FSNS) are also LD 87 features. The Home Area Code (HNPA) can be configured using the prompts and responses in LD 90. The settings for the remaining five items under Network Control & Services correspond to CLI prompts and responses in LD 86.

To view the total free and used Location Codes (LOCs), click **Customer xx > Network Control & Services > ESN Access Codes and Basic Parameters**. The ESN Access Codes and Basic Parameters Web page appears as shown in Figure 192: ESN Access Codes and Basic Parameters Web page on page 272.

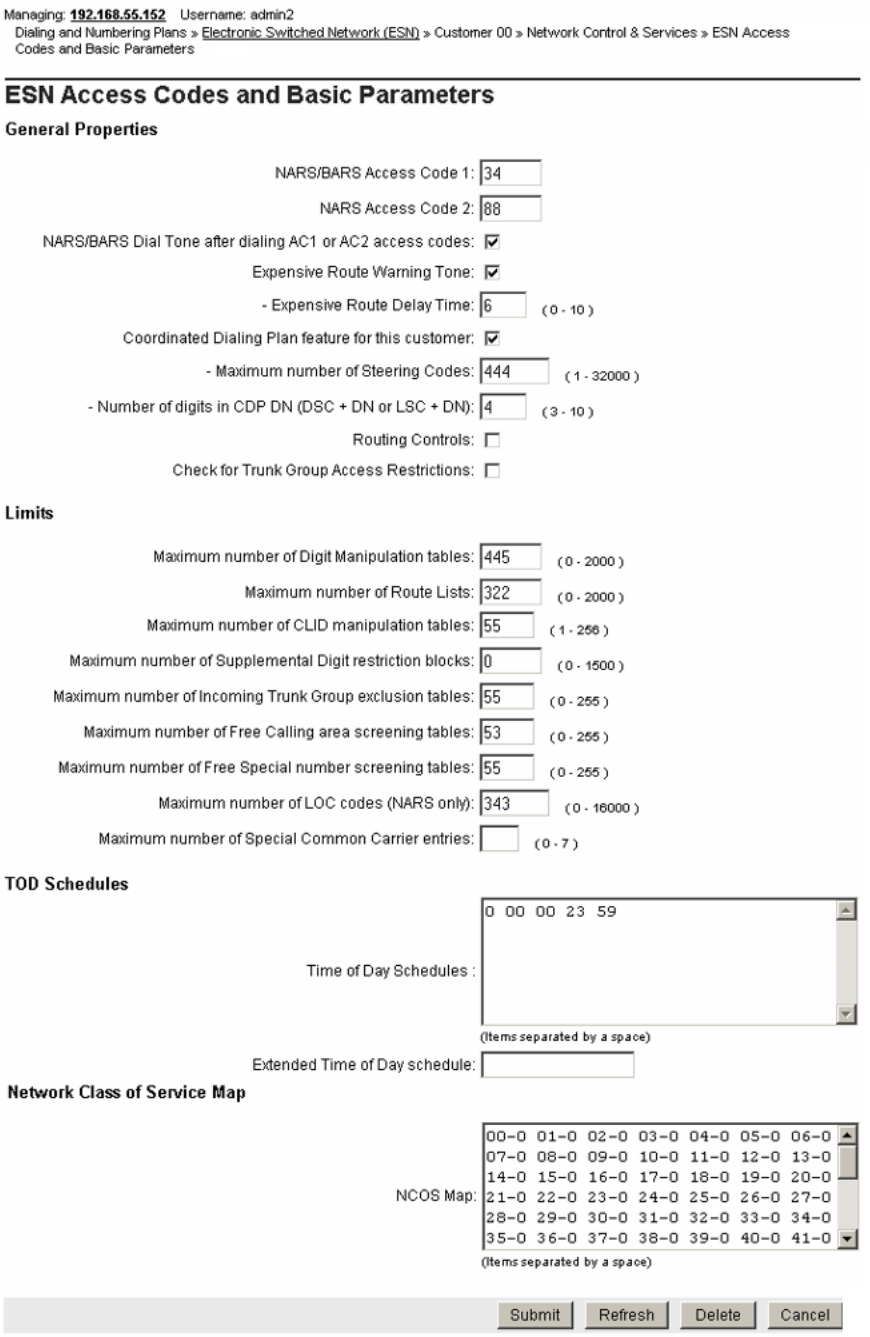


Figure 192: ESN Access Codes and Basic Parameters Web page

This feature has its own packaging (LOCX). The package must be added under **Customers > Customer xx Property Configuration > Feature Packages**. You can activate this package only when the FNP package is enabled.

Route List Block

In the ESN Web page, under the **Network Control & Services** tab, click **Route List Block (RLB)** . The Route List Blocks Web page appears.

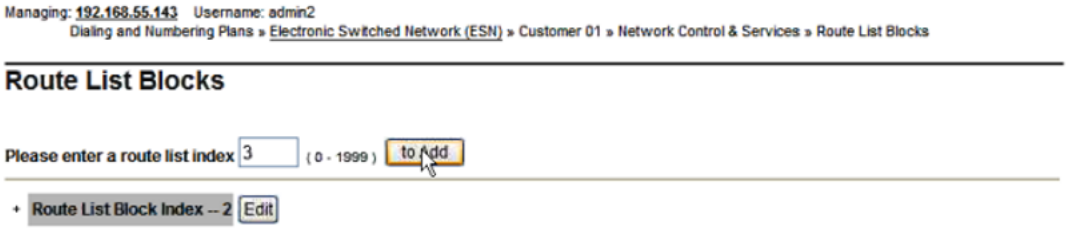


Figure 193: Route List Blocks

In the **Please enter a route list index** , enter the route list index and then click **to Add** . The Route List Block properties page appears.

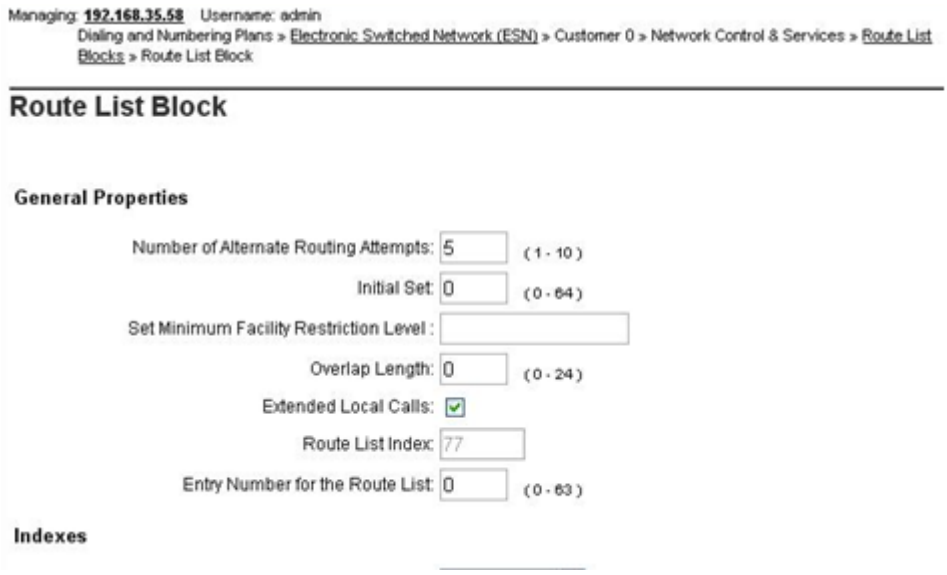


Figure 194: Route List Block properties

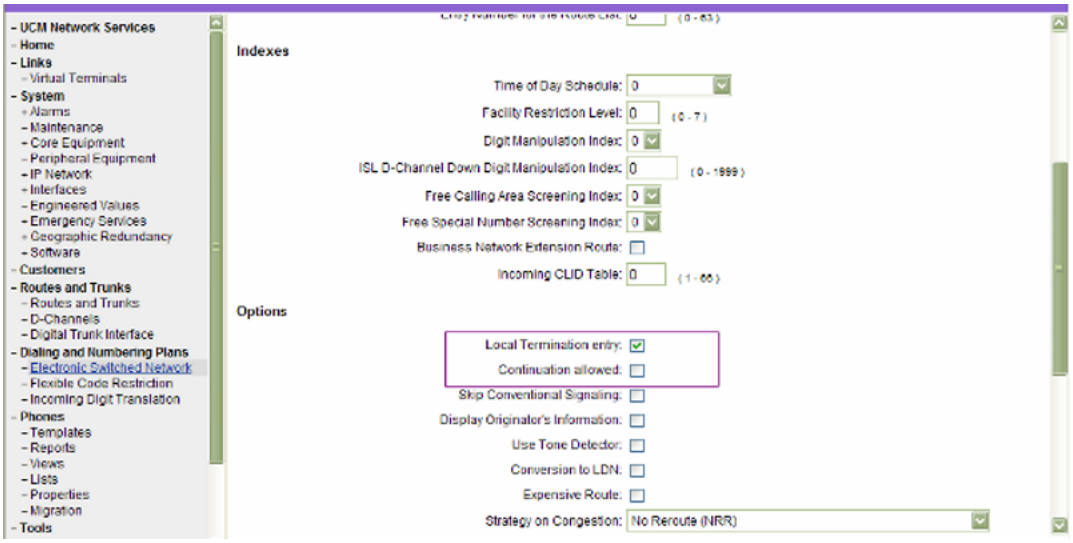


Figure 195: Route List Block properties (continued)

In the **Options** section, clear or disable **Local Termination entry** to enable the **Route Number** field. Select **Local Termination Entry** (LTER) to enable the **Continuation Allowed** (CONA) field.

CONA feature allows the next entry of the Route List Block if local termination fails for a NARS call. This operation cannot be used for Trunk Steering Code (TSC) or Distant Steering Code (DSC) configurations. To configure CONA, select **Local Termination Entry** and **Continuation Allowed** , and then click **Submit** .

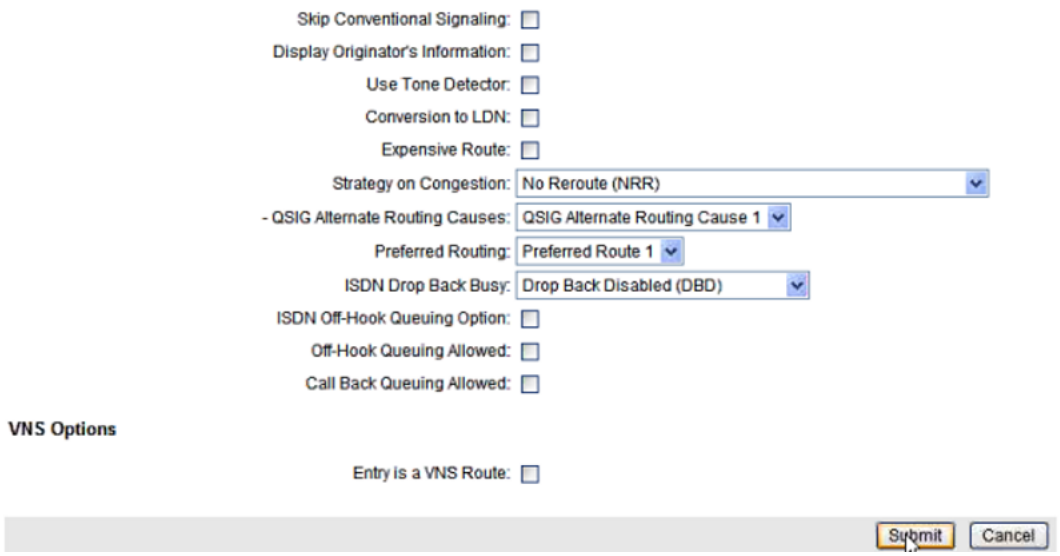


Figure 196: Route List Block properties (Continued1)

Select the required options and click **Submit** . The Route List Block with all the properties appears as shown below.

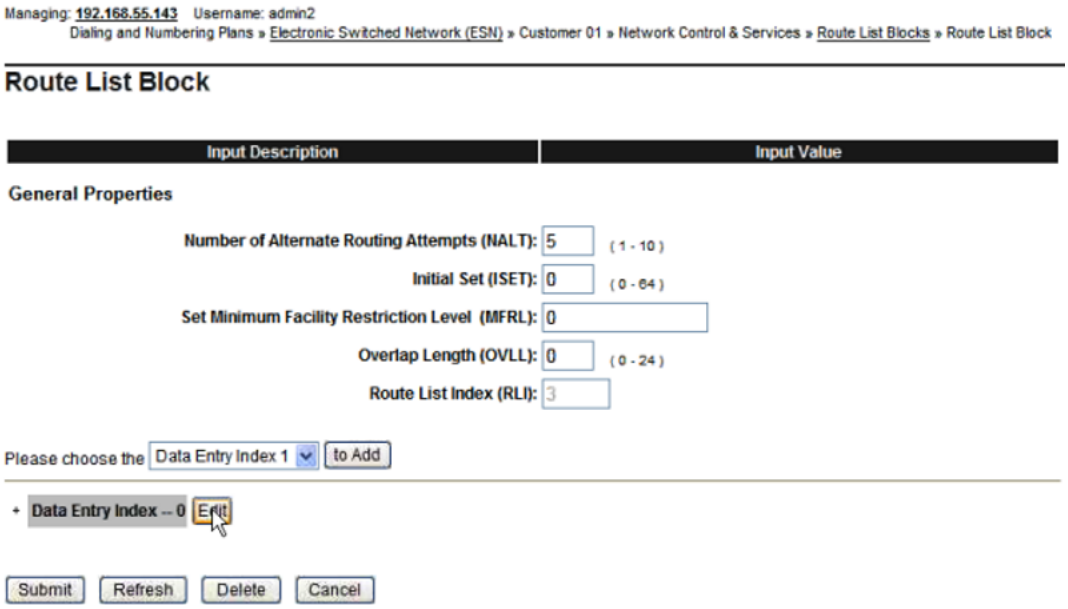


Figure 197: Route List Block Properties

Click on **Edit** next to Data Entry Index. The Data Entry of a Route List Block Web page appears as shown below.

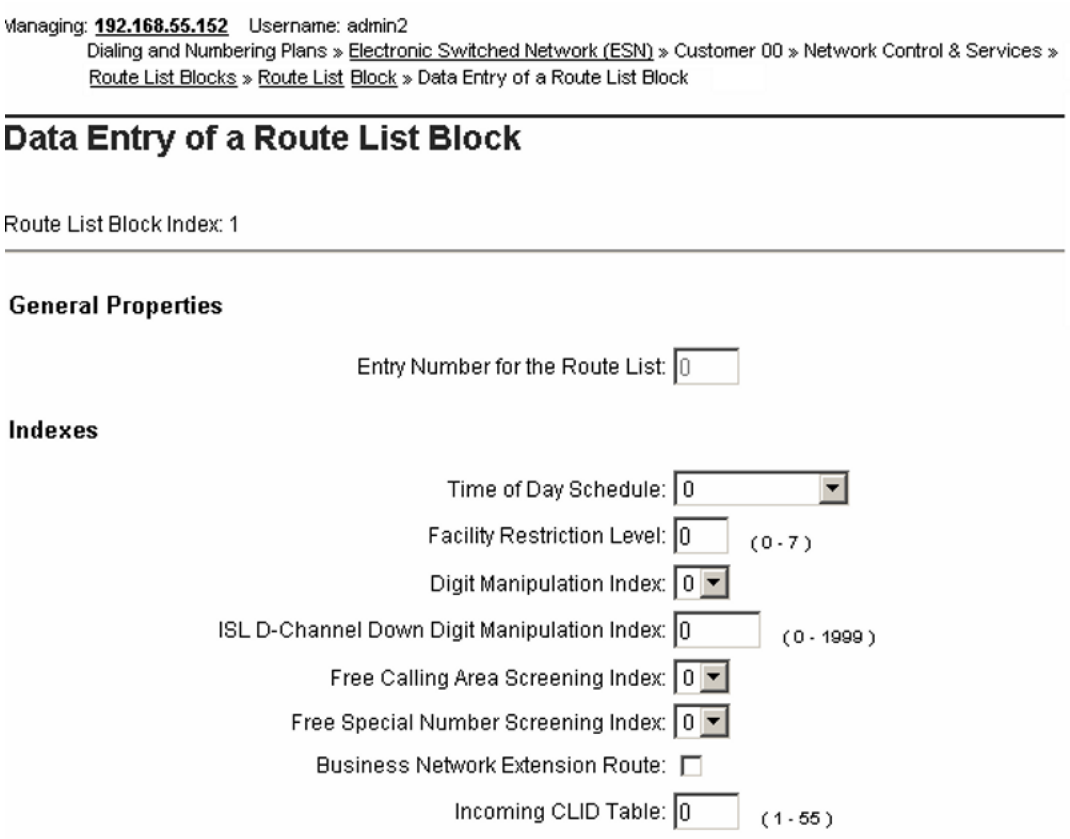
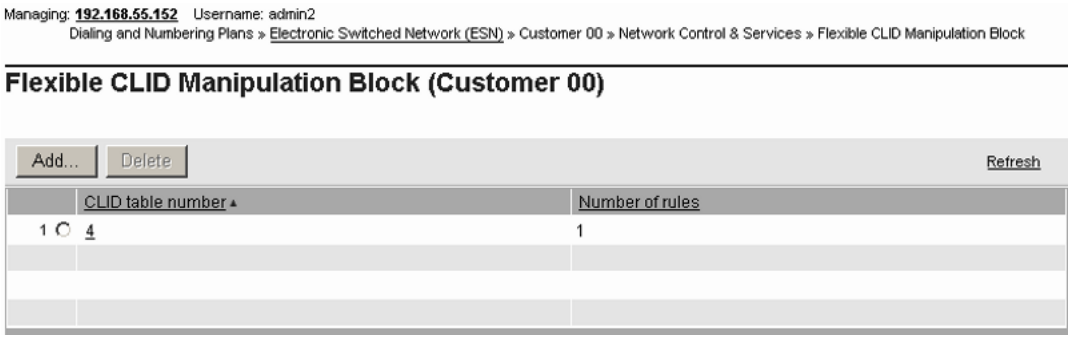


Figure 198: Data Entry of Route List Block

Flexible CLID Manipulation Block

In the ESN Web page, under the **Network Control & Services** tab, click **Flexible CLID Manipulation Block (CMDB)** . The Flexible CLID Manipulation Block Web page appears.

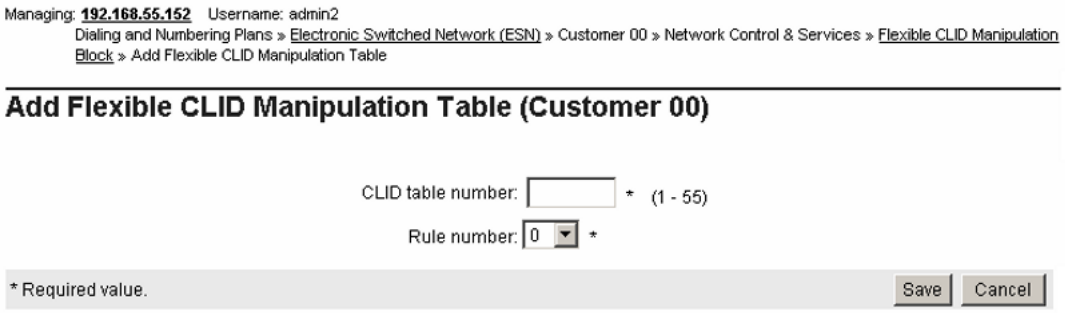


Use the following procedure, to add a CLID manipulation table.

Adding a CLID manipulation table

1. Click **Add** .

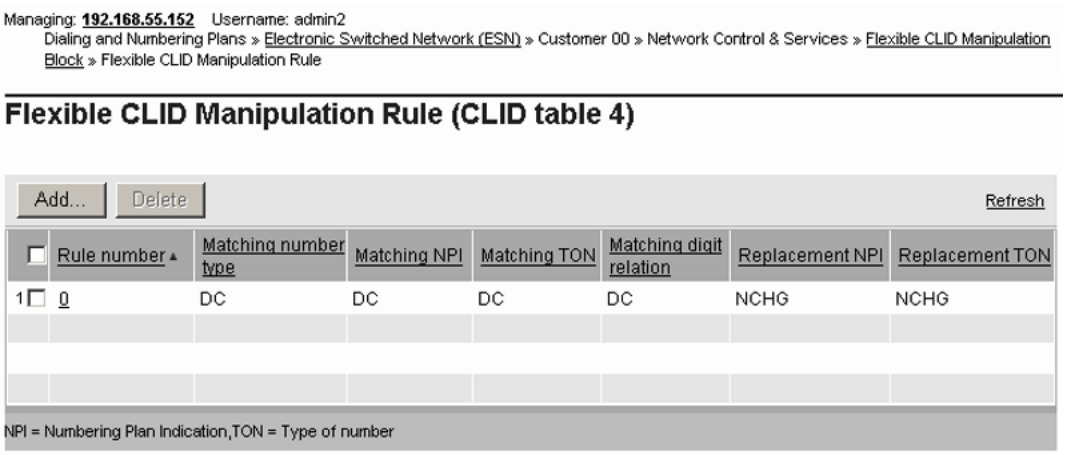
   The Add Flexible CLID Manipulation Table Web page appears.



2. In the **CLID table number** field, enter the required value.
3. In the **Rule number** field, select the required value.
4. Click **Save** .

   The page refreshes to display the Flexible CLID Manipulation Block Web page appears displaying the configured CLID manipulation table.

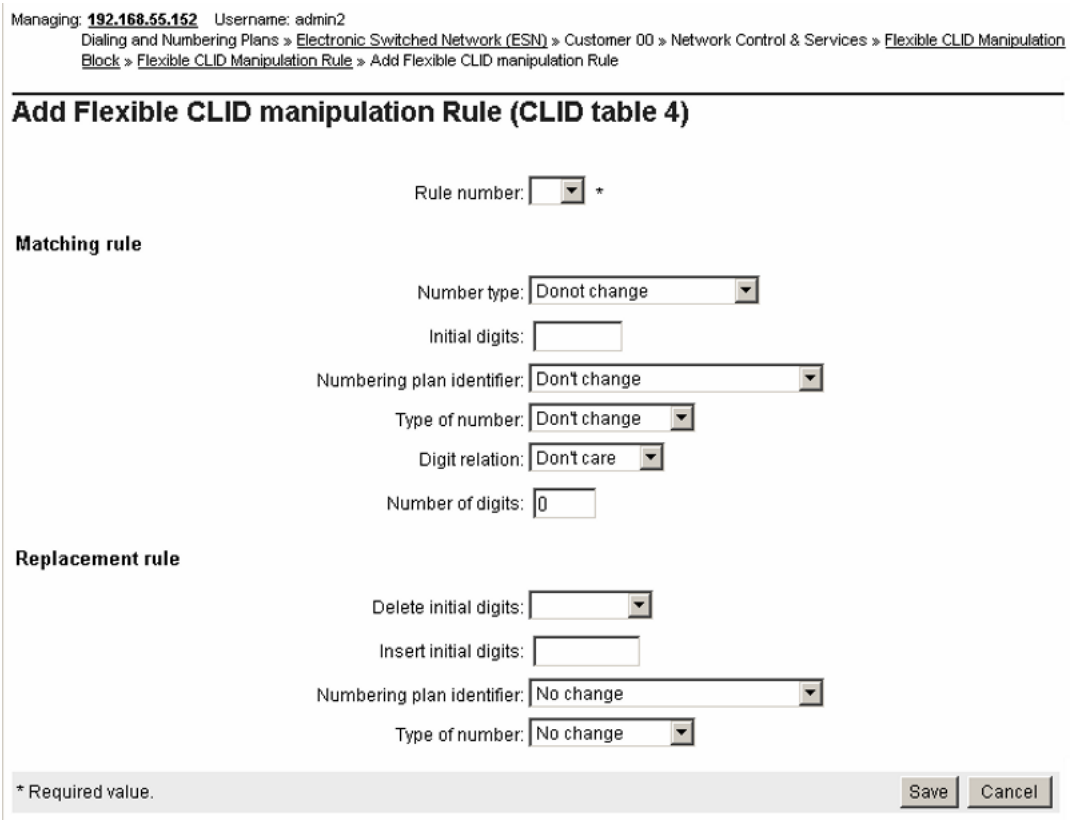
To view the details of a CLID manipulation table, click the table number in the Flexible CLID Manipulation Block Web page. The Flexible CLID Manipulation Rule Web page appears.



Adding a CLID manipulation rule to a table

1. In the Flexible CLID Manipulation Rule Web page, click **Add** .

   The Add Flexible CLID Manipulation Rule Web page appears.



2. Enter the required values in the fields.
3. Click **Save** .

   The page refreshes to display the Flexible CLID Manipulation Rule Web page with the new rule added.

You can delete a manipulation table or rule by selecting the corresponding check box and clicking **Delete** . To delete multiple values, select the corresponding check boxes.

Important:

Manipulation tables can be deleted one at a time. Multiple deletion is not allowed for the tables.

To edit or view the details of a manipulation rule, click on the rule number in the Flexible CLID Manipulation Rule Web page.

Coordinated Dialing Plan

Under Coordinated Dialing Plan (CDP), users can click links to configure or modify parameters associated with the following codes:

- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)

The Coordinated Dialing Plan parameters that are configurable using Element Manager correspond to data traditionally configured in LD 87.

Numbering Plan

Under Numbering Plan (NET), users can click links to configure or modify parameters associated with the following codes:

- Home Location Code (HLOC)
- Location Code (LOC). Maximum number of LOCs is 16 000.
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)

These codes can also be configured using the prompts and responses in LD 90.

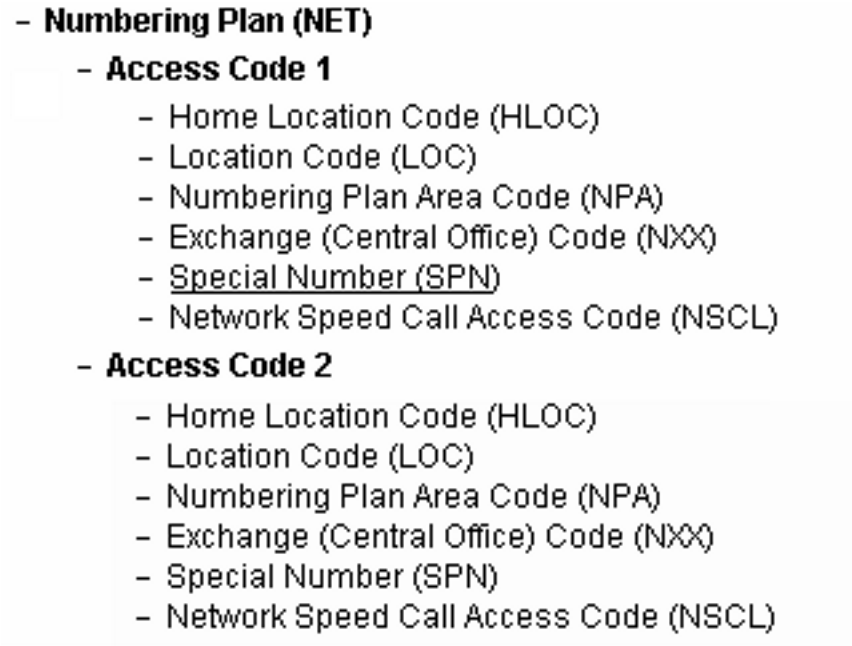


Figure 199: Electronic Switched Network (ESN)

In the ESN web page, click Special Number (SPN) in the Numbering Plan part as shown in the above figure. The Special Number List web page appears.

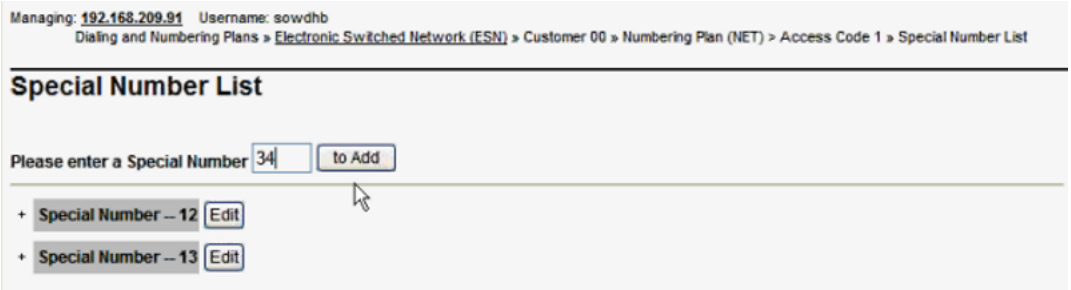


Figure 200: Special Number List

In the Special NUmber list web page, enter the special number snd click to Add. The Special Number web page appears.

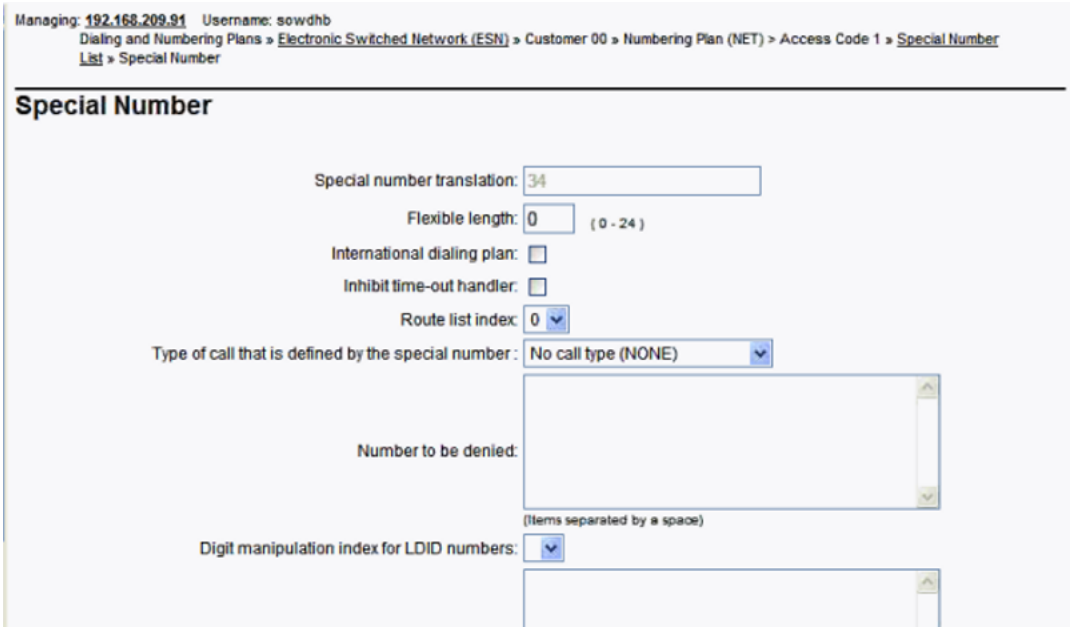


Figure 201: Special Number (Continued1)

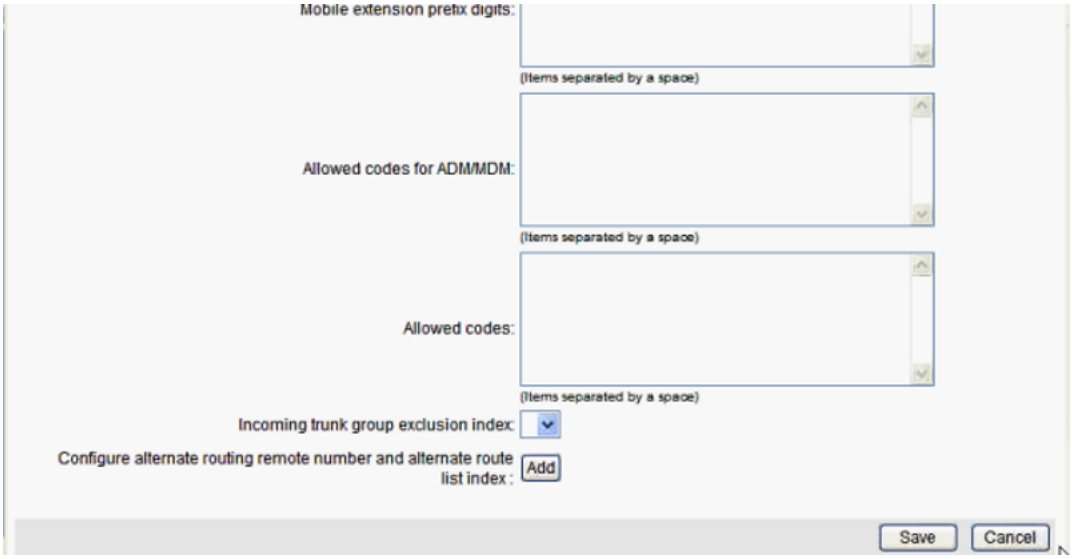


Figure 202: Special Number (Continued2)

Enter Mobile extension prefix digits and other required fields and then click Save.

Flexible Code Restriction

To configure or edit Flexible Code Restriction information, click the **Flexible Code Restriction** link in the **Dialing and Numbering Plans** branch of the Element Manager

navigator. The Flexible Code Restriction Web page appears, as shown in Figure 203: Flexible Code Restriction Web page on page 282.

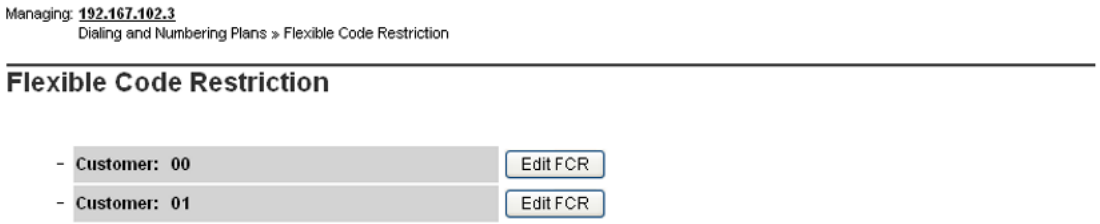


Figure 203: Flexible Code Restriction Web page

This Web page contains **Edit FCR** buttons that link to Flexible Code Restriction Property Web pages for each of the customers configured on the Call Server.

To view the list of Flexible Code Restriction Trees for a customer, click the **Edit FCR** button located beside the customer number. The Flexible Code Restriction Property Web page for the selected customer opens (see Figure 204: Flexible Code Restriction Property Web page on page 283).

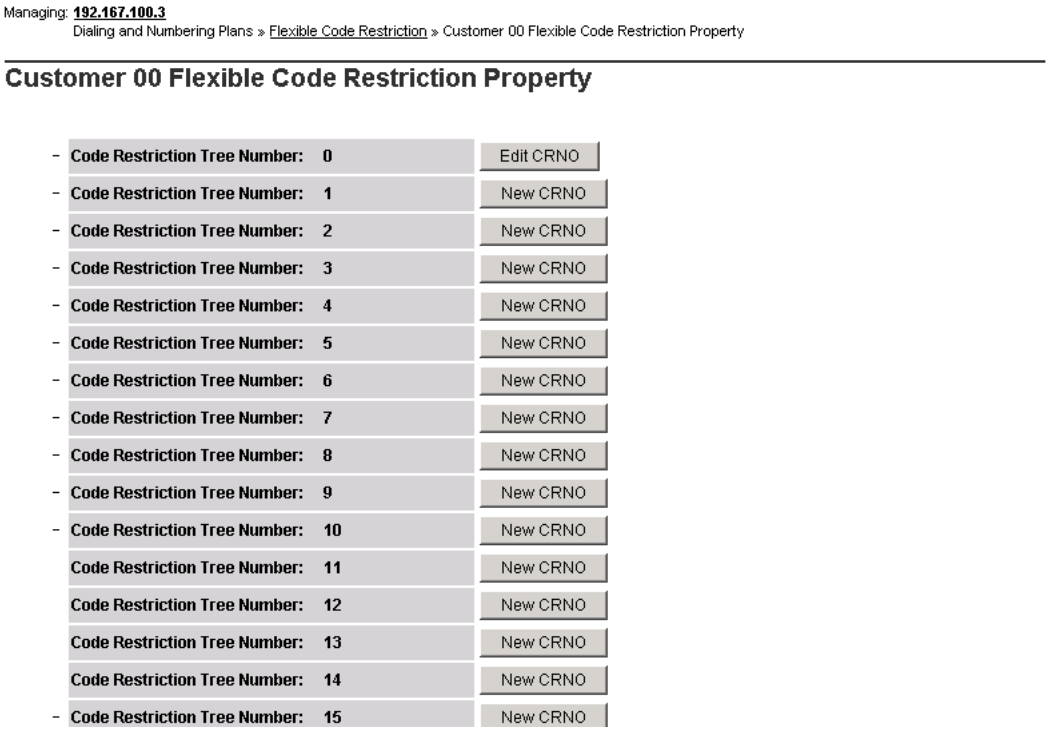


Figure 204: Flexible Code Restriction Property Web page

The Flexible Code Restriction Property Web page contains buttons that link to Code Restriction Tree Configuration Web pages for each Code Restriction Tree Number (CRNO). If there is an existing configuration for the CRNO, the button is labeled **Edit CRNO**. If a configuration has not been defined for the CRNO, the button is labeled **New CRNO**. Click the **Edit CRNO/New CRNO** button to open the Code Restriction Tree Configuration Web page for the corresponding CRNO, as shown in Figure 205: Code Restriction Tree Configuration Web page on page 284.

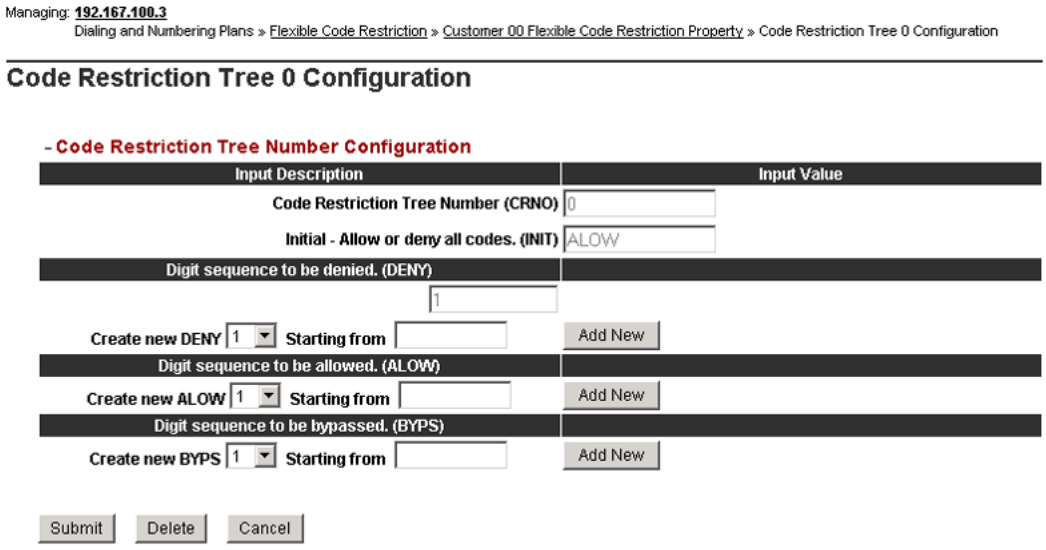


Figure 205: Code Restriction Tree Configuration Web page

By entering values in the appropriate text boxes, users can:

- add or edit digit sequences to be enabled
- add or edit digit sequences to be denied

The information entered in this section corresponds to data traditionally configured using LD 49 - Flexible Code Restriction and Incoming Digit Conversion.

To save changes made in the configuration for this Code Restriction Tree, click **Submit** at the bottom of the Web page.

Incoming Digit Translation

To configure or edit Incoming Digit Translation information, click the **Incoming Digit Translation** link in the **Dialing and Numbering Plans** branch of the Element Manager navigator. The Incoming Digit Translation Web page appears, as shown in Figure 206: Incoming Digit Translation Web page on page 285.

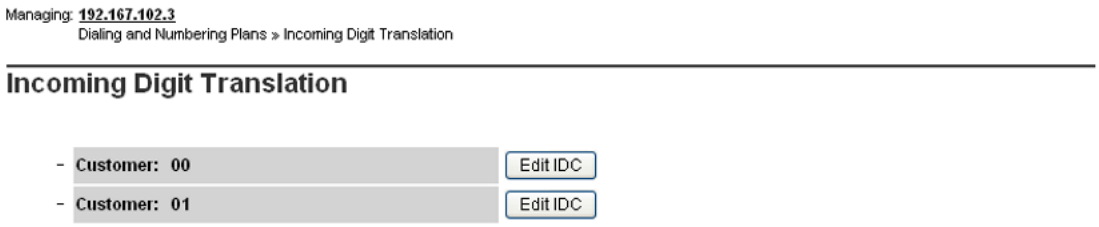


Figure 206: Incoming Digit Translation Web page

This Web page contains **Edit IDC** buttons that link to Incoming Digit Conversion Property Web pages for each of the customers configured on the Call Server.

To view the list of Incoming Digit Conversion Trees for a customer, click the **Edit IDC** button located beside the customer number. The Incoming Digit Conversion Property Web page for the selected customer appears. See Figure 207: Incoming Digit Conversion Property Web page on page 286.

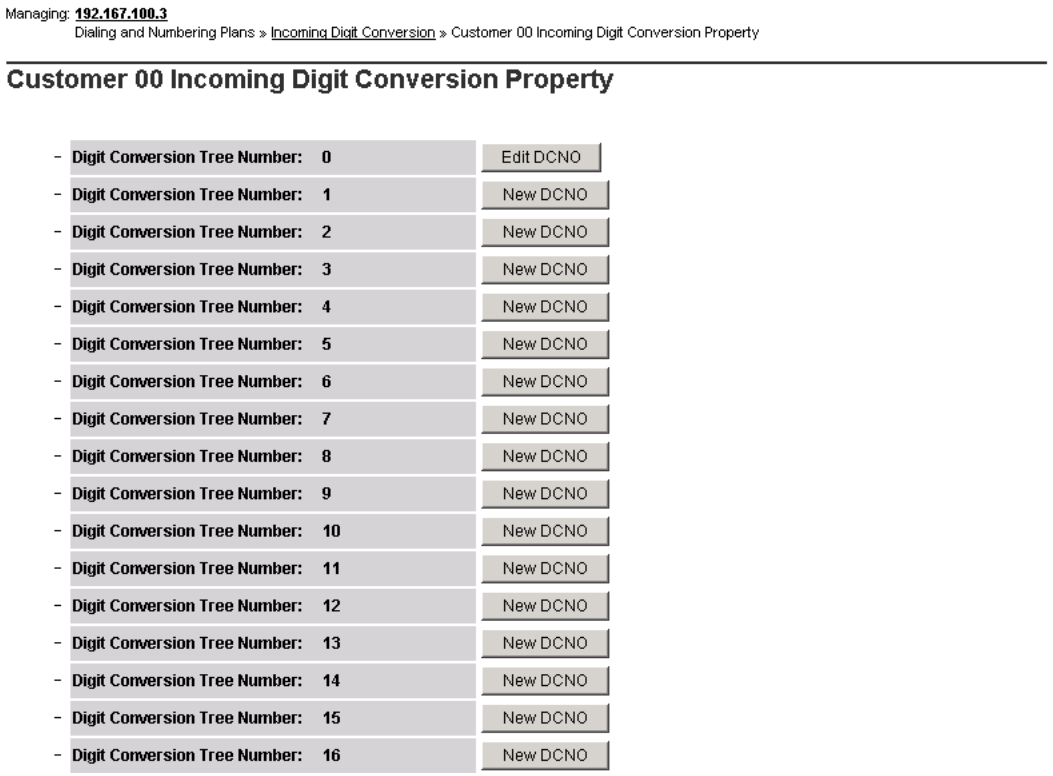


Figure 207: Incoming Digit Conversion Property Web page

The Incoming Digit Conversion Property Web page contains buttons that link to Digit Conversion Tree Configuration Web pages for each Digit Conversion Tree Number (DCNO). If there is an existing configuration for the DCNO, the button is labeled **Edit DCNO**. If a configuration has not been defined for the DCNO, the button is labeled **New DCNO**. Click the **Edit DCNO/New DCNO** button to open the Digit Conversion Tree Configuration Web page for the corresponding DCNO. From this Web page, users can configure Incoming Digit Conversion data.

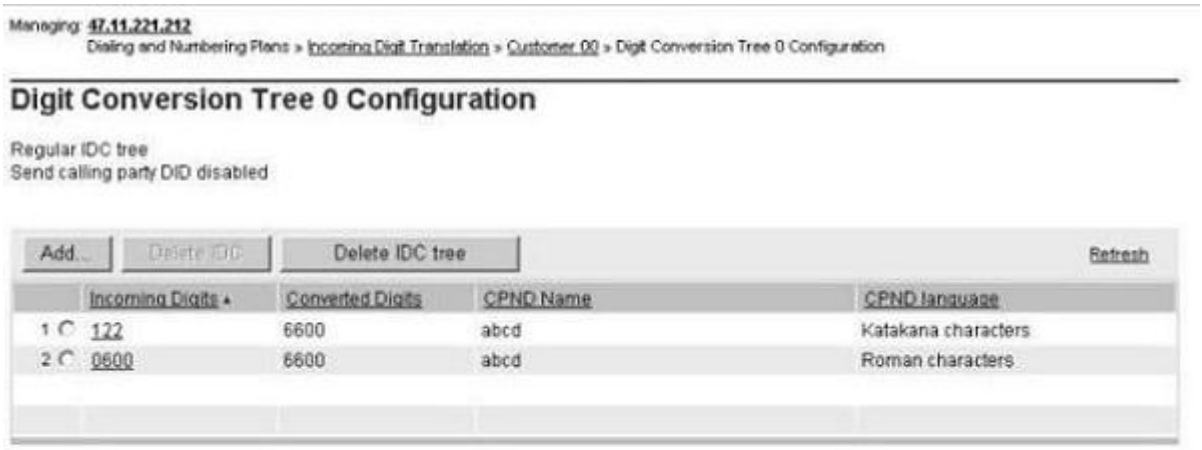


Figure 208: Digit Conversion Tree Configuration Web page

The information entered in this section corresponds to data traditionally configured using LD 49 - Flexible Code Restriction and Incoming Digit Conversion.

Chapter 11: Phones

Contents

This chapter contains the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Introduction

EM Phone Provisioning functionality provides an interface to provision phones on CS 1000 systems.

You access Phone Provisioning through the **Phones** link of the Element Manager navigator as shown in the following figure.

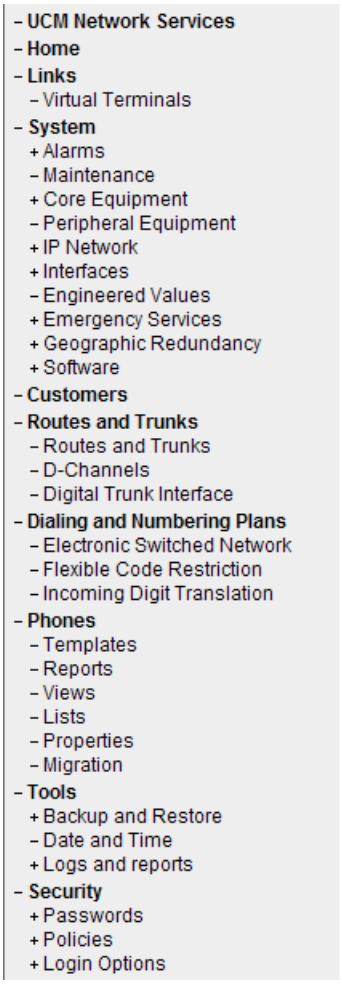


Figure 209: Phone Provisioning navigation

Use Element Manager to configure phones for the Call Server. The configuration information described in this chapter corresponds to the Command Line Interface (CLI) prompts and responses for Telephone Administration traditionally configured in LD 10, LD 11, and LD 12.

Additional information is retrieved from the Call Server for validation purposes corresponds to Print Routines traditionally performed in LD 20, LD 21, LD 22, and LD 117.

For more information about the overlays described in this chapter, see *Avaya Software Input Output Administration, NN43001-611,* and *Avaya Software Input Output Reference — Maintenance, NN43001-711*.

IP Attendant

The IP Attendant feature supports phone provisioning of type 3260 using the EM Phone Provisioning. The system supports a maximum of 63 attendant consoles.

Before you can manage IP Attendant consoles using the Phones page, the application must be enabled and configured using the IP Media Services configuration page. For information about configuring IP Media Services, see *Avaya Signaling Server IP Line Applications Fundamentals, NN43001-125*.

Limitations of deploying multiple Element Managers to manage a single Call Server

You can deploy more than one Element Manager to manage a single Call Server using Deployment Manager, but the EM Phone provisioning application (Phones) does not support this. The issues with duplicate Element Mangers are as follows:

- Changes made in Phones in one Element Manager are not synchronized with other Element Managers. You should perform a "Retrieve and Reconcile All" operation on other Element Managers to synchronize with Call Server. However, the non PBX fields (Subscriber and Template links) of a telephone are not updated even with this retrieval.
- Subscriber Manager considers these duplicate Element Manager applications as different Service Providers even though they are pointing to the same Call Sever. As a result, in some work flows you can have duplicate telephony accounts for the same telephone.

Feature Operation during upgrade

When you upgrade Element Manager to CS 1000 Release 7.0 or later, the process does not automatically upgrade the phone data. Use the following procedures to complete the upgrade.

Perform the following operations to upgrade from CS 1000 Release 6.0 to CS 1000 Release 7.0 or later.

Upgrading to CS 1000 Release 7.0 or later

1. Upgrade to CS 1000 Release 7.0 or later.
2. Launch Element Manager.
3. From the navigation tree, select **Phones > Properties**
4. On the Properties page, in the **Database Update** section, click **Update**.
5. Synchronize the data from the Call Server to the Phones database.

   For more information, see Retrieve Phones on page 332.

If you upgrade from CS 1000 Release 6.0 to CS 1000 Release 7.0 or later and you experience problems, such as accounts no longer associated with subscribers, perform the following procedure. These problems can occur if you redeployed elements, or if you used a redundant

Element Manager against a single call server, because these scenarios result in broken links between subscribers and accounts.

Upgrading to CS 1000 Release 7.0 or later and recreating accounts in Subscriber Manager

1. Upgrade to CS 1000 Release 7.0 or later.
2. Launch Element Manager.
3. From the navigation tree, select **Phones > Properties**
4. On the Properties page, in the **Database Update** section, click **Update**.
5. Synchronize the data from the Call Server to the Phones database.

   For more information, see Retrieve Phones on page 332.
6. Run the Migration utility to recreate accounts based on CPND names.

   Important:

   You must select the **Create New Subscribers** check box.

   For more information, see Migration on page 361.

You can follow the manual work around steps to bring back template information and link them to the corresponding phones.

You can create templates from existing phones. For more information, see Create a Template from an existing phone on page 300. With this procedure, you can create templates quickly, rather than creating them from scratch.

Use the Bulk Phone Edit procedure to link the selected phones with the template. For more information, see Update phones using the phone Templates on page 318.

System Properties Update

Database Update

When you click **Phones** for the first time, the application automatically updates the database in the background. You must perform the update before you manage telephones to retrieve configuration changes in packages, customer data blocks, and CPND customer blocks. You can configure telephones when the update finishes.

To manually update the database, click on the **Properties** link of the **Phones** branch of the Element Manager navigator and click **Update** in the **Database Update** section of the Properties Web page.

The Properties Web page appears, as shown in Figure 210: Properties Web page on page 294

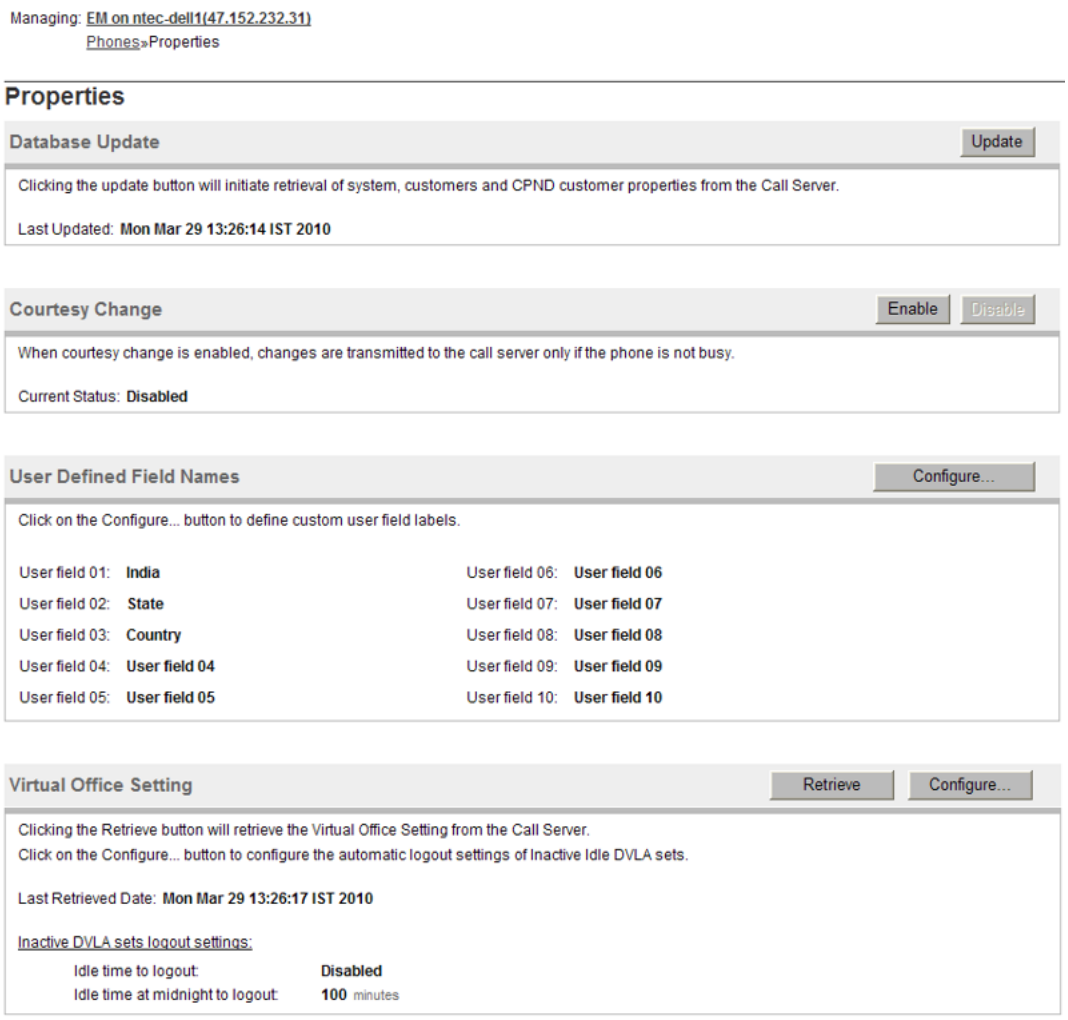


Figure 210: Properties Web page

The Last Updated field displays the timestamp of the last update performed.

Courtesy Change

The Courtesy Change feature checks the telephone busy/idle status before transmitting changes to the Call Server. If the telephone is busy, the change is not transmitted; the active call is disconnected, and the following error message appears: Telephone is busy. Changes are not transmitted.

Before a telephone call is transmitted to the Call Server, the LD 32 STAT command is used to check the idle/busy status of the telephone. If the telephone is busy, then the changes are not committed to the Call Server and you must perform the operation again.

Avaya recommends that you turn off this feature before doing a bulk import operation.

Enabling and disabling the Courtesy Change feature

You can turn the Courtesy Change feature on or off, from the existing Properties Web page.

To enable or disable the Courtesy Change feature, select the **Properties** link of the **Phones** branch of the Element Manager navigator, and select either **Enable** or **Disable**.

The Figure 211: Properties Web page on page 295 shows Courtesy Change on the Properties Web page.

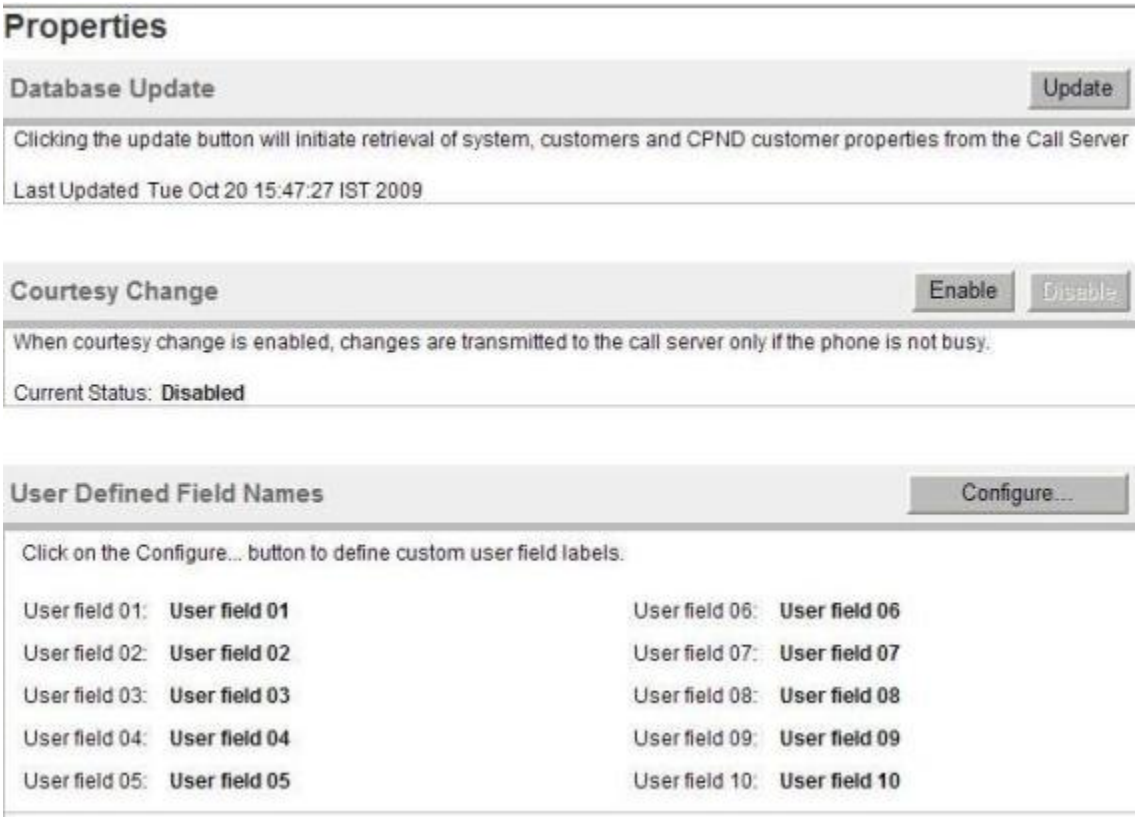


Figure 211: Properties Web page

Important:

Turning on the Courtesy Change feature significantly affects the performance of bulk add, delete, or import operations. Avaya recommends that you turn off the Courtesy Change feature before such operations.

Configuring user-defined field names

The user fields with default values User field 01, User field 02, User field 03, and User field 10 can be configured to a meaningful name, which can be a maximum of 30 alphanumeric

characters. The customized user field names are displayed in the Telephone Details Web page and the default user field names appear in the Telephone Details Web page. The values for the user fields have a maximum of 256 alphanumeric characters.

Configure user-defined field names

1. On the Properties Web page, click **Configure** .

   The Edit User Defined Field Names Web page appears.
2. Enter names for the default user-defined fields.
3. Click **Save** .

Important:

The default user field names are saved if no value is given. The maximum size of a field name is 30 alphanumeric characters.

The Virtual Office Setting section in the Properties Web page contains details of the current virtual office settings for idle DVLA sets.

The system supports the following two types of auto logout settings.

- Logout a DVLA Set after the specified idle time has elapsed.
- Logout a DVLA Set at midnight if the specified midnight idle time has elapsed.

Important:

The user can set the idle time in the range of 1 to 1440 minutes.

The system supports the following operations for Virtual Office Setting.

- Retrieve Virtual Office Setting
- Configure Virtual Office Setting

Important:

Only users with LD 117 permissions can perform the preceding operations.

To retrieve the Virtual Office Setting, use the following procedure.

In the Properties Web page, click **Retrieve** button.

The system retrieves the virtual office settings for idle DVLA sets from the Call Server and the details in the Virtual Office Setting section get updated.

Configure Virtual Office

To configure Virtual Office Setting, use the following procedure.

1. In the Properties Web page, click **Configure** button.

   The Edit Virtual Office Setting Web page appears displaying the current configuration.

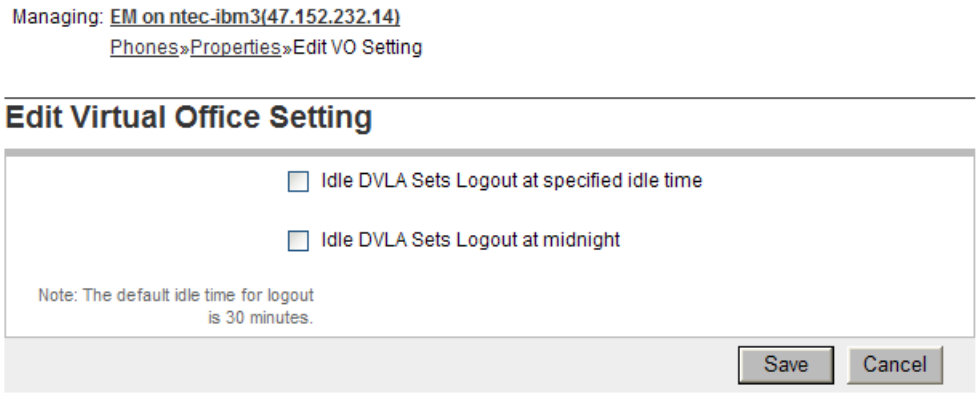


Figure 212: Edit Virtual Office Setting Web page

2. Select the check box corresponding to the options as required.

   The **Idle Time** field appears.

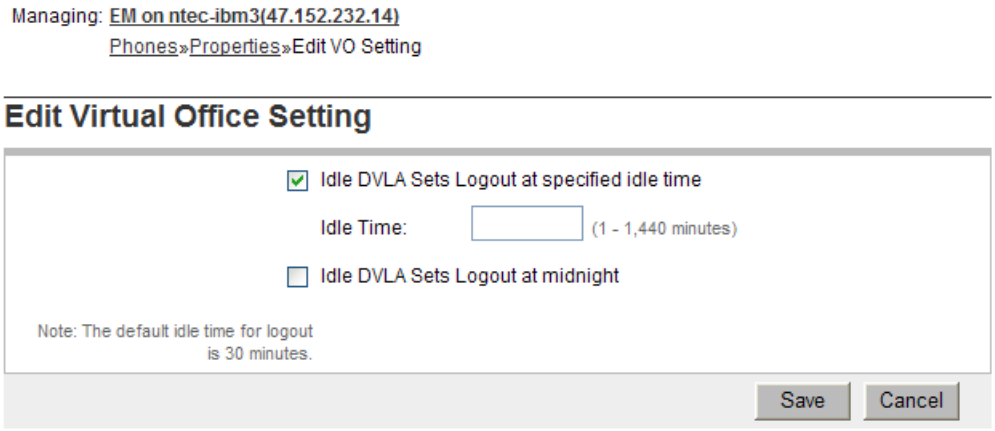


Figure 213: Edit Virtual Office Setting Web page

3. Enter the idle time in the **Idle Time** field.

   Important:

   The idle time must be a value between 1 and 1440.

4. To save the configuration , click **Save**.

   The page refreshes to display the Properties Web page.

Station Fast Sync feature

The Station Fast Sync feature keeps the Phones Database synchronized with the PBX. The 3260 phone type does not support this feature.

When a phone is modified on call server using CLI, then SNMP trap is sent from the Call Server to Element Manager. When Element Manager receives the notification, it retrieves changes or

deletes the TN/DN as required. This functionality is enabled by configuring the Element Manager IP address as an SNMP trap destination in LD 117. The EM IP address is configured automatically when EM Phones is launched for the first time. However, if changes from the CLI are not being reflected in EM Phones, Avaya recommends that you verify that the management trap destination is correct using LD 117. See *Avaya Communication Server 1000 Fault Management - SNMP, NN43001-719*.

A log entry is created for each Fast Sync notification received.

Important:

This feature is not applicable for LD 12.

Important:

A manual Retrieve and Reconcile All must be performed periodically to ensure data consistency with the Call Server. The automatic fast synchronization update relies on SNMP traps and overlay access to maintain the data. Blocked or dropped SNMP traps and overlay conflicts can result in a data mismatch between the Call Server and EM.

Templates

Use Element Manager to access Templates that contain attributes common to a CS 1000 phone type. After you create a template, use it to apply common attributes to a group of telephones, without having to repetitively define the same value for each telephone. In general, using a template is a more efficient method of adding large number of telephones than individually maintaining each telephone. Template support for 3260 set type (IP Attendant Console) but Subscriber Manager blocks the usage of this template.

To access the administration pages for Templates click **Phones > Templates** section of EM navigator.

The Templates Web page lists all available templates by name, the telephone type to which they apply, and the time and date of the last update. The action bar has buttons to add, export, import, and delete templates.

Important:

Due to performance considerations, the recommended maximum number of templates supported by the system is 1000.

Create a Template

To add a template, click **Add** on the Templates Web page. The Template Details Web page appears as shown in Figure 214: Template Details Web page on page 299. Select the telephone type to use for the Template.

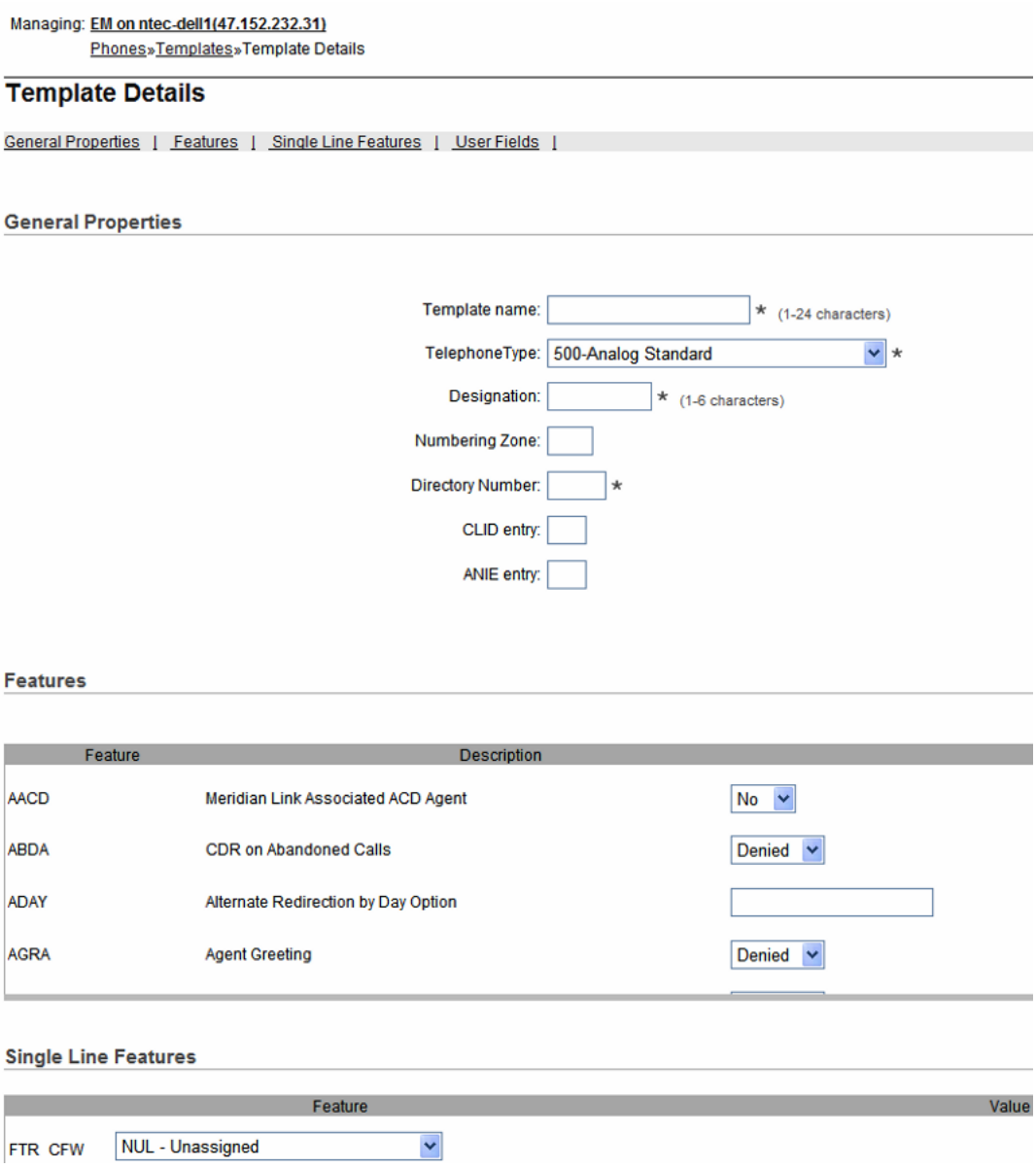


Figure 214: Template Details Web page

The fields marked with an asterisk (*) are mandatory.

The Template name identifies the template. If a template exists with the same name as specified, then an error message, "Template name already in use. Please specify another Template name." appears when you try to save the new template.

The templates are not system-specific; therefore, all the phone features and keys applicable to the selected phone type are available for configuration in the Template Details Web page. The available features and key features change based on the selected phone type.

Important:

Enter a partial DN as part of the key configuration parameter to enable a phone configured with this template to pick up a DN according to the partial DN.

Configure all required parameters, and click **Save** to save the template and return to the Templates Web page. The view refreshes to display the newly-added template.

Important:

The status of the Validation appears, listing validation errors that occur. If validation errors occur, repeat the relevant sections of this procedure to correct the errors.

After you create a template, you can use it to add telephones to the system. When you use a template to add a telephone, only those keys and features that are valid for the system in context appear in the Phone Details Web page.

Create a Template from an existing phone

You can define a new template from an existing telephone configuration.

Select a telephone to convert to a phone template and view the new template in the Template Details Web page.

Save a phone as template

1. To open the Search for Phones Web page, click the **Phones** branch of the Element Manager navigator.
2. To save as a template, select a telephone from the **Search Result** section of the Search for Phones Web page.

   Note:

   You can create a template only from one telephone. An error message appears if you select multiple phones for creating a template.
3. From the **More Actions** list, select **Save As Template** as shown in Figure 215: Search For Phones Web page with option to save a phone as template on page 301.

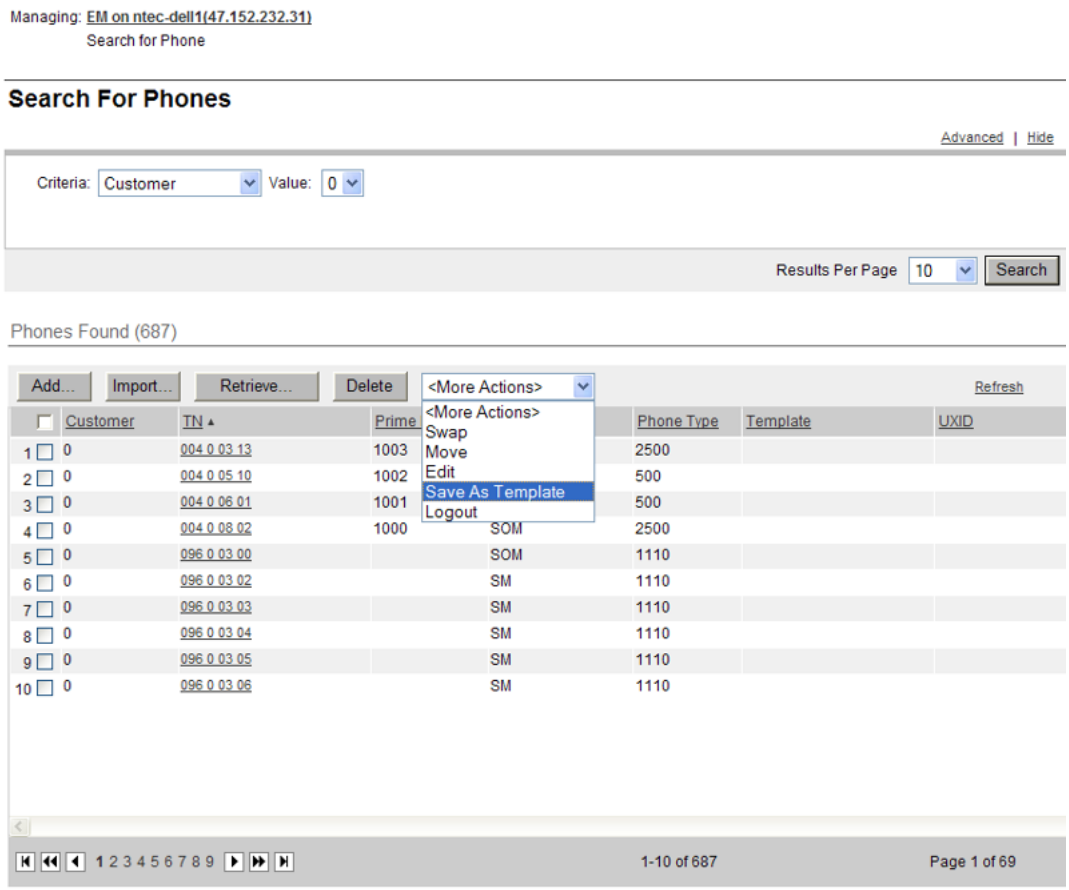


Figure 215: Search For Phones Web page with option to save a phone as template

The Template Details Web page appears as shown in Figure 216: Template Details Web page with the select phone converted into a template on page 302 .

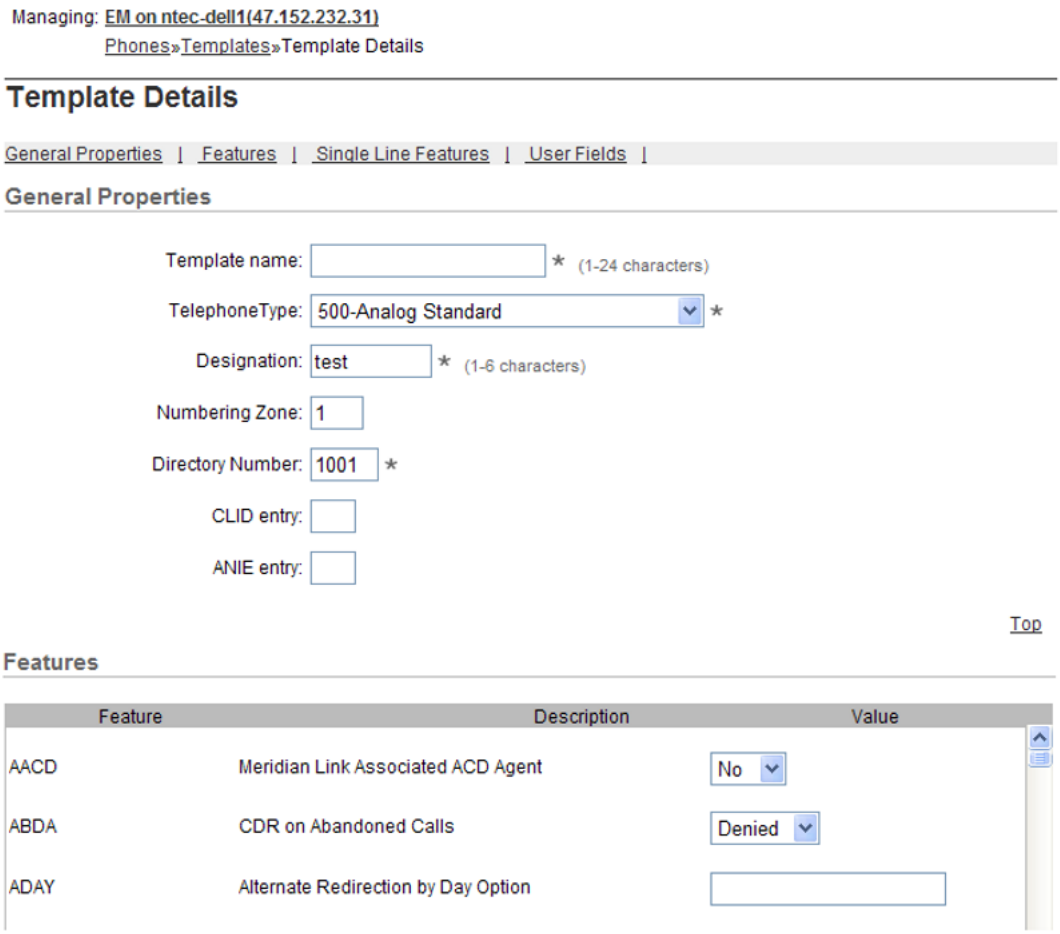


Figure 216: Template Details Web page with the select phone converted into a template

4. Click **Save As** .

   The page refreshes to display the Save Template Details Web page.
5. In the **Template name** box, type a name for the template.

   Note:

   The Template name must be unique. If you type an existing template name, an error message appears.
6. To save the template, click **Save** .

   The Search for Phones Web page appears. The information of the selected phone is converted into a telephone template.

View a Template

To view template details, click the template name link in the Templates Web page. The Template Details Web page appears displaying the selected template. You can make changes

to the template and save the changes. To save the template with a different name click **Save As** . The Save Template Details Web page appears, as shown in the following figure. Enter a unique name and click **Save** .

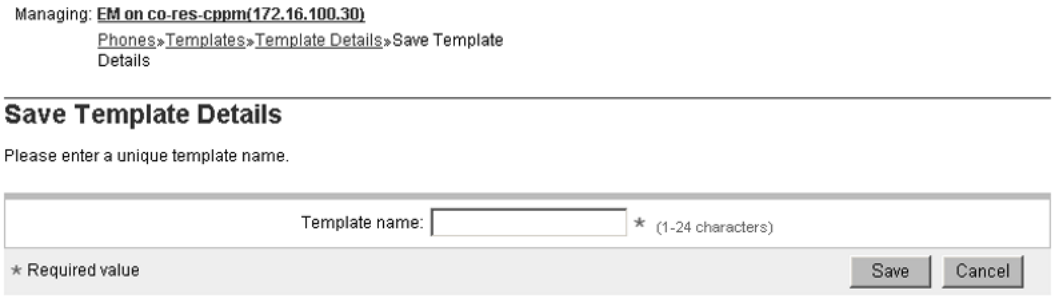


Figure 217: Save Template Details Web page

Update a Template

To update a template, click the template name link in the Templates Web page. The Template Details Web page appears displaying the selected template.

Make the required modifications to the template and save the changes.

Note:

When you update a Template, the telephones associated with this Template are not automatically updated. See, Update phones using the phone Templates on page 318.

Delete a template

Select any template from the Templates Web page and click **Delete** to remove the template.

You must confirm the deletion. When you click **OK**, the selected template is deleted immediately. If you click **Cancel**, the deletion is cancelled and the Templates Web page appears.

Important:

When you delete a template, its association with telephones is removed, but the telephones are not deleted.

Export and Import Templates

You can export and import templates in CSV format.

Template data configured at one EM is not available for every EM in the UCM Common Services framework. You must perform a manual export and import procedure to share this data between various Element Managers.

You import and export Templates from the Templates Web page as shown in Figure 218: Import and Export Templates on page 304.

Important:

No data validation occurs when you import a template. You must ensure that proper values are present under all fields in the CSV file that you import.

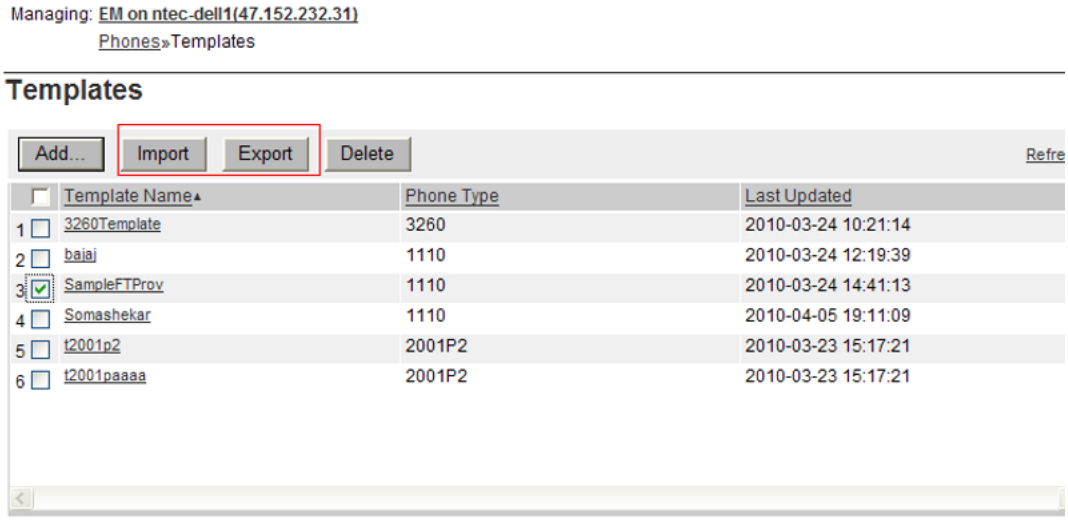


Figure 218: Import and Export Templates

You can use a comma-delimited ASCII text file, with a file extension of CSV as the data file. The first line or record of the file must contain the names of the fields that you import. You must enclose each field in the record in quotation marks. The first field in the data record is template name and is used as the key during the import. Existing templates are updated if a template with the same name exists. If the template name does not exist, a new template is created.

The following are the mandatory fields required for a template import:

- TEMPLATE_NAME
- PHONE
- DES

Depending on the imported telephone type, other mandatory fields are required. For example, in the case of an IP Phone, **Zone** is a mandatory field. If any of the mandatory fields are missing in a data record, the import process ignores that data record. The other data requirements for import of templates, as well as the list of field names used for import of templates, are similar to Import Telephones. See, Import Telephones on page 324.

Important:

You cannot import CPND because templates do not support them.

You can import Admin fields or the user fields also as Templates support these. The following is a sample of data in CSV format.

"TEMPLATE_NAME","PHONE","DES","ZONE","KEY0",
"USERFIELD1","USERFIELD2","USERFIELD3","USERFIELD4","USERFIELD5","USERFIELD6","USERFIELD7","USERFIELD8","USERFIELD9","USERFIELD10" "1110 for HR dept","1110","Test","000","SCR 2",
"Johny","Jimy","Tony","Clinton","Obama","Bush","Keny","Kitty","Tina","Ken"

In the above sample data, Key0 is configured with partial DN.

The UI reports errors encountered during the import operation. You can modify the CSV file and try the import again.

The template import is shorter than the telephone import operation so no log file is written.

Export Templates on page 305 describes the step you complete to export one or more templates.

Export Templates

1. On the EM navigator, click the **Templates** link .

   The Templates Web page appears.
2. Select the list of templates to export.
3. Click **Export** .

   The Bulk Export for Templates Web page appears as shown in Figure 219: Bulk Export for Templates Web page on page 306.

Figure 219: Bulk Export for Templates Web page

4. To download and save the exported data to your computer, click the **Download Exported Templates** link .

Import Templates

Import Templates on page 306 describes the steps to import one or more templates.

Import Templates

1. On the EM navigator, click the **Templates** link.

   The Templates Web page appears.

2. Click **Import** .

   The Import Templates Web page appears as shown in Figure 220: Import Templates Web page on page 307.

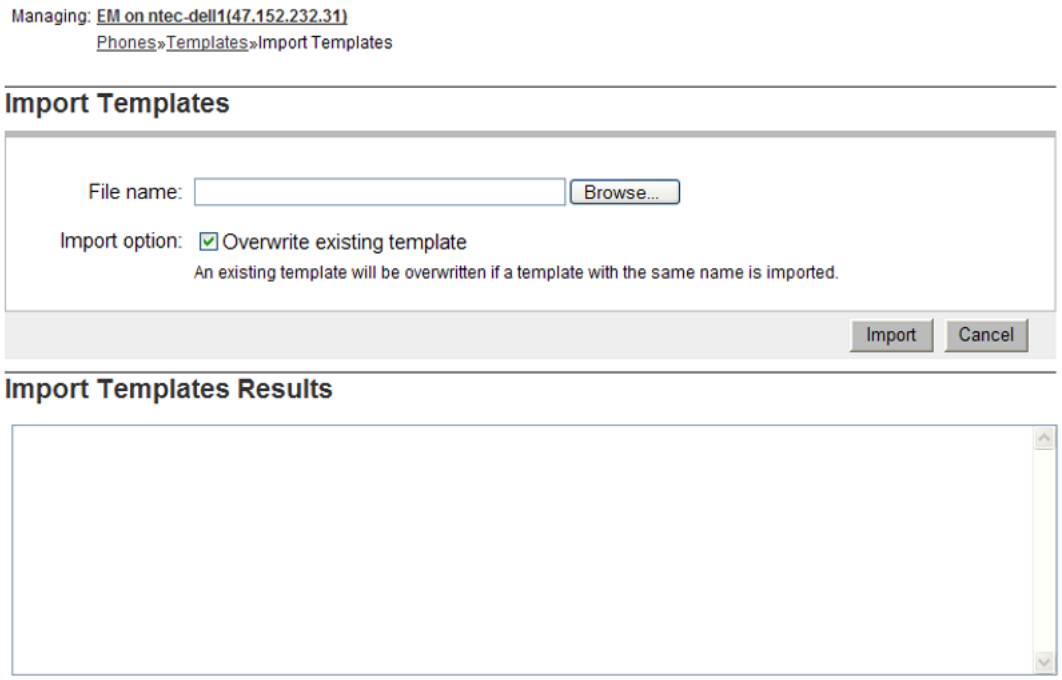


Figure 220: Import Templates Web page

3. Specify the source file name by performing one of the following steps:
   - Type the path and file name of the source file in the CSV file name box.
   - Click **Browse** to locate and select the file.
4. To perform the Import operation, click **Import** .

Search Phones

You access the Phones functions in Element Manager from the Search for Phones Web page. Search for phones based on the following criteria:

- **Prime DN**
- **Phone Type**
- **Terminal Number**
- **Designation**
- **Customer**
- **Template**
- **UXID**
- **Idle Time**

For example, to search for a telephone type, select **Phone Type** as the criteria and a telephone type from the **Value** list. Search for phones on page 308 describes searching for telephones using **Template** as the criteria.

Search for phones

1. To open Search for Phones Web page, as shown in Figure 221: Search for Phones Web page on page 308, click the Phones branch of the Element Manager navigator .

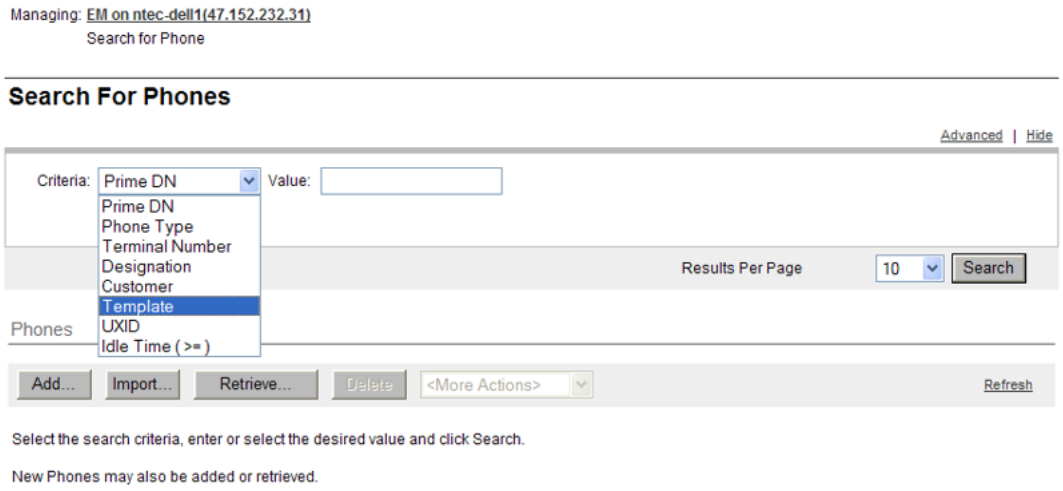


Figure 221: Search for Phones Web page

2. Select **Template** as the criteria from the **Criteria** list.

   Important:

   If you select **No template** as the criteria then the search returns all phones not associated to a template.

3. Type a **Value** for the template to search for.
4. Click **Search** .

   The Search for Phones Web page displays the telephones that match the specified Template as shown in Figure 222: Search for Phones Web page on page 309.

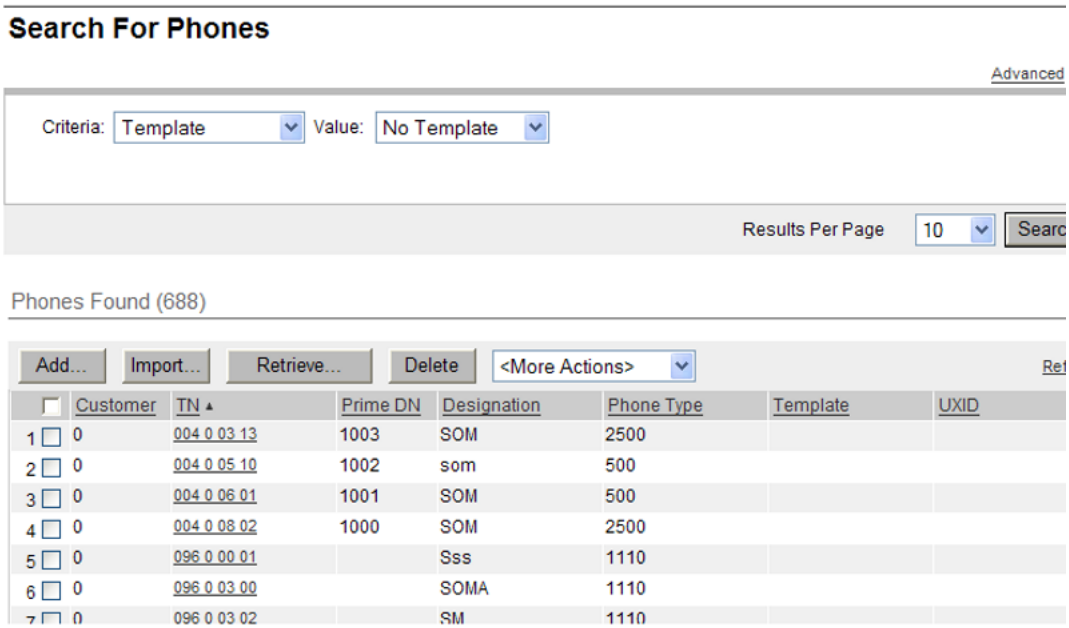


Figure 222: Search for Phones Web page

To search for a phone, based on the Idle Time criteria, use the following procedure.

Important:

Search operation based on the Idle Time criteria can be performed only for sets which belong to the DVLA class of service.

1. In the Search For Phones Web page, select **Idle Time (>=)** from the drop down available corresponding to the **Criteria** field.
2. Type the required value in the **Value** field.

   The following figure shows the Search For Phones Web page.

Figure 223: Search For Phones Web page

Important:

You must enter a value between 1 and 1440 as the idle time. If you enter an invalid value, a validation error occurs.

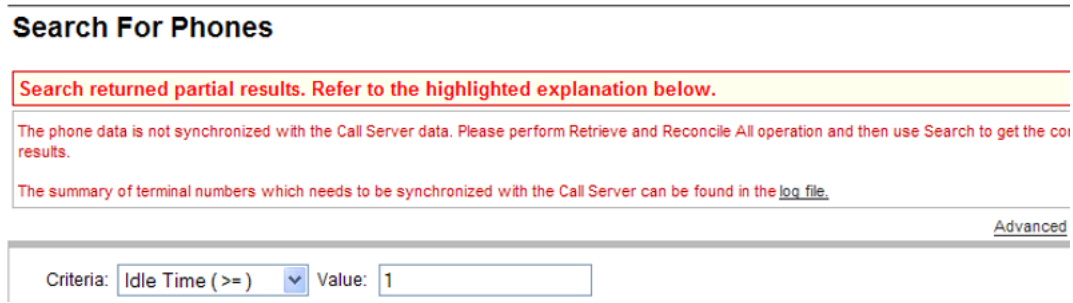
3. Click **Search**.

   The page refreshes to display the results matching the search criteria.

   Important:

   If the phone data is not synchronized with the Call Server, then the search returns partial results. Click the **log file** link to view the list of phones not present in the database.

   The following figure shows the partial result returned.



To search using additional criteria, click **Advanced** on the top right corner. The Advanced Search for Phones Web page appears, as shown in Figure 224: Advanced Search for Phones Web page on page 311.

Enter the criteria for the advanced search and click **Search**.

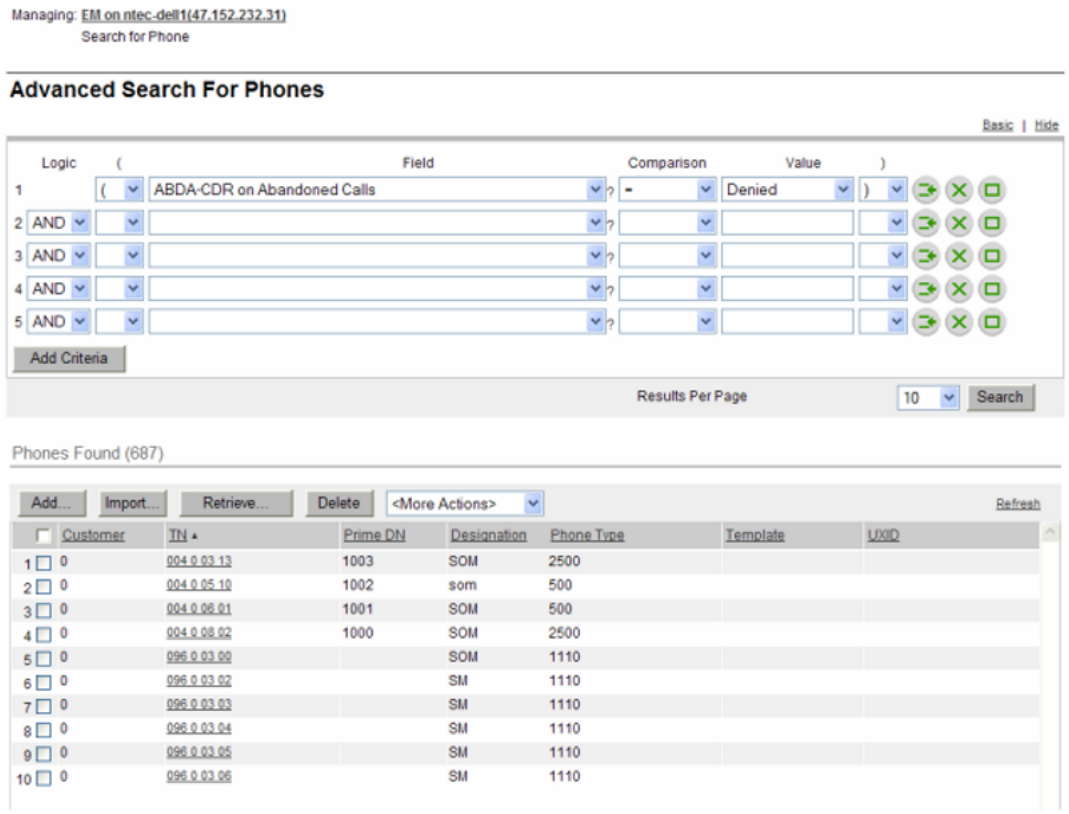


Figure 224: Advanced Search for Phones Web page

Important:

If you select LIKE or NOT LIKE operator under the **Logic** column and enter a value (for example, ABC) without the % wild card, % is appended for this value during the search (for example, %ABC%). This option behaves like the CONTAINS operator.

Add Phones

To add telephones, use the following methods.

- Add single or multiple telephones
- Add phones using a template
- Add phones using copy from TN option

To add a single telephone, perform the steps in Add Single Phone on page 311.

Add Single Phone

1. On the Search for Phones Web page, click **Add** .

The New Phones Web page appears.

2. Type 1 in the **Number of phones** box.
3. From the **Customer** list, select the number with which this telephone is associated.
4. Select the **Phone Type** from the list.
5. Select the check box corresponding to **Default value for DES** .
6. Type the value in the corresponding field.
7. Select **Automatically assign TN** to automatically assign the next available TN from the starting TN value.

   You can click the Magnifying Glass to look up a TN.
8. If the telephone type is analog, select **Automatically assign DN** to automatically assign the next DN from the starting DN value.

   Note:

   You can click the Magnifying Glass to look up a DN.

   Note:

   You can select **Automatically assign DN** for analog (500/2500-type) telephone types and while creating telephones and templates having a partial DN.
9. Click **Preview** .

   The Phone Details Web page appears, as shown in Figure 225: Phone Details Web page on page 313.

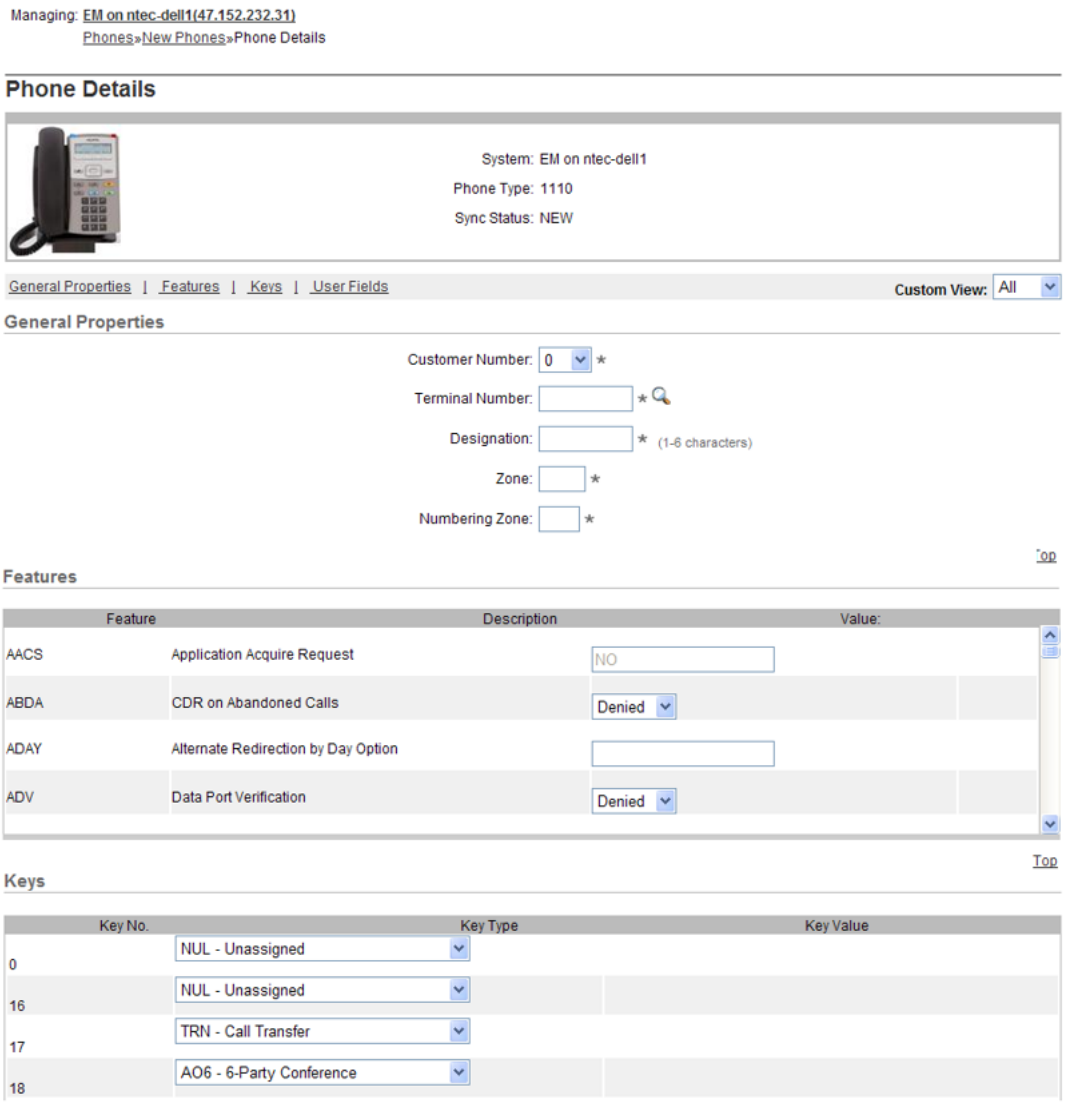


Figure 225: Phone Details Web page

10. If necessary, you can change the **Customer Number** from the default number you selected on the New Phones Web page.
11. If **Terminal Number** is empty, click the magnifying glass icon and select an available TN.
12. Enter or update the DES value in the **Designation** field.
13. Choose the desired features in the **Features** section.
14. Choose the desired keys in the **Keys** section.

    To program keys using the telephone GUI (graphical user interface), see Program Phone Keys on page 317.

Note:

If the telephone type is analog, the **Keys** section is not available.

Note:

The Match DN Web page is applicable only for Single Call Ringing (SCR). Search **Match DN** by clicking the Phone icon. When you search Match DN in the context of Digital and IP Phones, all UEXT telephones with same DN appear. If the context is UEXT, all the Digital and IP Phones appear in the Match DN page. When you select **Single Call Ringing (SCR)** for Key 0, the telephone icon (Match DN) appears. If you select any telephone and click **Assign** , FDN, HUNT, NCOS, TGAR, and CLS features are copied to the telephone that you are configuring or for which you are editing information.

15. To add user-defined fields, click **User Fields** .
16. To validate the new telephone, click **Validate** .

    The status of the Validation appears, listing validation errors that occur. If validation errors occur, repeat the relevant sections of this procedure to correct the errors.

    Important:

    To cancel the current operation and redirect to the Phone Search Web page, click **Cancel** .
17. To add the new telephone to the database, click **Save** .

On the New Phones Web page, if you select **Copy from TN** as the **Phone Type** , the new telephone uses the properties of the specified TN, with the following exceptions.

- The **Default value for DES**, if specified, takes precedence.
- The **Automatically assign DN**, if enabled, takes precedence.
- The **Automatically assign TN**, if enabled, takes precedence.

In the New Phones Web page, if you select **Template** as the **Phone Type** , the new phone uses the properties of the specified template, with the following exceptions.

- The **Default value for DES**, if specified, takes precedence.
- The **Automatically assign DN**, if enabled, takes precedence.

The Template field displays all templates. To add a telephone, select a template from the list.

When Auto Assign DN is on and you specify a starting DN, the starting DN overwrites the existing partial DN specified in the template. The message "The current DN is the specified starting DN. It is not the partial DN specified in the template" is displayed indicating that the starting DN overwrites the partial DN specified in the template.

When Auto Assign DN is switched off, a Partial DN specified in the template becomes the DN. The Add Phones operation fails unless the user corrects the DN. The message "The current DN is the partial DN specified in the template. The DN must be modified in order to successfully add the phone." appears.

To add multiple telephones, perform the steps in Add Multiple Phones on page 315.

Add Multiple Phones

1. On the Search for Phones Web page, click **Add** .

   The New Phones Web page appears.

2. In the **Number of phones** field, enter the number of telephones to add .

   You can add up to 100 phones at a time.

   Important:

   If the Phone Type is **IP Attendant 3260**, you can add a maximum of 63 phones.

3. In the **Customer** list, select the customer to which these telephones are associated.
4. Select the **Default value for DES** option, and type the value in the text box.
5. Select **Default value for Zone** , and type the value in the text box.
6. Select **Automatically assign DN** to automatically assign the next available DN.
7. Select **Automatically assign TN** and type the value in the starting TN box; or, you can leave the value blank and the system assigns the next available TN (Loop, Shelf, Card, Port or Unit) to the specified telephones as defined in the Hardware database for the system.
8. Click **Preview** .

   The Preview Phones Web page appears, as shown in Figure 226: Preview Phones Web page on page 315.

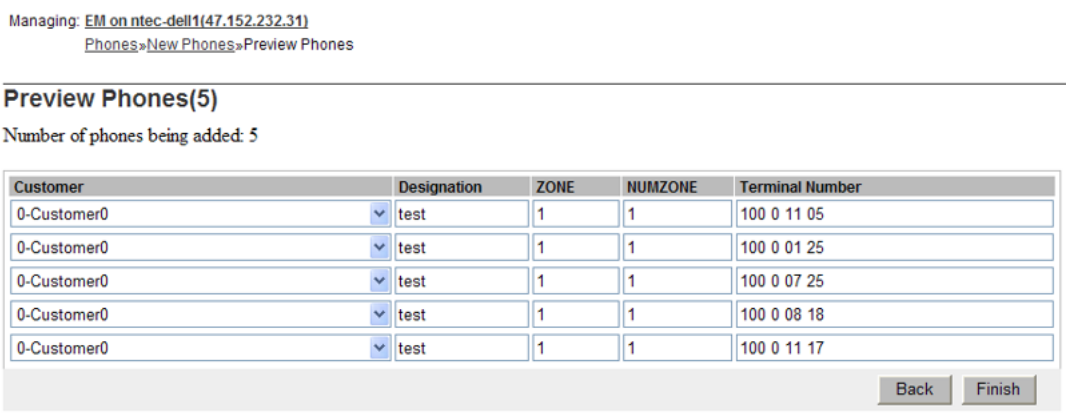


Figure 226: Preview Phones Web page

This Web page lists the attributes of each new telephone based on the selections entered in the New Phones Web page in previous steps.

The Preview Phones page lists the desired number of telephones with automatically assigned TN to each telephone either from the starting value entered or from the automatically assigned values.

9. If the **Customer** number is incorrect, select the correct value from the list.
10. If the **DES** field is empty or incorrect, type the correct value.
11. For an analog telephone, If the **DN** field is missing or incorrect, type the correct value.
12. If the **TN** field is missing or incorrect, type the correct value.
13. Click **Finish** to add the telephones to the database.

You can select a template to add multiple telephones.

To add multiple analog phones when Auto Assign DN is on and when the starting DN is specified, the DNs are used from the unused DN list of the call server. For example, if the starting DN is 100 and the user adds three phones then 105, 115, 116 could be the DNs if they are the next available free DNs for the given starting DN.The DNs appear in the Preview Phones Web page and you can edit it.

To add multiple analog telephones when Auto Assign DN is switched off, the Partial DN specified in the template becomes the DN. Adding multiple telephones fails unless you correct the DN. The message "The current DN is the partial DN specified in the template. The DN must be modified in order to successfully add the phone." appears.

To add multiple digital or virtual telephones when Auto Assign DN is switched on and when starting DN is specified, the starting DN is incremented and used. For example, if the starting DN is 100 and you try to add three telephones, then 100, 101, and 102 are the DNs. The DNs do not appear in the Preview Phones Web page so you cannot modify the DNs.

To add multiple digital or virtual telephones when Auto Assign DN is switched off, you cannot use the template with partial DN for adding multiple digital or virtual telephones. The error message "Multiple phone addition is not allowed since the template selected has a partial DN" appears indicating that this scenario is not allowed. However, no restriction is placed on adding telephones if the template does not contain a partial DN.

The maximum available list of DNs and TNs are displayed. If the user selects Auto Assign DN and TN, and the system cannot obtain the list, then the system displays an error message. The error message is displayed for those phones for which no free TN or DN could be obtained.

Important:

When the system searches for terminal numbers (either for a single terminal or for multiple units), the search looks for unused units on line cards that already exist with the correct type. It is not possible for the system to select an unused card because the location of a new line card cannot be determined automatically. Within the Command Line Interface (CLI) the user can create a new card explicitly, with no units equipped, by using overlay 10 or 11 as appropriate, to configure a CARDSLT for single line terminals (500 sets) or CARDMLT for multi-line terminals (digital or IP sets). Once you create the card the search tool will find unused units on that card.

Program Phone Keys

You can program telephone keys by using a graphical image of the telephone.

You can program telephone keys from the Phone Details Web page by using the graphical image of the telephone, which appears when you click on the telephone image at the top left of the page.

Programing phone keys using phone graphical interface

1. In the **Search Result** section of the Search for Phones Web page, click the telephone to be updated.

   The Phone Details Web page appears.
2. Click on the telephone image at the top left of the page.

   The graphical interface for the selected telephone appears.
3. Click the key button of the telephone you want to program.

   The select box for the selected key of the **Keys** section of the Phone Details Web page appears highlighted.
4. Change the key configuration as required.
5. Click **Finish** to add the telephone.

   The window closes and the Search for Phones Web page appears.

There are help, minimize, maximize, and close buttons on the title bar of the Phone Graphical Interface window. Click the question mark, to open the corresponding help page for the telephone displayed, .

Use the minimize and maximize buttons to hide and display the graphical image window. Hover the mouse over the key buttons on the image to display a tool tip with the key number and the current configured value.

When minimized, the Phone Graphical interface title bar remains visible. You can move the title bar so it does not obscure your view of the Phone Details Web page. However, you cannot drag and place the title bar on top of the navigation pane of the browser.

You can configure telephones with a key-based add-on module. Use the navigation button at the bottom to navigate to the extended keys for the telephone.

Edit Phones

Use the Edit feature to edit a single telephone or multiple telephones.

Edit single or multiple phones

Click the **Phones** branch of the Element Manager navigator to open the Search for Phones Web page.

To edit a single telephone or multiple telephones, perform the following procedure.

Update phones using the phone Templates

The association of telephones to a template simplifies the bulk change procedure. Use this association to enable a change to the template content to be applied to all telephones that use the template.

The Bulk Phone Edit Web page allows the user to update the telephone from templates. The value **Template** of the edit **Field** list, enables the user to update the telephone based on the value in the template.

In the edit **Field** , if you select **Template** and click **Add** , the **Old Value** field displays an asterisk (*). The **New Value** field displays all templates configured for the selected telephone type as seen in Figure 227: Bulk Phone Edit Web page on page 318.

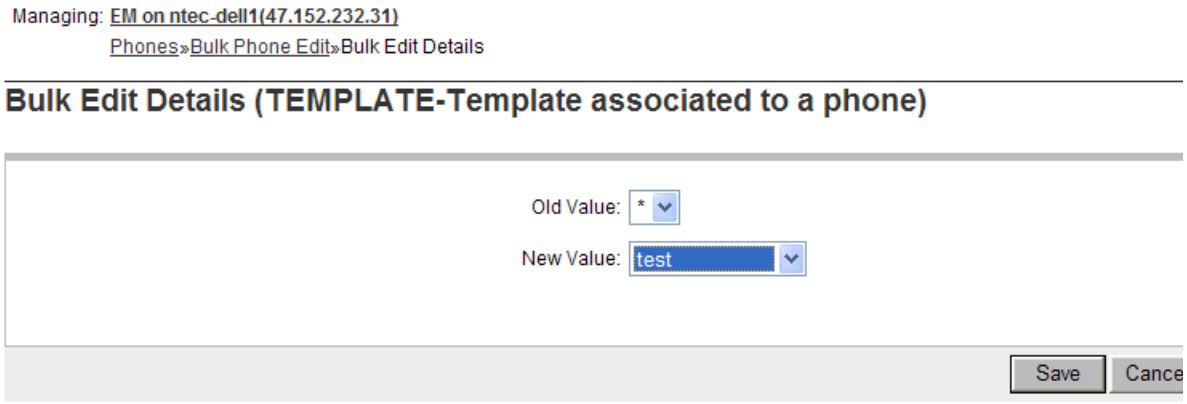


Figure 227: Bulk Phone Edit Web page

The template is considered the master during this update. All configured telephone attributes are overwritten with the attributes in the selected template. The CPND name configured in the telephone is retained during the update.

If the telephones selected for updating are of different telephone types, the **Template** field is not available in the edit **Field** list. You cannot change the following telephone properties when

you update using Templates. These properties are different for every telephone and updating it from template is not supported.

- **Designator (DES)**: This property is part of the General Properties section of the telephone details page.
- **Station Control Password (SCPW)**: This property is part of the Features section of the telephone details page.
- **Directory number** parameter of any key feature.

In addition, certain properties are not part of the template and can be changed in the telephone.

- **Terminal Number (TN)**: This property is part of the **General Properties** section of the telephone details page.
- **Call Party Name Display (CPND)**: This property is part of the **Keys** section of the telephone details page.
- **Voice Mail Box (VMB)**: This property is part of the **Keys** section of the telephone details page.

If a template has a partial DN configured, you cannot update a telephone with the Template by using the Edit function. The error message "Editing phones is not allowed since the template selected has a partial DN" appears. However, no restriction is placed on editing if the template does not contain partial DN.

Perform this procedure to associate a template with telephones that are not associated with a template.

Associating a Template to Phones

1. From the Search for phones on page 308 Web page, search for telephones that are not associated with a template.
2. Sort the telephone list by telephone type.
3. Select telephones to update.
4. Select **Edit** from the **<more actions>** list.

   The Bulk Phone Edit Web page appears.
5. In the edit **Field** , specify the value to update as **Template** and click **Add** .

   The Bulk Edit Details Web page appears.
6. In the **Old Value** field, select Asterisk (*****).
7. In the **New Value** field, select the template to associate with the telephone.
8. Click **Save** to complete the edit.

   OR

   Click **Cancel** to undo changes and return to the Bulk Phone Edit Web page.

Important:

When you update the telephone, Element Manager may send an update to the account in Subscriber Manager depending on the attributes you updated.

Phone properties that can change without breaking the Template association

Certain properties differ for various telephones; therefore, changing these properties does not break the telephone-to-template association. The following is a list of properties:

- **Designator (DES)**: This property is part of the **General Properties** section of the phone details page.
- **Station Control Password (SCPW)**: This property is part of the **Features** section of the phone details page.
- **Directory number** parameter of any key feature.

In addition, certain properties are not part of the template, and can be changed in the phone.

- **Terminal Number (TN)**: This property is part of the **General Properties** section of the phone details page
- **Call Party Name Display (CPND)**: This property is part of the **Keys** section of the phone details page.
- **Voice Mail Box (VMB)**: This property is part of the **Keys** section of the phone details page.

Employee reference field support when exporting and import phone database

Including this attribute in the export and import tools enables you to retain important data that is not persisted on the call server such as the employee reference and template ID. You can export and the import employee reference fields along with other supported telephone fields. The employee reference field stores the ID of the subscriber associated with the telephone. This field is the link between a telephone in EM Phone Provisioning and a subscriber in Subscriber Manager.

When you need to retain this offline data, perform Retaining offline data on page 321.

Retaining offline data

1. Export the Phones database as a CSV file with the mandatory fields (TN, CUSTOMER, PHONE, DES), Template ID, and Employee Reference field.
2. Perform the Retrieve and Reconcile procedure to populate the phone database.
3. Import phones from the CSV file generated in step 1 to re-establish the link from telephone to template and telephone to subscriber.

Export and Import of employee reference field

Certain limitations apply while importing the EMPLOYEEREFERENCE field. In the import CSV file, if you update the EMPLOYEEREFERENCE field of an existing telephone, the following work flow occurs:

- EM Phone Provisioning updates the employee reference field in the telephone database.
- An update account notification is sent to Subscriber Manager. Because the notification is not an update to an existing account, Subscriber Manager ignores this notification.
- Run the Account Synchronization operation to synchronize the account differences between EM phone provisioning and Subscriber Manager. Account synchronization resynchronize the accounts as follows:
  - Account Synchronization finds that the older account exists in Subscriber Manager but not in EM phone provisioning. This account is automatically removed from Subscriber Manager.
  - Account Synchronization identifies a newer account in EM phone provisioning but not in Subscriber Manager, but the account has a subscriber ID in the directory. The newer account is automatically created in Subscriber Manager.

Generating a report and exporting phones with employee reference in the selected report field

1. Select **Report** from the **Phones** branch of the EM navigator.
2. Click **Add** to add a Report profile.
3. In the **Field Selection** section, select the fields to include in the report. Include EMPLOYEEREFERENCE field as well.
4. In the **Custom Criteria** section, select the criteria to determine which telephones are included in the report.
5. Select **CSV** as the report format from the **Report Format** list.
6. Click **Generate Report** .

The Download Generated Report Web page appears.

7. Download the report.
   - EMPLOYEEREFERENCE field is included in the generated report.
   - All telephones linked to a subscriber have a value for the EMPLOYEEREFERENCE field.
   - All telephones not linked to a subscriber do not have a value for the EMPLOYEEREFERENCE field.

   For more information, see Reports on page 334

Generating a report and exporting phones with employee reference field as the criteria.

1. Select **Report** from the **Phones** branch of the EM navigator.
2. Click **Add** to add a Report profile.
3. Select the fields to include in the report.
4. In the **Custom Criteria** section, select the EMPLOYEEREFERENCE field.
   - The corresponding **Value** field changes to a text box.
   - The corresponding **Comparison** list contains only the equal to (=) operator.
5. Enter a value in the **Value** field.
6. Select **CSV** as the report format from the Report Format list.
7. Click **Generate Report** .

   The Download Generated Report Web page appears.
8. Download the report.
   - EMPLOYEEREFERENCE field is in the generated report.
   - All telephones linked to a subscriber have a value for the EMPLOYEEREFERENCE field.

   For more information, see Reports on page 334

Importing a new phone with employee reference field

1. Modify the generated CSV, and add a new telephone with a valid employee reference field.
2. Click **Import** on the Search for Phones Web page.

   The Import Phones Web page appears.
3. Specify the name of the source file by performing one of the following steps:
   - Type the path and name of the file in the import source file text box
   - Click **Browse** to locate and select the file.
4. Click **OK** to import the file.

The Import Status Web page appears indicating the success or failure of the import.

5. Click **Common Manager** to go to UCM home page.
6. Click the **Subscribers** link in UCM.

   The Search for Subscribers Web page appears.

7. Enter the subscriber's last name in the **Name** field of the search criteria, and click **Search** . Use the name of the subscriber whose ID you used in step 1.

   The Search for Subscriber Web page appears with search results that match the search criteria.

8. Click the name of the subscriber.

   The Subscriber Details Web page appears with a new account added to the account list.

Importing an existing phone with no update to employee reference field

1. Modify the generated CSV to update an existing telephone.

   Update the DN of Key 0 so that the change is visible in Subscriber Manager.

2. Click **Import** on the Search for Phones Web page.

   The Import Phones Web page appears.

3. Specify the name of the source file by performing one of the following steps:

   - Type the path and name of the file in the import source file text box
   - Click **Browse** to locate and select the file.

4. Click **OK** to import the file.

   The Import Status Web page appears indicating the success or failure of the import operation.

5. Click **Common Manager** to go to UCM home page.
6. Click the **Subscribers** link in UCM.

   The Search for Subscribers Web page appears.

7. Enter the subscriber's last name in the **Name** field of the search criteria and click **Search** . Use the subscriber name that you used in step 1.

   The Search for Subscriber Web page appears with search results that match the search criteria.

8. Click the name of the subscriber.

   The Subscriber Details Web page appears with the DN changes made to the account in the account list.

Importing an existing phone with updated employee reference field

1. Modify the generated CSV to update an existing telephone.

Update the employee reference field to another valid subscriber.

2. Click **Import** on the Search for Phones Web page.

   The Import Phones Web page appears.

3. Specify the name of the source file by performing one of the following steps:

   - Type the path and name of the file in the import source file text box
   - Click **Browse** to locate and select the file.

4. Click **OK** to import the file.

   The Import Status Web page appears indicating the success or failure of the import.

5. Click **Common Manager** to go to UCM home page.
6. Click the **Subscribers** link in UCM.

   The Search for Subscribers Web page appears.

7. Enter the subscriber's last name in the **Name** field of the search criteria, and click **Search** . Use the subscriber name that you used in step 1.

   The Search for Subscriber Web page appears with search results that match the search criteria.

8. Click the name of the subscriber.

   The Subscriber Details Web page appears with no changes made to the account in the account list. No changes are made to the account list of the subscriber whose employee reference field you used in step 1.

Import Telephones

You can import telephones into the telephone database by using the import function. Use the Import Telephones feature to import telephone data into the database from a comma-separated value (CSV) file. The Import Telephones Web page as shown in Figure 228: Search for Phones Web page on page 325 appears when you click the **Phones** link in EM navigator and then click **Import** on the Search for Phones Web page.

The Import Template feature accepts phone features, phone keys, and ten user defined attributes (USERFIELD1, USERFIELD2, USERFIELD3, and USERFIELD10) in the CSV format for adding and updating a template.

Important:

While entering values in the Userfields, ensure that the values are within double quotes (") and the userfield value itself does not contain any double quote (").

Figure 228: Search for Phones Web page

The Import Telephones Web page appears, as shown in Figure 229: Import Telephones Web page on page 325.

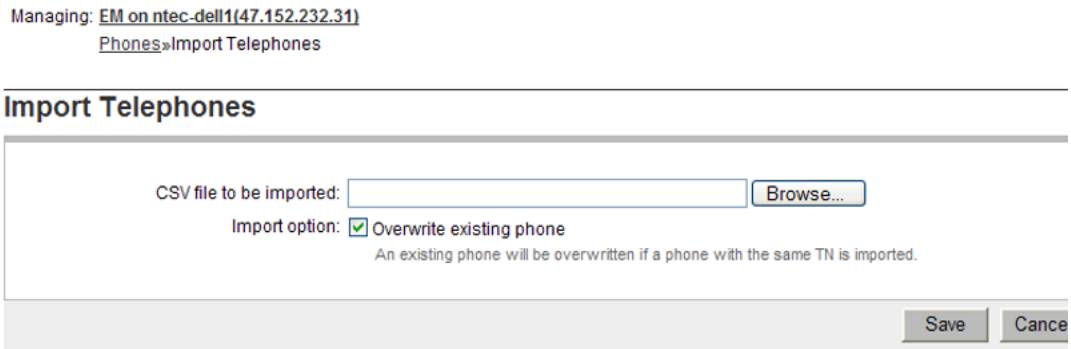
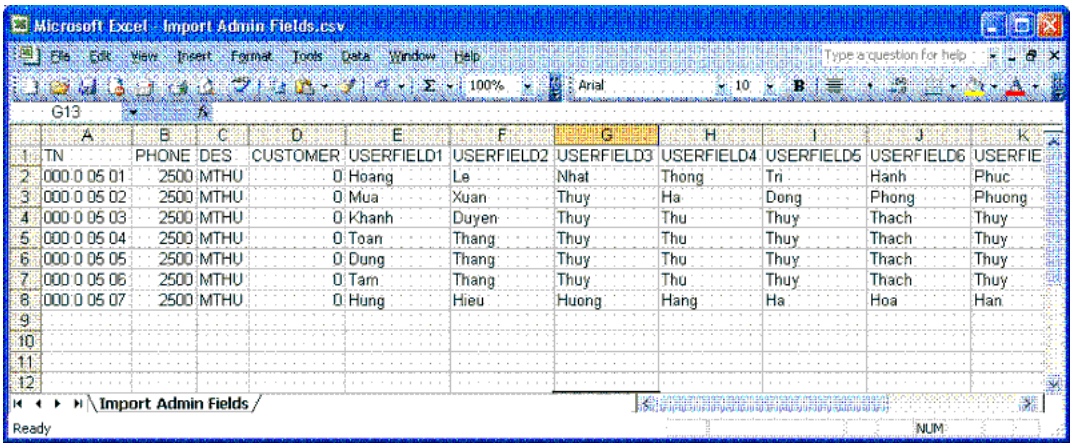


Figure 229: Import Telephones Web page

Specifications for CSV file

- The data file must be in CSV format.
- The first line in the CSV file must contain a list of fields to import.
- Subsequent lines in the CSV file must contain data values for each field being imported and are in the same order as the corresponding field names appear in the first line.



	A	B	C	D	E	F	G	H	I	J	K
1	TN	PHONE	DES	CUSTOMER	USERFIELD1	USERFIELD2	USERFIELD3	USERFIELD4	USERFIELD5	USERFIELD6	USERFIE
2	000 0 05 01	2500	MTHU	0	Hoang	Le	Nhat	Thong	Tri	Hanh	Phuc
3	000 0 05 02	2500	MTHU	0	Mua	Xuan	Thuy	Ha	Dong	Phong	Phuong
4	000 0 05 03	2500	MTHU	0	Khanh	Duyen	Thuy	Thu	Thuy	Thach	Thuy
5	000 0 05 04	2500	MTHU	0	Toan	Thang	Thuy	Thu	Thuy	Thach	Thuy
6	000 0 05 05	2500	MTHU	0	Dung	Thang	Thuy	Thu	Thuy	Thach	Thuy
7	000 0 05 06	2500	MTHU	0	Tam	Thang	Thuy	Thu	Thuy	Thach	Thuy
8	000 0 05 07	2500	MTHU	0	Hung	Hieu	Huong	Hang	Ha	Hoa	Han
9											
10											
11											
12											

Figure 230: Example Contents of CSV file

The valid field names to be used while importing data into the database are in the **Available fields** list in the **Fields selection** section of the Reports UI. Click the **Reports** link in the **Phones** branch of the Element Manager navigator, and then click **Add** to access the Report UI. See Reports on page 334. For more information, see *Avaya Software Input Output Administration, NN43001-611*.

Mandatory Fields

The first column of the import file must be either TN or PRIMEDN. The first column is used as a key to identify the telephones update.

Table 1: Mandatory Fields

Operation	Mandatory Fields
Update an existing telephone record	TN (Terminal Number) or PRIMEDN (Prime Directory Number)
Add a new telephone record	TN (Terminal Number), PHONE (Phone type), CUST (Customer Number), and DES (Designation)
Add an IP Phone record	TN (Terminal Number), PHONE (Phone type), CUST (Customer Number), DES (Designation), and ZONE (Zone)

Add DCS	TN (Terminal Number), PHONE (Phone type), DES (Designation), CUST (Customer Number), PRIMEDN (Prime Directory Number), FTR_CFW (Forward All Calls), DMC (DECT Mobility Controller), and IDNX (Index on DMC)

If PRIMEDN is the first column, you can import only to update telephones.

If TN is the first column, you can import to add or update a telephone.

For a TN, if a matching telephone is found, then the configuration is updated using data from the import file. If no matching telephones are found for a TN, then a new telephone is added to database if all the mandatory parameters for telephone configuration are specified in the import file.

Important:

When you add DCS telephones, you cannot assign a TN to the telephone; the Call Server automatically assigns the TN after the telephone is added. Therefore, for DCS telephones, the telephone is imported if the TN field remains blank. If a TN is assigned to a DCS telephone, the import ignores the user-specified TN.

Data requirements for importing Keys, CPND names and VMB

To import keys, the field name used in CSV file uses the format *Key <number>* where*<number>* is the key number. For example, to import Key 10, the field name is Key10 The value for the key is specified in the following format:

<mnemonic> [<parameters>] [MARP] [ANIE(<value>)] [CPND_FIRST_NAME (<value>) CPND_LAST_NAME(value) CPND_LANG(value) CPND_DISPLAY_FORMAT(value) [VMB_CLASS_OF_SERVICE(value) VMB_SECOND_DN(value) VMB_THIRD_DN(value) VMB_KEEP_MESSAGES(value)]

The entries in square brackets ([ ]) are optional and are based on key mnemonic and import requirements:

- <*mnemonic*>: Represents the key feature mnemonic to be assigned to the key.
- <*parameters*>: Represents the key parameters. The values described in this section depend on the key feature mnemonic.
- *MARP*: Indicates that the DN specified in the <*parameters*> section should use MARP on the key.
- *ANIE(<value>)*: Specifies the value for ANIE entry. The <*value*> represents the ANIE entry value.

You can use the sections with names starting with *CPND_* to import the CPND name for the DN specified in the <*parameters*> section. To import new CPND names, specify a nonblank value for at least one of the two name fields:

- CPND_FIRST_NAME and CPND_LAST_NAME: Use this section to update existing CPND names using import, specify values for only those fields that need to be updated. It is not mandatory to specify a value for all fields.
- CPND_FIRST_NAME: Use this section to specify the CPND first name for the DN specified in <parameters> section.
- CPND_LAST_NAME: Use this section to specify the CPND last name for the DN specified in <parameters> section.
- CPND_LANG: Use this section to specify the CPND language for the CPND name.
- CPND_DISPLAY_FORMAT: Use this section to specify the CPND display format for the CPND name.

You can use the sections with names starting with *VMB__* to import VMB configuration data for the DN specified in the <*parameters*> section. It is not mandatory to specify values for all fields; specify a value only for those fields that must be updated:

- VMB_CLASS_OF_SERVICE: Use this section to specify the class of service value for the VMB.
- VMB_SECOND_DN: Use this section to specify a second DN for the VMB.
- VMB_THIRD_DN: Use this section to specify the third DN for the VMB.
- VMB_KEEP_MESSAGES: Use this section to specify the preference for keep messages field of the VMB.

The valid values are the same as those accepted by PBX overlays.

Figure 231: Example of a CSV file to import on page 328 is an example of a CSV file to import.

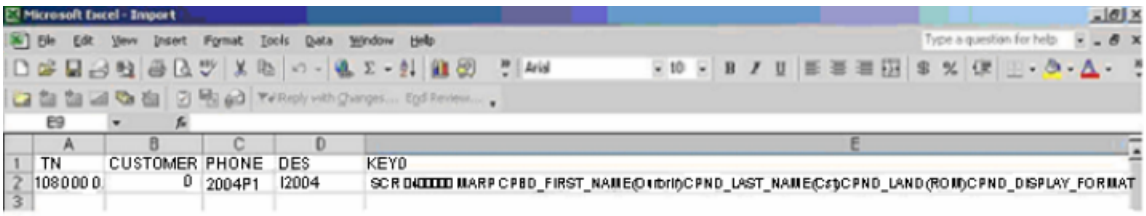


Figure 231: Example of a CSV file to import

Data requirements for importing Single Line Features

You can import Single line features (FTR) by specifying the field name in the format *FTR_<mnemonic>*, where *<mnemonic>* is the mnemonic for a single line feature, and by specifying the value in the format *<mnemonic> <parameters>*.

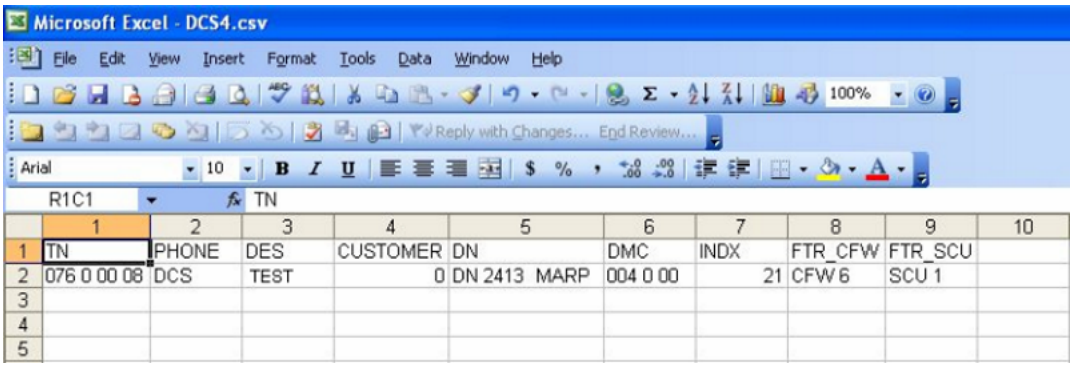


Figure 232: Example of a CSV file of FTR data to import for a DCS phone

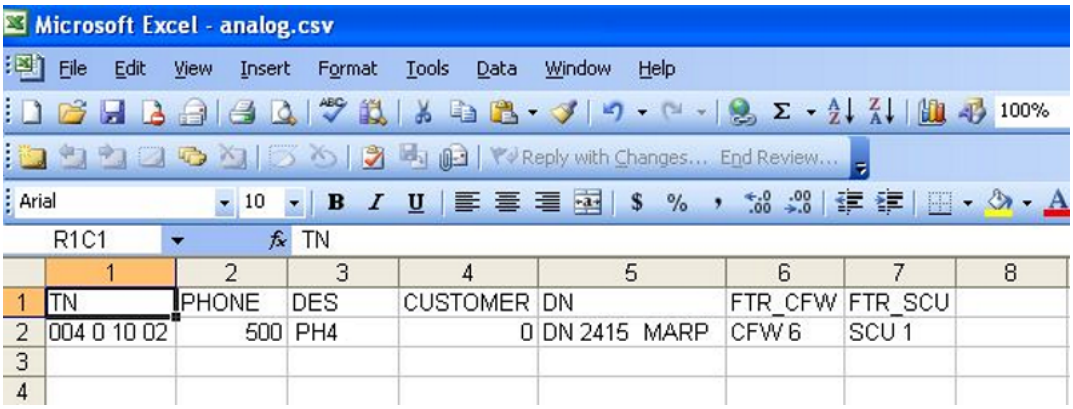


Figure 233: Example of a CSV file of FTR data to import for an analog telephone

Data requirements for importing DN for analog telephones

The DN field for analog telephones can have MARP and ANIE settings and, CPND and VMB configuration. You can import the DN field for analog telephones by specifying the field name as DN and by specifying the value in the following format:

DN<DNvalue> [MARP] [ANIE(<value>)] [CPND_FIRST_NAME (<value>) CPND_LAST_NAME(value) CPND_LANG(value) CPND_DISPLAY_FORMAT(value)] [VMB_CLASS_OF_SERVICE(value) VMB_SECOND_DN(value) VMB_THIRD_DN(value) VMB_KEEP_MESSAGES(value)]

To Import telephones, perform the steps in Import Telephones on page 330.

Import Telephones

1. Click the **Phones** link in EM navigator.

   The Search for Phones Web page appears.

2. Click **Import** to open the Import Telephones Web page.
3. Specify the name of the file from which the telephone details are to be imported by using the browse button or by entering the file name.

   The file must be a CSV file.

4. Click **Save**.

The status of the import is displayed. Obtain an initial format of the CSV file by generating a Report in CSV format using the **Reports** link of the **Phones** branch of the Element Manager navigation page.

Important:

The maximum session time in UCM is 2 hours by default. You must change the maximum session time for the import operation that exceeds 2 hours in the **UCM Session Properties** section. To change the maximum session time, refer to *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116*.

Move Phones

You can move a telephone to another TN with the same property values. To do this, perform the steps in Move Phones on page 330.

Move Phones

1. From the **Search Results** section of the Search for Phones Web page, select **Move** from the **More Actions** list.

   The Move TN Web page appears, as shown in Figure 234: Move TN Web page on page 331.

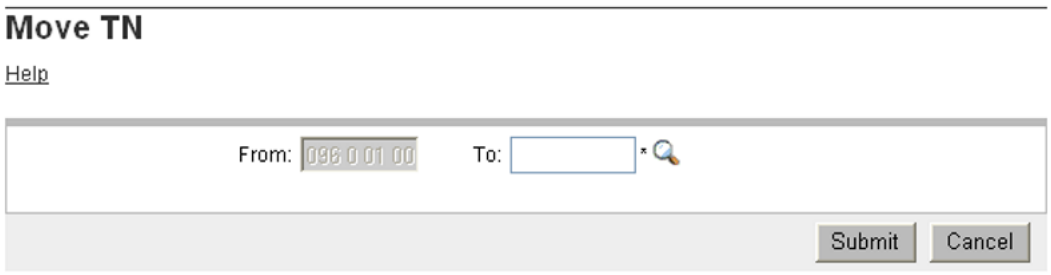


Figure 234: Move TN Web page

For Attendant consoles/phones, the Move TN Web page displays two prompts for **Terminal Number** and **Secondary Terminal Number** .

2. Enter the TN to move the telephone, and click **Submit**.

Moving an IP Attendant 3260 Phone

1. In the Search For Phones Web page, select the check box corresponding to the 3260 phone to be moved.
2. Select the value **Move** from the **More Actions** drop-down list.

   The Move TN Web page appears as shown in the following figure.

   The current Primary and Secondary TNs appear in the **From** fields.

3. Fill in the required values in the **To** fields corresponding to the **Terminal Number** and **Second Terminal Number** fields.
4. Click **Submit** to move the phone to the specified TNs.

   The page refreshes to display the Search For Phones Web page.

Retrieve Phones

The Retrieve Phones function synchronizes data from the Call Server to the Phones database. Perform the steps in Retrieve Phones on page 332.

Retrieve Phones

1. From the Search for Phones Web page, click **Retrieve**.
2. The Retrieve Options Web page appears, as shown in Figure 235: Retrieve Options Web page on page 332.

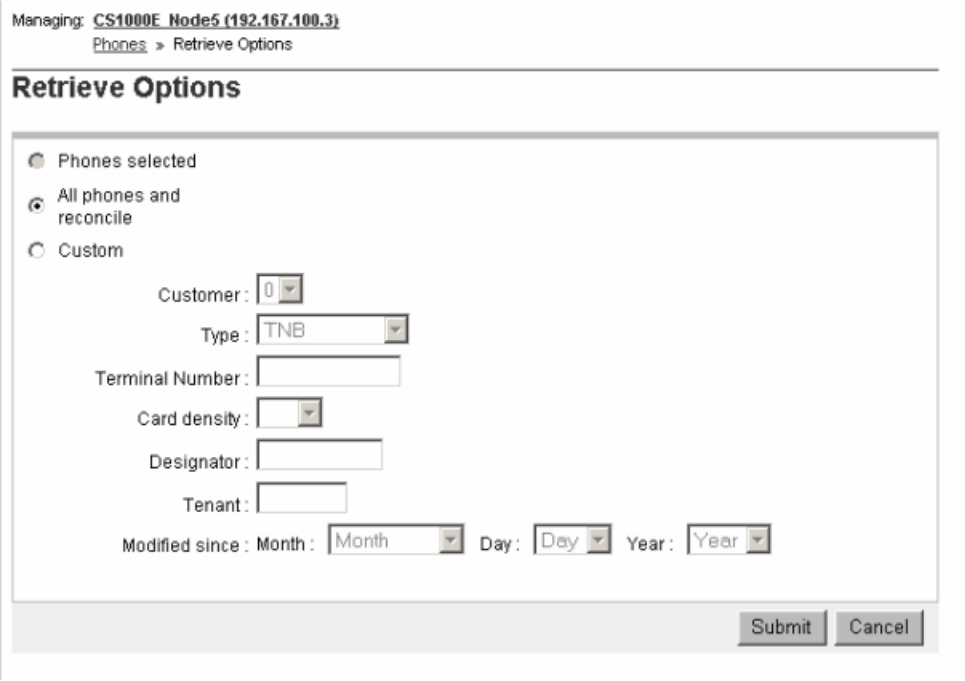


Figure 235: Retrieve Options Web page

3. Select one of the Retrieve Options, as follows:

   Select **Phones selected** to retrieve the telephones in the phone Search Results section.

   Select **All phones and reconcile** to retrieve the telephones.

   Select **Custom** and enter any combination of search criteria to retrieve telephones that meet those criteria.

4. Click **Submit**.

Important:

The maximum session time in UCM is 2 hours by default. You need to change the maximum session time for import operation that exceeds 2 hours in the UCM Session Properties section. To change the maximum session time refer to *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116* .

Important:

It is recommended that only one user at a time perform a retrieve and reconcile operation. EM Phone Provisioning does not support concurrent users for a retrieve and reconcile operation.

Delete Phones

To delete telephones, perform the steps in Delete Phones on page 333.

Delete Phones

1. From the Search for Phones Web page, search for telephones based on a search criteria.
2. Click the boxes beside all the telephones to delete.
3. Click **Delete** .
4. Click **OK** to confirm the deletion of the telephones selected, or click **Cancel** to stop the operation.

Swap Phones

When you swap telephones, two telephones exchange TNs. The following limitations apply to a swap:

- You can swap only two telephones at a time.
- The telephones to be swapped must belong to the same customer.
- The telephones to be swapped must have compatible TN types. For example, you cannot swap an analog (500/2500-type) telephone with a digital telephone.
- Swapping is not supported for DCS telephones. Element Manager does not control the allocation of virtual TNs for DCS telephones.
- If the synchronization status of one of the telephones to be swapped is New, it must be swapped with another telephone with a synchronization status of New.
- The telephones to be swapped must have the same VCE or DTA Class of Service.
- Swapping is not supported for IP Phones.
- Swapping is not supported with the BFS feature.
- Swapping is not supported if one of the telephones is an ACD telephone in the acquired state.
- Swapping is not supported for telephones with a branch office link.

Swap Phones

1. From the Search for Phones Web page, search for telephones based on a search criteria.
2. From the list of telephones, select the two telephones to swap.
3. Select **Swap** from the **More Actions** list.

   The changes are submitted to the database.

Reports

Element Manager provides the ability to construct complex queries against the Phones database in the form of reports. The results can be in either HTML or CSV format. If you choose HTML format, only a maximum of 1000 records appear.

Click the **Reports** link of the **Phones** branch of the Element Manager navigator. The Edit a Report Web page appears, as shown in Figure 236: Edit a Report Web page on page 334.

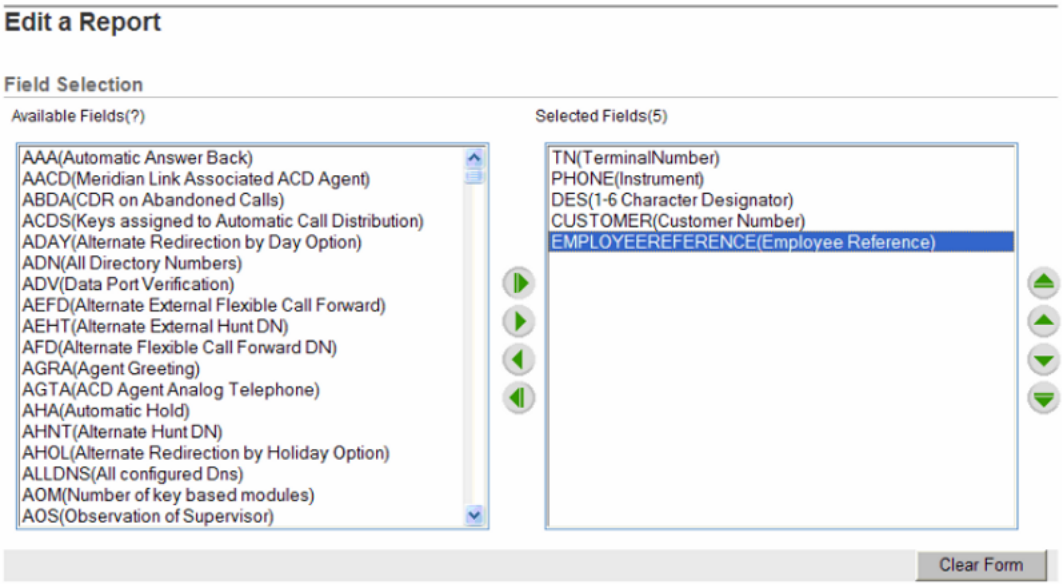


Figure 236: Edit a Report Web page

Configure the desired criteria and report format, and then click **Generate Report** to generate the report.

Note:

Due to performance issues, Avaya does not recommend concurrent execution of reports with large databases.

Canned Reports

The Element Manager provides the ability to create, copy, edit, import, export, and delete report definitions. You can generate a telephones report, which can be saved in HTML or CSV format. The CSV file can be used to import phones.

Important:

The maximum number of report definitions supported by the system is 100.

Report definition

A report definition consists of the following:

1. Report name and description — These are required only if the definition is going to be saved; otherwise, they are optional.
2. Report schema — This is the set of parameters defining the report format and its contents. The following parameters are defined in the schema:
   - **Report fields** : telephone properties required in the report.
   - **Set of report criteria** : conditions based on which telephone records are filtered.
   - **Sort fields** : telephone properties based on which the report is sorted.
   - **Report format** : the format of the report and options for displaying the report.

Default Reports

Pre-defined reports are part of the Report List Web page and they appear in the Report profile Name list. See Figure 237: Report List on page 338.

The predefined report is generated by clicking **Generate Report** on the Report List Web page. You cannot delete or rename default reports. All default reports are identified by the prefix: Default_, followed by the report name. The Reports and descriptions table lists the reports that appear in EMPP, along with a brief description.

Table 2: Reports and descriptions

Report Name	Description
Default_HuntPatterns Report	Displays all telephones that have HUNT configured. The following fields are displayed:

Report Name	Description
	• HUNT • EmployeeReference* • PrimeDN
Default_KeyAssignments Report	Displays all telephones. The following fields are displayed: • TN • PrimeDN • Location • Keys Assigned (Key Number, Key Mnemonic and Key Value) • EmployeeReference* • Instrument (Phone Type) - CLS (Trunk/Call Access Restriction)
Default_MessageCenters Report	Displays all telephones that have keys assigned to Message Waiting. The following fields are displayed: • Message Center DN (Keys Assigned to message waiting - PHONE(phone) • Instrument (Phone Type) • TN
Default_Phones Report	Displays all telephones that have an EmployeeReference. The following fields are displayed: • EmployeeReference • PrimeDN • TN
Default_PrivateLine Report	Displays all telephones that have Ringing Number Pick-up Group configured. The following fields are displayed: • RNPG (Ringing Number Pick-up Group) • PrimeDN • Instrument (Phone Type) • EmployeeReference** • PHONE(phone)
Default_AccessRestriction Report	Displays all telephones. The following fields are displayed:

Report Name	Description
	• PrimeDN • CLS (Trunk/Call Access Restriction) • NCOS (Network Class of Service) • Location • TN • EmployeeReference*
Default_AutomaticCallDistributionPhones Report	Displays all telephones that have Automatic Call Distribution Phones configured. The following fields are displayed: • ACDS (Automatic Call Distribution Stations) • CLS (Trunk/Call Access Restriction) • SPID (Supervisor Position ID) • Location • TN • EmployeeLastName
Default_DialIntercomGroups Report	Displays all telephones that have a Dial Intercom Group configured. The following fields are displayed: • DIG (Dial Intercom Group) • PrimeDN • Instrument (Phone Type) • Location • Department • EmployeeLastName

Generating a report

Reports are generated based on report definitions. If an existing report definition is not suitable, you must create a new definition.

Generate a report

1. From the navigation tree, click **Phones** and then **Report** .

   The Report List Web page appears as shown in the figure Figure 237: Report List on page 338.

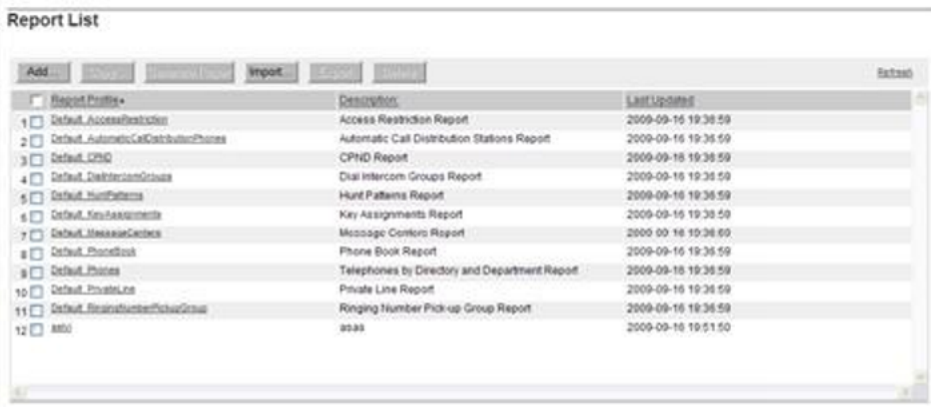


Figure 237: Report List

2. From the **Report List** , select a report by clicking the check box.
3. Click **Generate report** .

   The report appears in HTML table format as shown in the figure Figure 238: Phone Report on page 339.

Phone Report

Report Details | View As CSV | 2051 Rows Fetched

Title: test2

Criteria: SYNCSTATUS = Transmitted

Report Date: Tue Oct 13 11:57:46 IST 2009

TN	PHONE	DES	CUSTOMER	KEY0
)96 0 00 01	1110	TEST	0	
)96 0 00 05	1110	SOM	0	
)96 0 00 12	1110	PRANIT	0	
				SCR 76144 0 MARP CPND
176 0 00 00	2004P2	HURJAB	0	First Name: Last Name: SB_05_16144 Language: ROM Display format: FIRST,LAST
				SCR 76145 0 MARP CPND
176 0 00 01	2004P2	HURJAB	0	First Name: Last Name: SB_05_16145 Language: ROM Display format: FIRST,LAST
				SCR 76146 0 MARP CPND
176 0 00 02	2004P2	HURJAB	0	First Name: Last Name: SB_05_16146 Language: ROM Display format: FIRST,LAST
				SCR 76147 0 MARP CPND
176 0 00 03	2004P2	HURJAB	0	First Name: Last Name: SB_05_16147 Language: ROM Display format: FIRST,LAST
				SCR 76148 0 MARP CPND
176 0 00 04	2004P2	HURJAB	0	First Name: Last Name: Language: Display format:

Figure 238: Phone Report

4. To view the report in CSV format, click **View as CSV** .

   The report opens in Microsoft Excel. If you save the report in CSV format, the report must be downloaded to your PC.

Creating a new report definition

You can create a new report profile definition in one of the following ways:

- Create a new report definition
- Modify or customize an existing definition

When you create a new report definition, you can generate the report immediately, or save the report definition and use it later to generate a report.

Adding a new report profile

You can define each component of the new report definition using the report definition option.

Add a new report profile

1. From the navigation tree, click **Phones** and then **Report** .

   The Report List Web page appears, as shown in the figure Figure 237: Report List on page 338.

2. Click **Add** .

   The Report Details Web page appears, as shown in the figure Figure 239: Report Details on page 340.

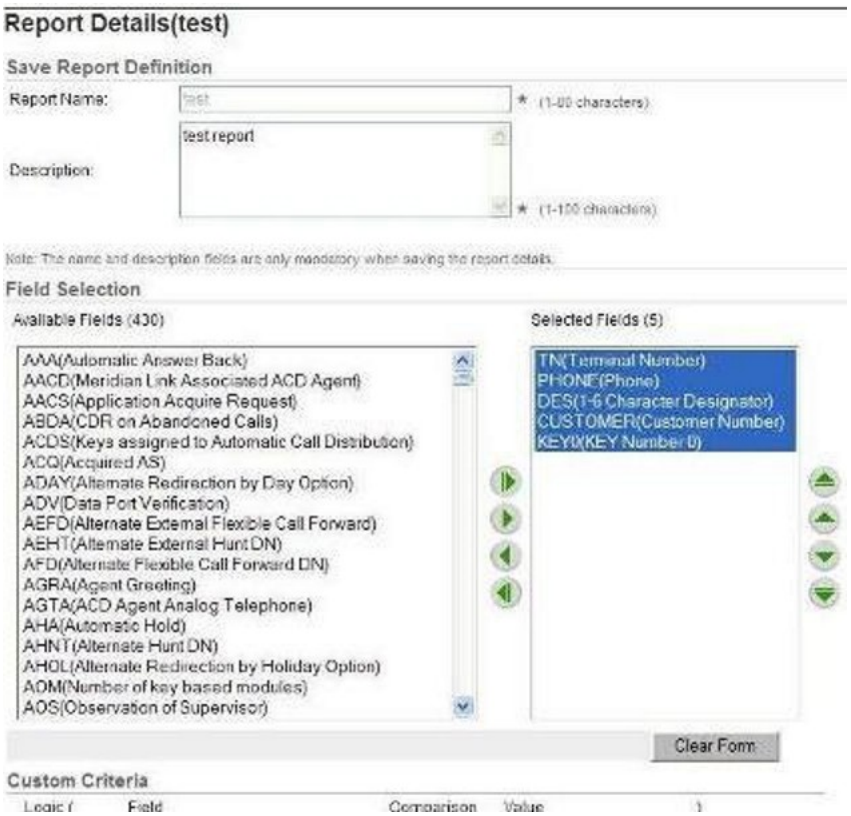


Figure 239: Report Details

3. In the **Field Selection** section, select the fields to include in the report:

   - Hold down the CTRL key, and click on each required field in the **Available Fields** list.
   - Click the **Add** arrow. The selected fields appear in the **Selected Fields** list.

To remove a field from the **Selected Fields** list, click on the field and click the **Remove** arrow.

- Click the **Top**, **Up one**, **Down one**, or **Bottom** arrows as required to move the fields into the order in which you want them to appear in the report.

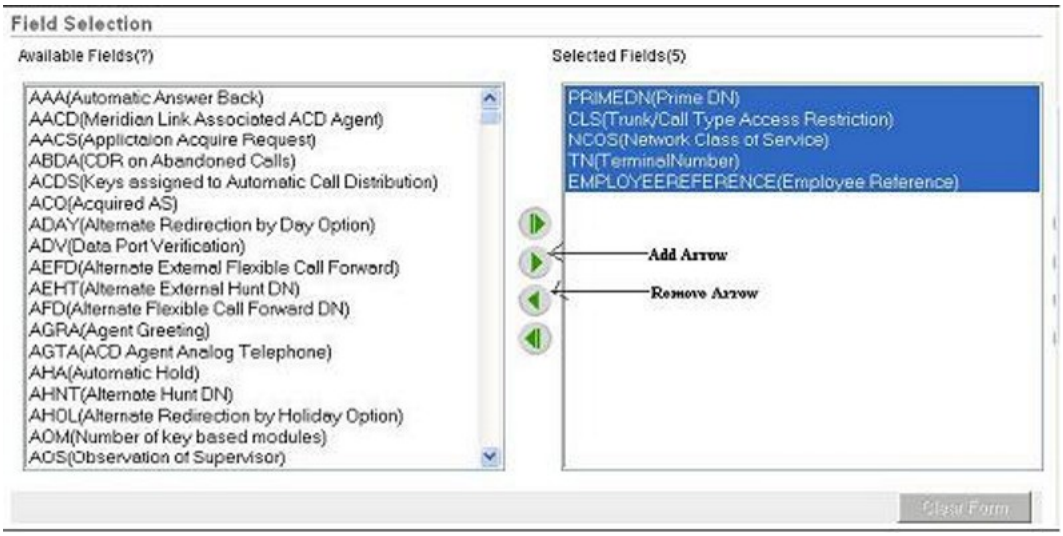


Figure 240: Define a New Report: Field Selection

4. In the **Custom Criteria** section, as shown in the figure Figure 241: Define a New Report: Custom Criteria, Sorting, Report Format, and Format Options on page 342, select the criteria for the records to report:

    a. From the **Field** list, select a field.

    The corresponding **Value** field changes to a text box or a list, depending on the field selected.

    b. From the **Comparison** list, select the appropriate comparison operator.

    c. Enter a value in the **Value** field by selecting from the **Value** list, or typing values in the **Value** box.

    d. (Optional) To extend the expression to another row, click **Add Criteria** . Select **AND** or **OR** from the **Logic** list and enter the next expression.

    e. (Optional) Click **Delete Criteria** to remove the corresponding row.

    f. (Optional) Click **Clear Criteria** to clear the row and reenter the expression.

    g. Select the appropriate number of parentheses from the opening, (, and closing,), parentheses.

    Parentheses set the precedence of evaluation of each expression in the search criteria.

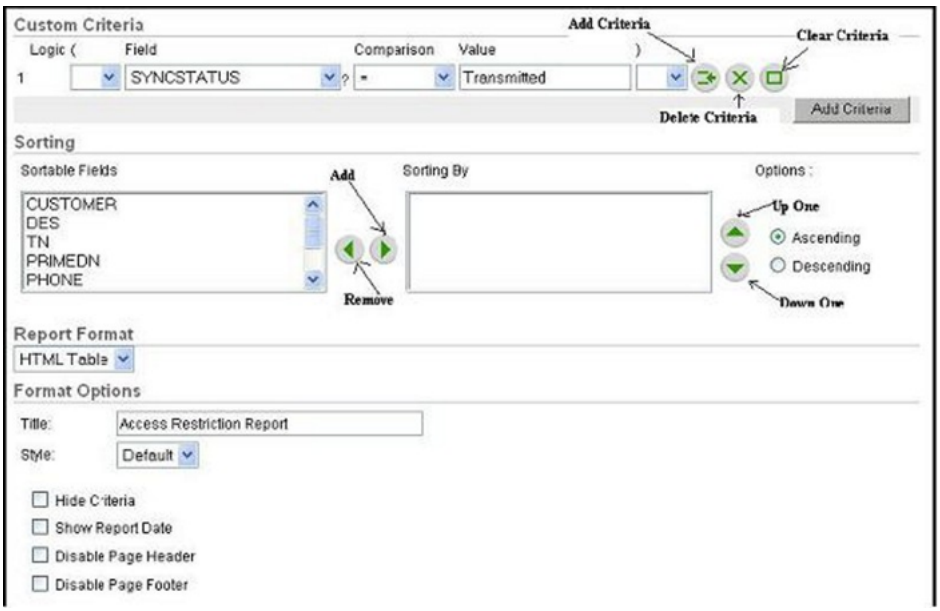


Figure 241: Define a New Report: Custom Criteria, Sorting, Report Format, and Format Options

5. If there are fields listed in the **Sortable Fields** list box in the **Sorting** section shown in the figure Figure 241: Define a New Report: Custom Criteria, Sorting, Report Format, and Format Options on page 342, select the sorting order of the records, if required:

    a. From the **Sortable Fields** list, select a field by which the data is to be sorted.

    Select the field to be the primary sort key; that is, the first field selected always determines the order of the records. The next field selected determines the order of those records where the values in the first field are identical and cannot be sorted. This sort precedence continues through all selected fields.

    b. Click **Add** to move the field to the **Sorting By** list box.

    c. If required, click **Up One** and **Down One** to reorder the sort fields.

    d. Click **Ascending** or **Descending** to sort the records in ascending or descending order.

    e. Repeat steps 1 through step 4 for each field to be selected as a sort key.

    Note that the sortable fields have only predefined values:

        i. CUSTOMER
        ii. DES
        iii. TN
        iv. PRIMEDN
        v. PHONE

vi. LASTUPDATEDBY

vii. LASTUPDATEDON

6. From the **Report Format** list, select **HTML Table** or **CSV** as the report format.

   If the report is in HTML Table format, the report is displayed in a Web page. If the report is in CSV format, the report is generated as a CSV file and you are prompted to download the file.

7. In the **Format Options** section, define additional format options as required:

   - Enter a title for the report in the **Title** box.
   - Select the report style from the **Style** list.

     The two options are **Default** and **Print**. The **Default** style formats the report for viewing in a Web page. The **Print** style formats the report for printing.
   - Select **Hide Criteria** to hide the criteria in the report.
   - Select **Show Report Date** to include the generation date in the generated report.
   - Select **Disable Page Header** to hide the report header.
   - Select **Disable Page Footer** to hide the report footer.

8. Enter a name for the report definition in the **Report Name** box.
9. Enter a description for the report definition in the **Description** box.
10. Click **Save** .

Creating a new report definition from an existing definition

This method consists of modifying an existing report definition and saving it as a new definition.

Create a new report definition from an existing definition

1. From the navigation tree, click **Phones** , and then **Report** .

   The Report List Web page appears, as shown in the figure Figure 237: Report List on page 338.
2. Select the check box corresponding to the report to copy.
3. Click **Copy** .

   The Report Details Web page appears as shown in the figure Figure 239: Report Details on page 340.
4. Make the necessary modifications to the report, following step 3 to step 7 of Adding a new report profile on page 340.
5. Enter a name for the definition in the **Report Name** box.

6. Enter a description for the definition in the **Description** box.
7. Click **Save** .

Deleting a report definition

1. From the navigation tree, click **Phones** , and then **Report** .

   The Report List Web page appears, as shown in the figure Figure 237: Report List on page 338.
2. Select a report profile from the list.
3. Click **Delete** .

Exporting a report definition

1. From the navigation tree, click **Phones** , and then **Report** .

   The Report List Web page appears, as shown in the figure Figure 237: Report List on page 338.
2. Select a report profile from the list.
3. Click **Export** .

   The Bulk Export for Report Profiles Web page appears.
4. Click **Download Exported Report Profiles** to save it in CSV format.

Importing a report definition

Import a report definition

1. From the navigation tree, click **Phones** , and then **Report** .

   The Report List Web page appears, as shown in the figure Figure 237: Report List on page 338.
2. Click **Import**.

   The Import Report Profiles Web page appears, as shown in the figure Figure 242: Import Report Profiles on page 345.

Figure 242: Import Report Profiles

The file to be imported should be in csv format as shown in the figure Figure 243: ImportReportProfile.csv on page 345.

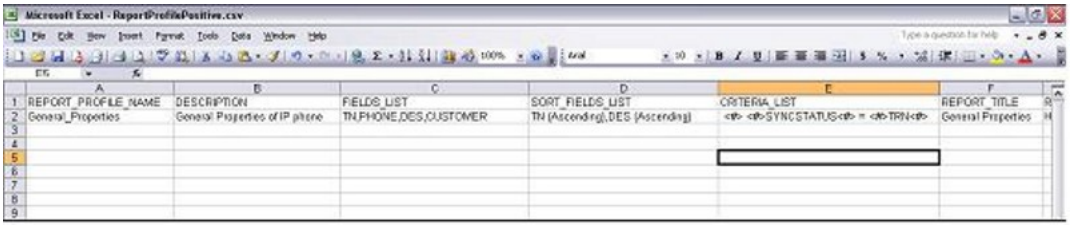


Figure 243: ImportReportProfile.csv

3. Browse for the file to be imported and click **Save** to save it in CSV format.

   Import progress page appears, including information about the number of report profiles imported successfully. For more information, see Figure 244: Report Profile Import Progress on page 345.

Figure 244: Report Profile Import Progress

When the import is complete, the Profile Import Summary Report Web page appears, as shown in the figure Figure 245: Report Profile Import Summary on page 345.

Figure 245: Report Profile Import Summary

4. Click the **log file** link as shown in the figure Figure 245: Report Profile Import Summary on page 345.

The File Download dialog box appears with **Open** and **Save** options.

5. Click **Open** .

   The log file appears with the details of the errors for the failed report profiles.

Custom Views

The Custom Views feature allows the user to specify the telephone fields to be displayed on the Telephone Details Web page. Each field is validated based on the telephone type and system configuration, before displaying it on the Web page. This applicability checking allows the view to be independent of telephone type at the time of view configuration.

The Views Web page displays a list of configured views, the name, description, and last updated date and time. The maximum number of custom views supported by the system is 100. You can perform the following actions on the views.

- Add a view.
- Edit an existing view.
- Copy an existing view.
- Delete a view.
- Apply view to the Telephone Details Web page.

To open the Views Web page on the Element Manager navigator, expand the **Phones** branch and then click **Views** .

The following figure shows the Views Web page.

Figure 246: Views Web page

Adding a custom view

To add a custom view, use the following procedure.

1. Select **Phones > Views** .
2. On the Views Web page click **Add**.

Important:

The **Add** button is disabled when the maximum custom views limit is reached.

The View Details Web page appears.

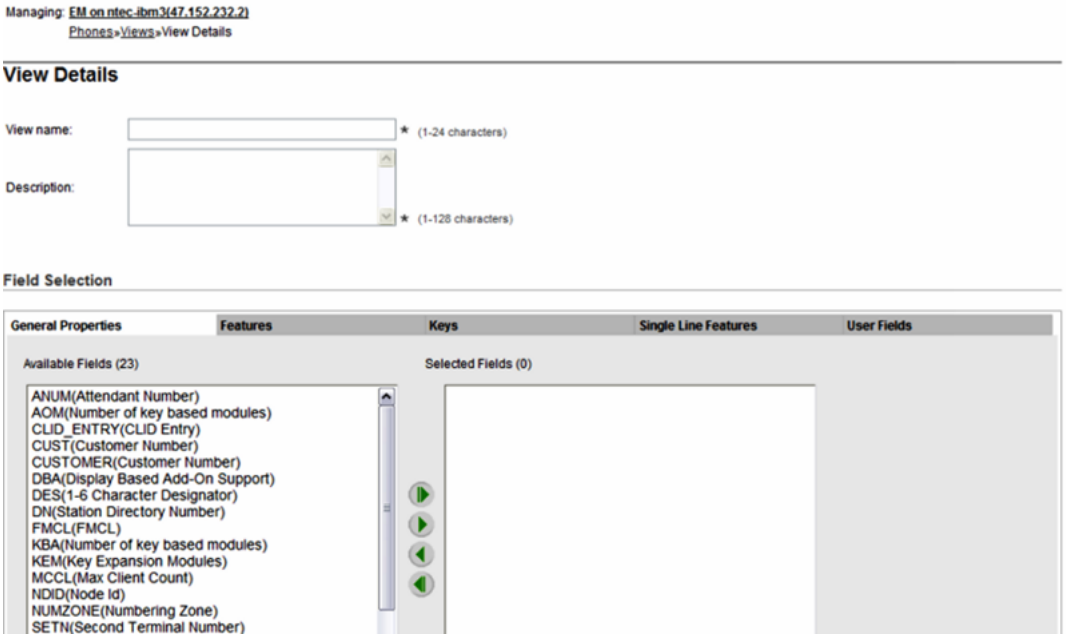


Figure 247: View Details Web page

3. Enter the name of the view in the **View name** field.

   The name can have a maximum of 24 characters.

4. Enter a description of the view in the **Description** field.

   The description can be a maximum of 128 characters.

   In the **Field Selection** section of the Web page, the following five tabs are available:

   - **General Properties**
   - **Features**
   - **Keys**
   - **Single Line Features**
   - **User Fields**

   The **Available Fields** list under each tab contains all fields applicable to the particular tab.

5. Move the required fields from the **Available Fields** list on the left side to the **Selected Fields** list on the right side.

   You can move selected fields, or all fields together, to and from the lists.

Important:

You must select at least one field under any of the five tabs.

6. Click **Save** to save the configuration.

   The Views Web page appears with the newly added view.

Editing a custom view

To edit a custom view, use the following procedure.

1. Select **Phones > Views** .
2. In the Views Web page, click the link of the custom view to be edited.

   The View Details Web page appears with the details of the selected custom view.
3. Edit the description in the **Description** field.

   Important:

   You cannot edit the name of the custom view.
4. Add or remove the fields under the tabs as required.
5. Click **Save**.

   The page refreshes to display the Views Web page.

Copying from an existing custom view

To create a copy of an existing custom view, use the following procedure.

1. Select **Phones > Views** .
2. Select the check box corresponding to the custom view to be copied from the Views Web page.
3. Click **Copy**.

   Important:

   Select at least one custom view, to enable the **Copy** button.

   The page refreshes to display the View Details Web page with the details of the selected custom view except the name and description.
4. Type the name for the new custom view in the **View name** field.
5. Type the description for the new custom view in the **Description** field.
6. Click **Save**.

Deleting a custom view

To delete a custom view, use the following procedure.

1. Select **Phones > Views** .
2. Select the check box corresponding to the custom view to be deleted.

   To delete multiple custom views, select the check boxes corresponding to the custom views to be deleted.
3. Click **Delete**.

   Important:

   The **Delete** button is enabled only when at least one custom view is selected.

   The system displays a dialog box asking for confirmation to delete the custom view.
4. Click **OK** to delete the selected custom view.

Applying custom view to Telephone Details

To apply custom view to Telephone Details, use the following procedure.

1. Select **Phones > Search For Phones > Add** .

   The New Phones Web page appears.
2. Configure the following fields as required.

   - **Number of phones**
   - **Customer**
   - **Type**
   - **Default value for DES**
   - **Default value for Zone**
   - **Automatically assign TN starting TN**
   - **Automatically assign DN starting DN**
3. Click **Preview**.

   The Phone Details Web page appears. The Custom View box is listed with the available views.
4. Select the required view from the values available in the **Custom View** drop-down box.

   All views applicable to the selected telephone type is displayed in the list.

If you select the value **All** in the **Custom View** list, all fields applicable to the selected telephone type gets listed.

Virtual Office Search and Logout

The user can search for virtually logged in sets, based on idle time criteria and then logout, based on the duration for which the set is idle. Only those users with LD 117 permission can perform these operations.

To access the Search For Phones Web page, click **Phones** in the navigation tree. The user can search for those virtually logged in sets which are idle for greater than or equal to a specified time, based on the Idle Time criteria.

For more information on searching for phones, see Search for phones on page 308.

The Logout option enables the user to select phones from the searched phones list, based on idle time criteria, and log out. This option also is available in the Search For Phones Web page. The default time out for an idle set is 30 minutes.

For more information on the Virtual Office logged in sets, see *Avaya Features and Services Fundamentals - Book 6 of 6, NN43001-106-B6*.

Logout a phone

To logout a phone, use the following procedure.

1. On Search For Phones Web page, search for a phone.
2. Select the check box corresponding to the phone to logout.

   You can logout from multiple phones by selecting the corresponding check boxes.
3. Select **Logout** from the **More actions** drop down.

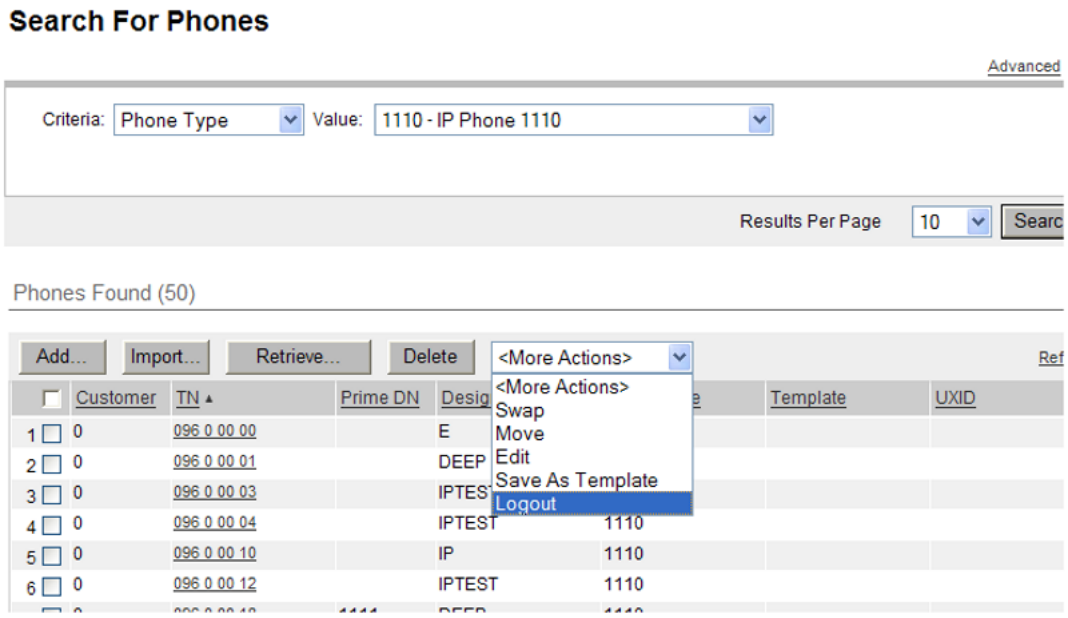


Figure 248: Search For Phones Web page

The system asks for a confirmation to logout from the selected phone.

4. Click **OK**.

   The page refreshes to display the Search for Phones Web page with the selected phones removed from the search result list.

Lists

The Lists feature enables you create, view, edit, and delete lists in the Element Manager. You can also add and modify lists through a CSV or a web detailed interface. You can import new lists into the system in the CSV format. To access the list feature you can click the **Lists** link of the **Phones** branch of the Element Manager navigator. The Lists Web page appears, as shown in the following figure.

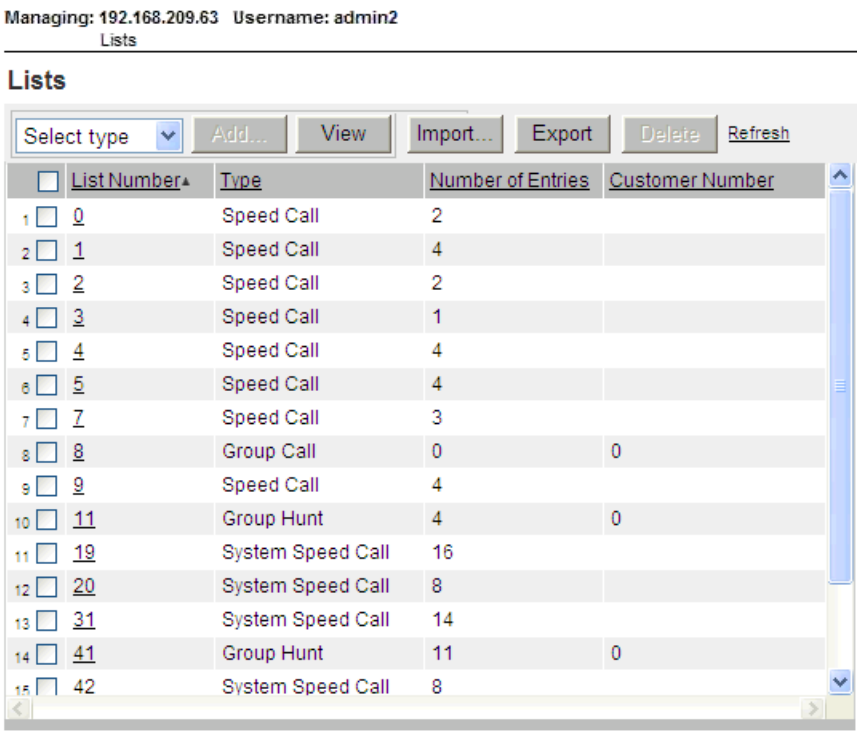


Figure 249: Lists Web page

Using the Lists web page, you can perform the following actions:

- view the lists
- import new lists in CSV format
- export the lists
- add lists
- delete lists
- edit lists

The different types of Lists supported in Element Manager are as follows:

- Speed Call
- System Speed Call
- Group Call
- Group Hunt

In the Lists web page, you get a view of the lists available. To see the details of a particular list, you can click on the required list number. The corresponding details Web page appears.

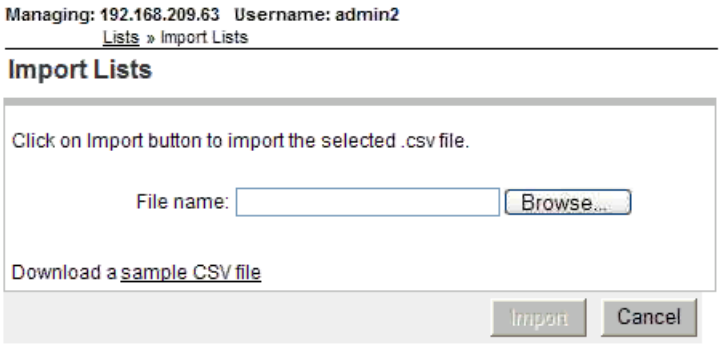
If you add, modify, or delete lists information directly from the CLI of the Call Server or from another Element Manager web page, click the **Refresh** link on the Lists Web page to see the updated information about lists.

Use the following procedure to import a list into the Element Manager:

Importing a List

1. Click **Import** on the Lists Web page.

   The Import Lists Web page appears.



2. Click **Browse** .

   The Choose File dialog box appears.
3. Select the file to be imported.
4. Click **Open** .

   The dialog box closes and the path of the selected file appears in the **File name** field.
5. Click **Download a sample CSV file** if you want to view a valid format of a CSV file.
6. Click **Import** .

   The processing status of the import appears. When the file is imported, the Lists web page appears and the details of the new list are displayed with the pre existing lists.

Important:

If you try to import a list with an existing number in the Call Server and if the list type in the csv file is the same as the one configured in the Call Server, the list is updated with the new values from the csv file.

If you try to import a list with the same list number as that of an existing list but the list type in the csv file is not the same as on the one configured in the Call Server, the import fails and Element Manager displays a message that the List number already exists.

The following table is a sample of a CSV file format:

Table 3: Sample CSV file format

List Type	Cols	Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
Group call	5	List Number	GroupCtrl	CustomerNo	EntryNo	DN	
Group hunt	6	List Number	MaxDnSize	CustomerNo	ListSize	EntryNo	DN
Speed call	5	List Number	MaxDnSize	ListSize	EntryNo	DN	
System speed call	6	List Number	NetworkCOS	MaxDnSize	ListSize	EntryNo	DN

To export a list from the Element Manager, you can click on the **Export** button. The files are exported in the CSV format.

Use the following procedure to add a Speed Call list.

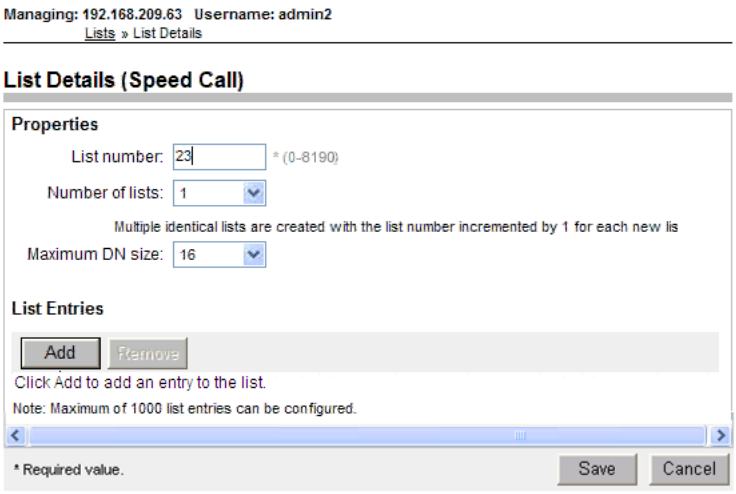
Adding a Speed Call List

1. Select **Speed Call** from the drop-down list on the Lists Web page.

   The **Add** button is enabled.

2. Click **Add** .

   The List Details (Speed Call) Web page appears.



3. Type the number of the list in the **List number** field.

   You can give a value between 0 and 8190.

4. Select the number of Speed Calls lists to be created from the drop-down list in the **Number of lists** field.

Default value of the field is **1** .

If you select a value more than one, the system creates the specified number of identical lists. The list number of each list gets incremented by one from the previous list number.

5. Select the maximum DN size of the Speed Calls lists to be created from the drop-down list in the **Maximum DN size** field.

   Default value of the field is **16** .

6. Click **Add** .

   A row for the **Entry Number** and **DN** fields appear in the **List Entries** block.

7. Type the first number for the list entry in the **Entry Number** field.
8. Type the first DN number for the list entry in the **DN** field.

   To add more rows, you can use the **Add** button.

   You can add up to 1000 list entries for a Speed Call.

9. To remove a list entry perform the following steps:

   - Select the check box corresponding the entry to be removed.

     The **Remove** button gets enabled.

   - Click **Remove** .

     The selected list entry is removed from the block.

10. Click **Save** .

    The processing status appears. When the list is added successfully , the Lists web page appears and the details of the new list are displayed with the existing lists.

    When the list is added to the Element Manager, the Lists Web page appears and the new list appears with the existing lists.

Use the following procedure to add a System Speed Call list.

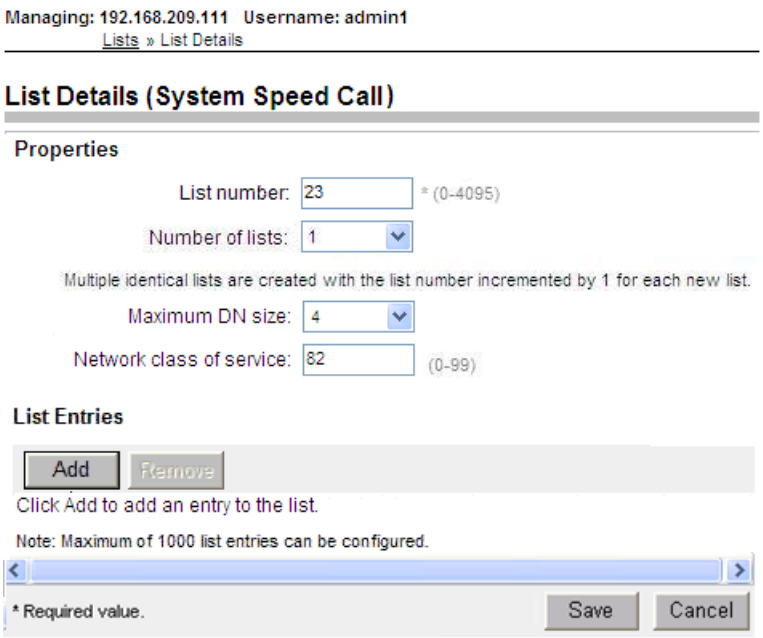
Adding a System Speed Call List

1. Select **System Speed Call** from the list on the Lists Web page.

   The **Add** button is enabled.

2. Click **Add** .

   The List Details (System Speed Call) web page appears.



3. Type the number of the list in the **List number** field.

   You can give a value between 0 and 4095.

4. Select the number of Speed Calls lists to be created from the drop-down list in the **Number of lists** field.

   Default value of the field is **1** .

   If you select a value more than one, the system creates the specified number of identical lists. The list number of each list gets incremented by one from the previous list number.

5. Select the maximum DN size of the Speed Calls lists to be created from the drop-down list in the **Maximum DN size** field.

   Default value of the field is **16** .

6. Type the required value in the **Network class of service** field.

   You can give a value between 0 and 99.

7. Click **Add** .

   A row for the **Entry Number** and **DN** fields appear in the **List Entries** block.

8. Type the first number for the list entry in the **Entry Number** field.

9. Type the first DN number for the list entry in the **DN** field.

   To add more rows, you can use the **Add** button.

   You can add up to 1000 list entries for a System Speed Call.

10. To remove a list entry perform the following steps:

    • Select the check box corresponding the entry to be removed.

The **Remove** button gets enabled.

- Click **Remove** .

  The selected list entry is removed from the block.

11. Click **Save** .

    The page refreshes to show the status of the process. The page displays the following information:

    - **Status**
    - **Total call list(s)**
    - **List(s) processed**
    - **Successfully configured**
    - **Failed to configure**
    - **List(s) pending to be processed**

    When the list is added to the Element Manager, the Lists Web page appears and the new list appears with the existing lists.

Use the following procedure to add a Group Call list.

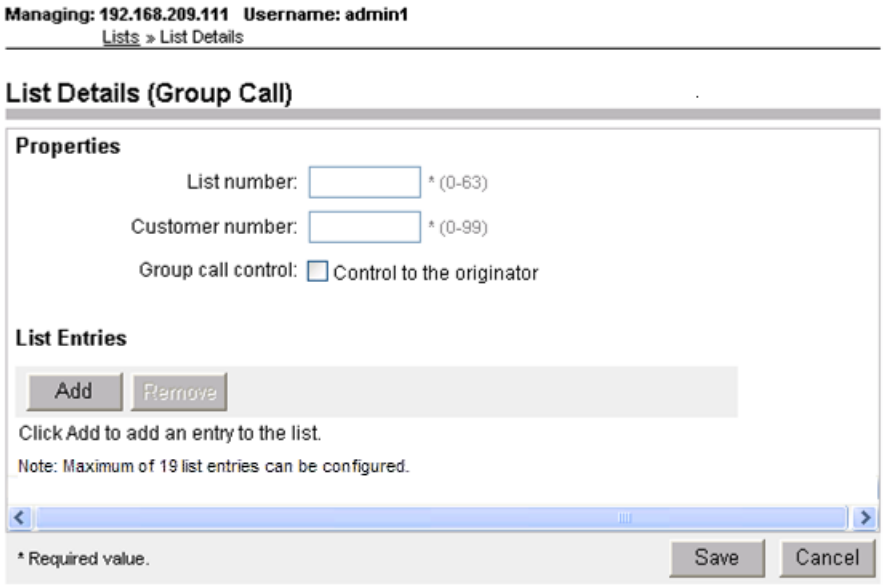
Adding a Group Call List

1. Select **Group Call** from the drop-down list on the Lists Web page.

   The **Add** button is enabled.

2. Click **Add** .

   The List Details (Group Call) web page appears.



3. Type the number of the list in the **List number** field.

You can give a value between 0 and 63.

4. Type the customer number for the list in the **Customer number** field.

   You can give a value between 0 and 99.

5. Select the check box corresponding to the field **Group Call control** if you want to give control of the list to the originator.
6. Click **Add** .

   A row for the **Entry Number** and **DN** fields appear in the **List Entries** block.

   You can add a maximum of 19 list entries.

7. Type the first number for the list entry in the **Entry Number** field.
8. Type the first DN number for the list entry in the **DN** field.

   To add more rows, you can use the **Add** button.

9. To remove a list entry perform the following steps:

   - Select the check box corresponding the entry to be removed.

     The **Remove** button gets enabled.

   - Click **Remove** .

     The selected list entry is removed from the block.

10. Click **Save** .

    The page refreshes to show the status of the process. The page displays the following information:

    - **Status**
    - **Total call list(s)**
    - **List(s) processed**
    - **Successfully configured**
    - **Failed to configure**
    - **List(s) pending to be processed**

    When the list is added to the Element Manager, the Lists Web page appears and the new list appears with the existing lists.

Use the following procedure to add a Group Hunt list.

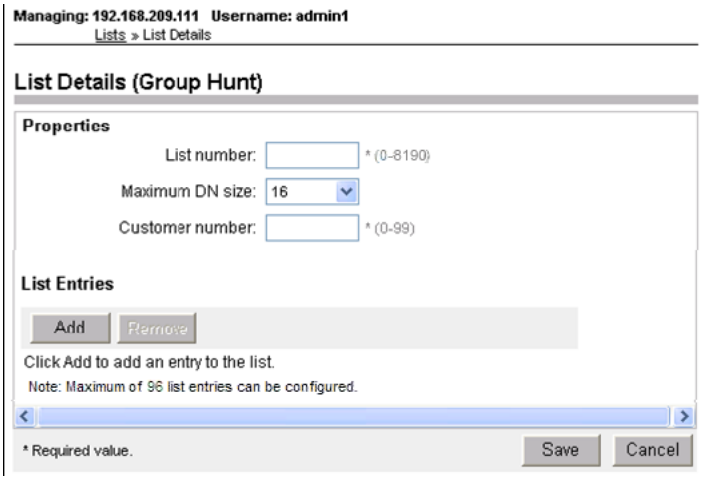
Adding a Group Hunt List

1. Select **Group Hunt** from the drop-down list on the Lists Web page.

   The **Add** button is enabled.

2. Click **Add** .

   The List Details (Group Hunt) web page appears.



3. Type the number of the list in the **List number** field.

   You can give a value between 0 and 8190.

4. Select the maximum DN size of the Speed Calls lists to be created from the drop-down list in the **Maximum DN size** field.

   Default value of the field is **16** .

5. Type the customer number for the list in the **Customer number** field.

   You can give a value between 0 and 99.

6. Click **Add** .

   A row for the **Entry Number** and **DN** fields appear in the **List Entries** block.

7. Type the first number for the list entry in the **Entry Number** field.

8. Type the first DN number for the list entry in the **DN** field.

   To add more rows, you can use the **Add** button.

   You can add up to 96 list entries for a Group Hunt list.

9. To remove a list entry perform the following steps:

   - Select the check box corresponding the entry to be removed.

     The **Remove** button gets enabled.

   - Click **Remove** .

     The selected list entry is removed from the block.

10. Click **Save** .

    The page refreshes to show the status of the process. The page displays the following information:

    - **Status**
    - **Total call list(s)**

- **List(s) processed**
- **Successfully configured**
- **Failed to configure**
- **List(s) pending to be processed**

When the list is added to the Element Manager, the Lists Web page appears and the new list appears with the existing lists.

Perform the following procedure to edit a list.

Editing a List

1. Click the required list from the Lists Web page.

   The details page of the particular list appears

2. Edit the values as required.

   You can update the values for List types, Group call, Group hunt, Speed call, and System speed call. For more information about List types, refer Table 4: Editing List Types on page 360.

3. Click **Add** to add list entries.
4. To remove any list entries, select the entry and click **Remove** .
5. Click **Save** to save the changes made to the list.

Table 4: Editing List Types

List Types	Fields
Group call	Group call control list entries
Group hunt	Maximum DN size list entries
Speed call	Maximum DN size list entries
System speed call	Maximum DN size network class of service list entries

Deleting a List

1. Select the check box of the list you want to delete.

   If you want to delete more than one list, select the check boxes against each list. If you want to delete all the lists, select the check box corresponding to the **List Number** field.

   The **Delete** button gets enabled.

2. Click **Delete** .

   A dialog box appears asking confirmation to delete the list.

3. Click **Yes** to delete the selected lists.

   Status of deleting is displayed as Completed and the Lists Web page is updated with current information about lists.

Migration

Use the Migration Web page to migrate telephone data from Element Manager to Subscriber Manager. This feature associates the telephone with existing subscribers, or adds a subscriber and then adds accounts to them.

Note:

For systems that have migrated to System Manager 6.2, Subscriber Manager has been replaced with User Profile Management (UPM). There is no automatic migration between EM (BCC) and UPM as there was between EM and Subscriber Manager for creating the subscribers. In System Manager 6.2 the EM Migration menu option is not intended to work in the UPM environment. It is only applicable to UCM deployments.

You can migrate only telephones that have a CPND name configured. During migration, the system checks with the Subscriber Manager for a subscriber with the same name as the CPND name in the telephone. Based on the search result, it either adds an account under the existing subscriber, or creates a new subscriber and then adds an account under it.

To start the Migration, select on the **Migration** link on the **Phones** branch of the Element Manager navigator. The Migration Web page appears as shown in Figure 250: Migration Web page on page 361.

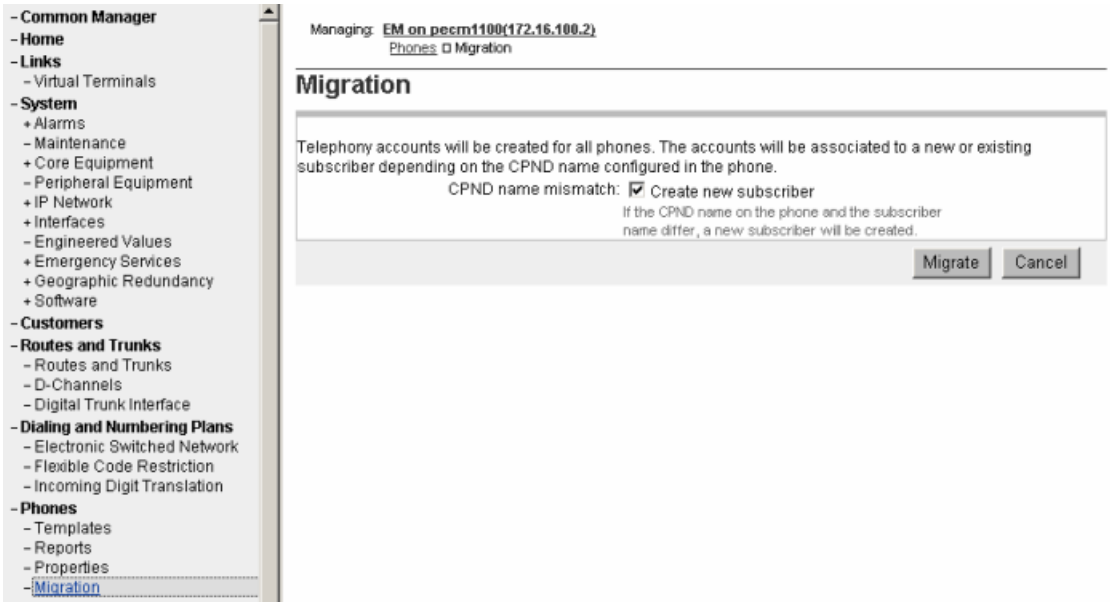


Figure 250: Migration Web page

To create a new subscriber when a CPND name mismatch occurs, ensure the **Create new subscriber** box is selected.

When you click **Migrate** , a confirmation message box appears before the migration starts.

While the migration is in progress, the system displays a status page that provides the current status of the migration. The page refreshes every 5 seconds with the latest status.

After the migration is complete, the page shows the summary as shown in Figure 251: Migration Results Web page on page 362.

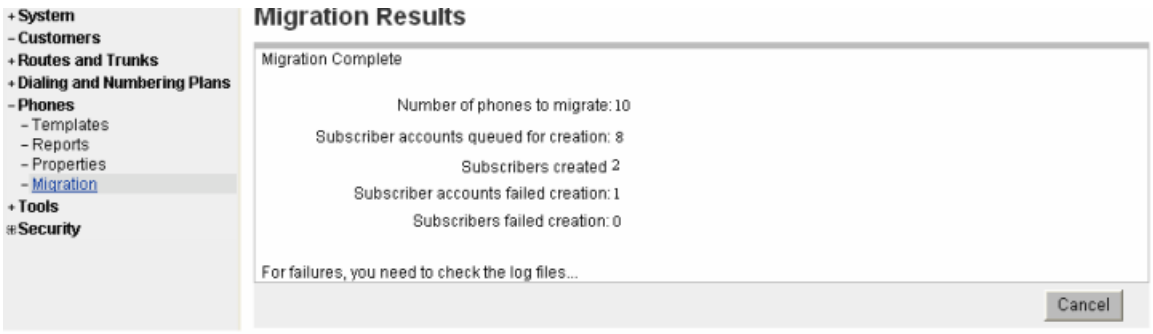


Figure 251: Migration Results Web page

High Scalability

The High Scalability feature centralizes and simplifies the phone configuration processes of the individual CS 1000 systems that constitute a CS 1000E HS system. This reduces the administrative effort and ensures data consistency. The user can use the HS-EM to perform phone operations like add, modify, and delete on different CS 1000 HA Systems, also known as cores, with the High Scalability feature.

When you launch the System Overview Web page, **Common Data** is the selected core in the **View** drop down . The core Common Data includes all the configurable values that can be applied commonly across the cores. When Common Data is the selected value, only **Template** link is available under **Phones** in the navigation tree.

The following figure shows the System Overview Web page when **Common Data** is the selected core.

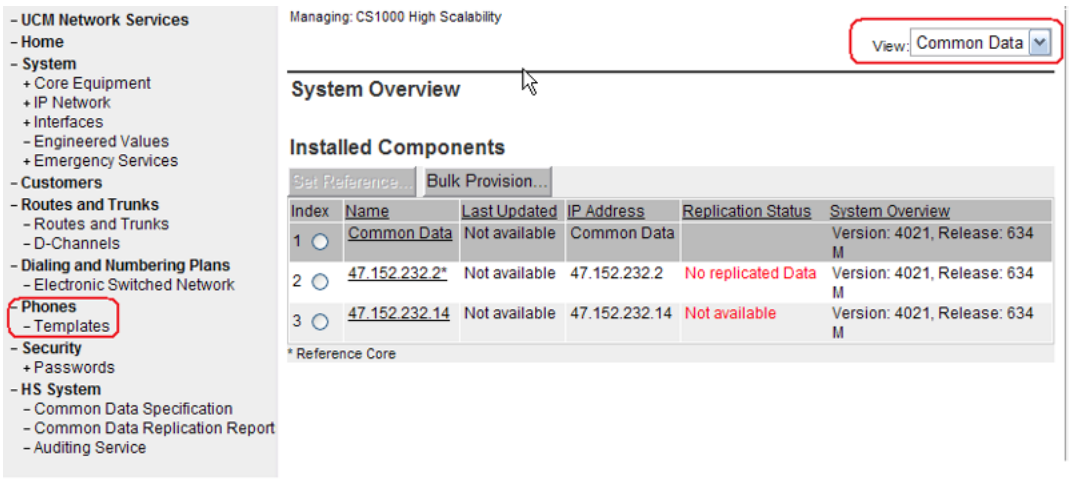


Figure 252: System Overview Web page

If you select any other core, other links under **Phones** appear in the navigation tree.

Launching EM by using reference core in HS EM

1. In the System Overview Web page, select a value from the box corresponding to the **View** field.

   The page refreshes to display the other links under **Phones** in the navigation tree.

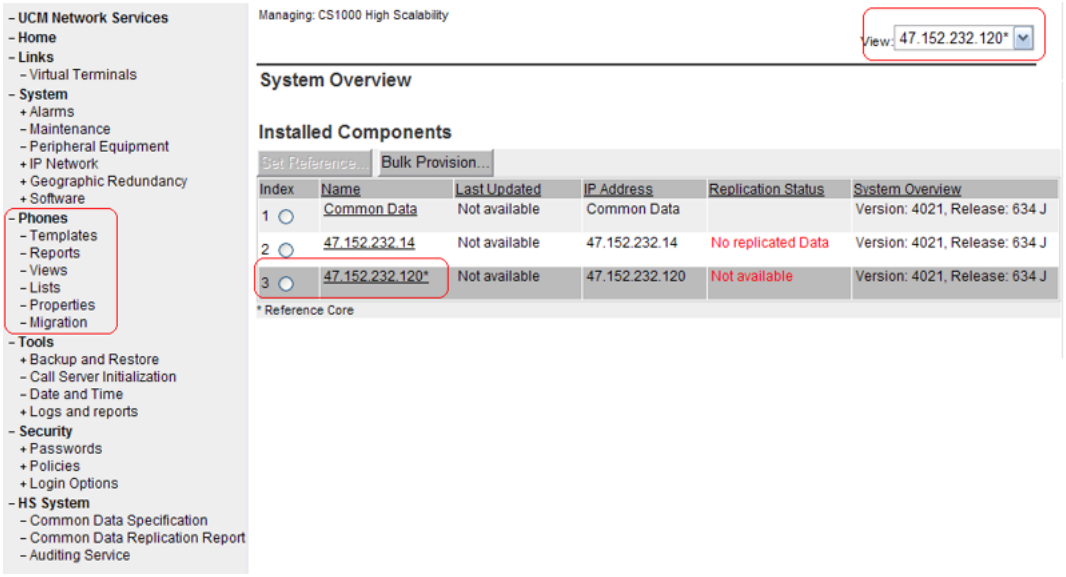


Figure 253: System Overview Web page

2. Click **Phones**.

   The Search For Phones Web page appears.

3. To change the core information, select the required value from the **View** drop down box.

The page refreshes to display the System Overview Web page with the selected value in the **View** drop down box.

Chapter 12: Tools

Contents

This chapter contains the following topics for Avaya Communication Server 1000 (Avaya CS 1000):

Introduction

The following Call Server Tools can be accessed through Element Manager:

- Backup and Restore
- Call Server Initialization
- Date and Time
- Logs and Reports

Backup and Restore

The **Backup and Restore** link of the **Tools** branch of the Element Manager navigator provides access to Call Server Backup and Restore functions, as well as Personal Directories Backup and Restore functions.

The User Admin Fields is backed and restored up as part of the sysbackup/sysrestore command or Backup/Restore Option from Deployment Manager. This is same for any other data (keys and features) in Element Manager. Backing up the data is important as the userfields are not stored on the Call Server.

Call Server

In the Services branch of the Element Manager navigator, click **Backup and Restore > Call Server**. The Call Server Backup and Restore Web page opens (see Figure 254: Call Server Backup and Restore Web page on page 366).

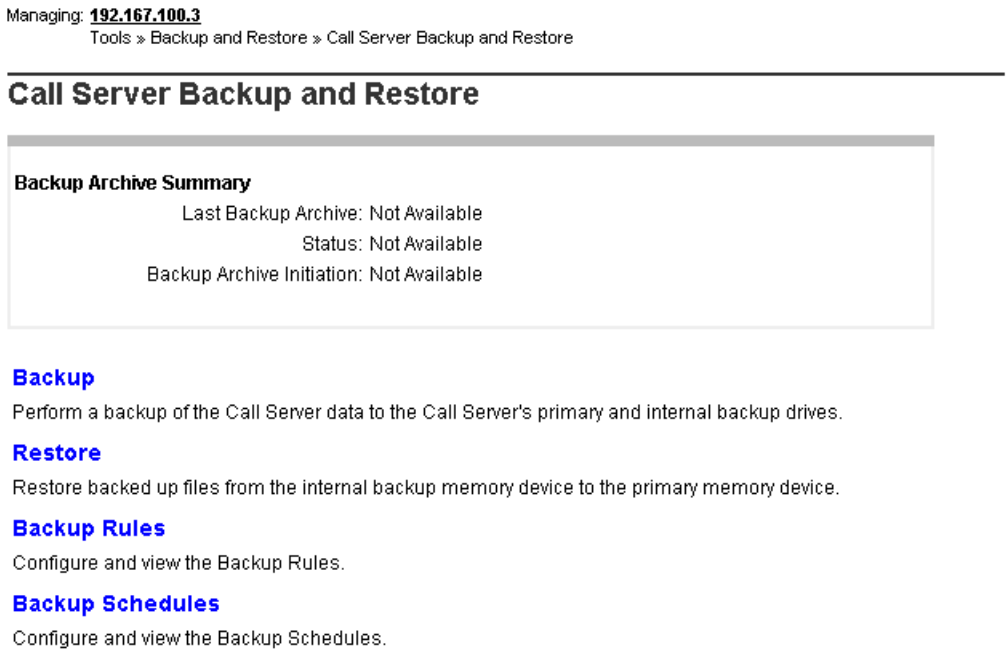


Figure 254: Call Server Backup and Restore Web page

Note:

Backup Rules and Backup Schedules are available only on CPP IV and CP PM systems.

Important:

For information about restoration from a prior-Release Call Server, see Restoration of IP Telephony Nodes from a prior-Release Call Server on page 369.

Backup

To back up the Call Server, click the **Backup** link on the Call Server Backup and Restore Web page. The Call Server Backup Web page opens, as shown in Figure 255: Call Server Backup Web page on page 367.

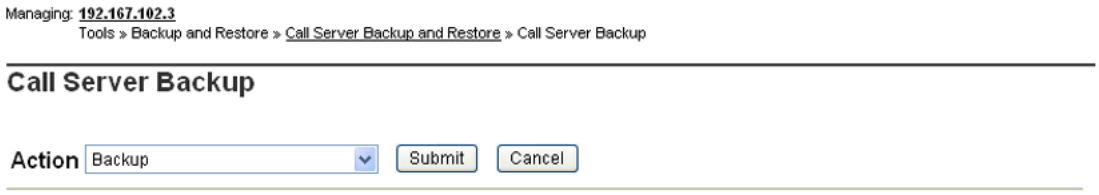


Figure 255: Call Server Backup Web page

Select **Backup** from the **Action** drop-down list and click **Submit**. The Call Server Backup Waiting Web page opens to indicate that the backup is in progress.

The Backup function invokes a data dump and writes the Call Server data to the primary and internal backup drives.

The Backup function performs the same task as the EDD CLI command traditionally configured in LD 43.

A summary of the results of the EDD appears at the bottom of the Call Server Backup Web page.

Performing manual database replication

To manually invoke the database replication process, select **Backup According to Rule** from the **Action** drop-down list, and click **Submit**. The **Backup Rule Number** drop-down list appears. In the **Backup Rule Number** drop-down list, enter the Backup Rule number to use for the restore operation. Click **Submit**.

For more information on backing up and restoring databases for Geographic Redundancy, see *Avaya System Redundancy Fundamentals, NN43001-507* .

Restore

The Call Server Restore function restores the backed-up files from the internal backup device to the primary device. The Restore function performs the same task as the CLI RIB command traditionally configured in LD 43.

Important:

For information about restoration from a prior-Release Call Server, see Restoration of IP Telephony Nodes from a prior-Release Call Server on page 369.

Warning:

The process to restore data using the Element Manager interface is immediate. There is no warning or detailed information provided on the specifics of the data to be restored.

Also, note that a "cold start" of the system is required before the restored data is in effect.

Click the **Restore** link on the Call Server Backup and Restore Web page. The Call Server Restore Web page opens (see Figure 256: Call Server Restore Web page on page 368).

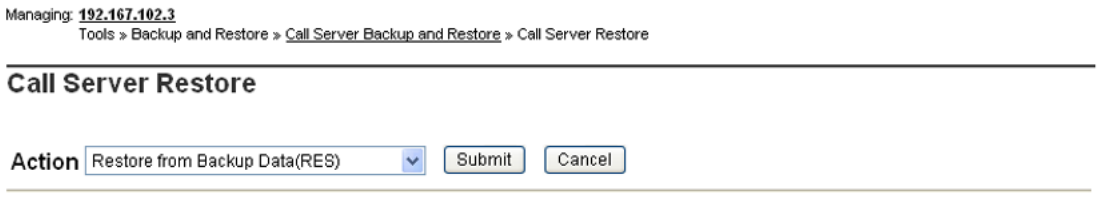


Figure 256: Call Server Restore Web page

Select **Restore from Backup Data (RES)** in the **Action** drop-down list, and click **Submit**.

Note:

The database for Element Manager IP Telephony is updated immediately after the restore. Other call server databases require a cold start after the restore.

For information about the server databases and when they were created, select **Database issue and creation date** in the **Action** drop-down list, and click **Submit**. The information is displayed in the text area below the command.

To manually invoke a database restore process, select **Restore According to Rule (RSR X Y)** from the **Action** drop-down list. The **Backup Rule Number** and **Restore Version** drop-down lists appear, as well as the Apply Filtering checkbox.

In the **Backup Rule Number** drop-down list, enter the Backup Rule number to use for the restore operation.

For more information on backing up and restoring databases for Geographic Redundancy, see *Avaya System Redundancy Fundamentals, NN43001-507* .

Restoration of IP Telephony Nodes from a prior-Release Call Server

You can restore Call Servers from prior releases to a Call Server running the current Release. Before you begin the restore operation, you must delete all of the IP Telephony Nodes, which exist on the current-Release Call Server. Deleting the IP Telephony Nodes removes the mapping between the elements and the nodes, so that all elements of the current-Release IP Telephony Nodes are available to add to the restored nodes. For more information about management of IP Telephony Nodes, see IP Telephony Nodes on page 123.

You must remove all elements from the node that are not a part of the current Release configuration, before you perform Save and Synchronize operations.

Backup Rules

To add or edit a Backup Rule, click the **Backup Rules** link on the Call Server Backup and Restore Web page. The Backup Rules Web page opens as shown in Figure 257: Backup Rules Web page on page 370.

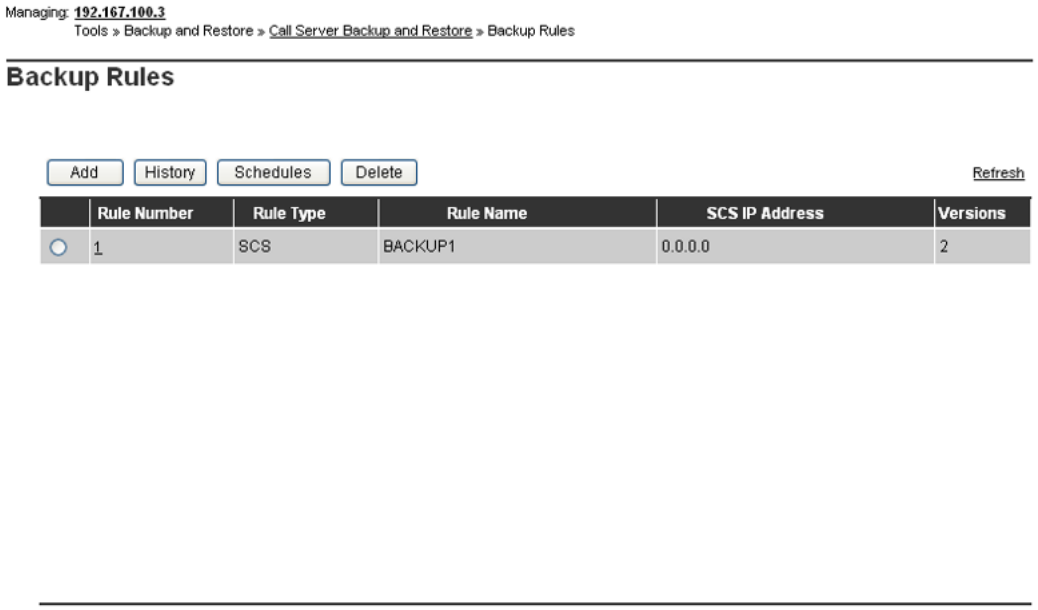


Figure 257: Backup Rules Web page

To view a log of backup attempts, select a **Backup Rule** and click **History** . The Backup History Web page opens. This Web page displays information for each backup attempt based on the given Backup Rule.

To add a Backup Rule, click **Add** on the Backup Rules Web page. The Add Backup Rule Web page opens. To edit a Backup Rule, click the Backup **Rule Number**. The Edit Backup Rule Web page opens, as shown in Figure 258: Edit Backup Rule Web page on page 371.

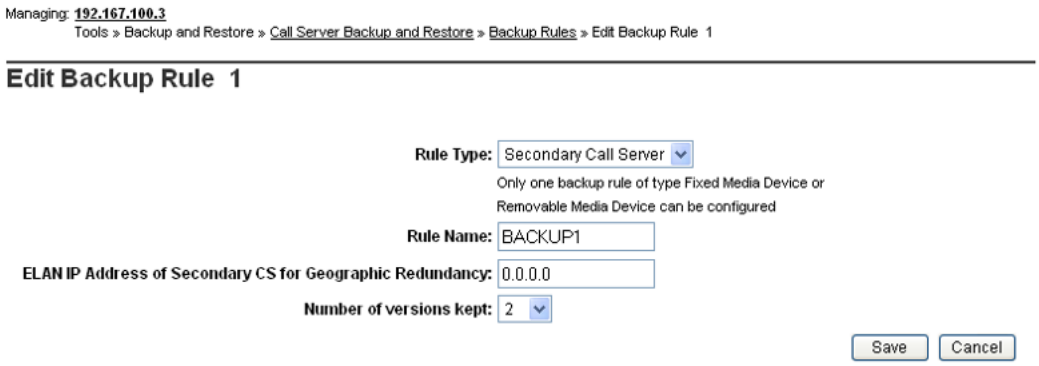


Figure 258: Edit Backup Rule Web page

The following Backup Rule Types are available:

- Fixed Media Device
- Protected Fixed Media Device
- Removable Media Device
- FTP
- Secondary Call Server

For more information about how to configure backup rules for Geographic Redundancy, see *Avaya System Redundancy Fundamentals, NN43001-507* .

Backup Schedules

Backup schedules provide the user with the ability to schedule backup operations associated with a specified backup rule. To add or edit a Backup Schedule, click the **Backup Schedules** link on the Call Server Backup and Restore Web page. The Backup Schedules Web page opens as shown in Figure 259: Backup Schedules Web page on page 372

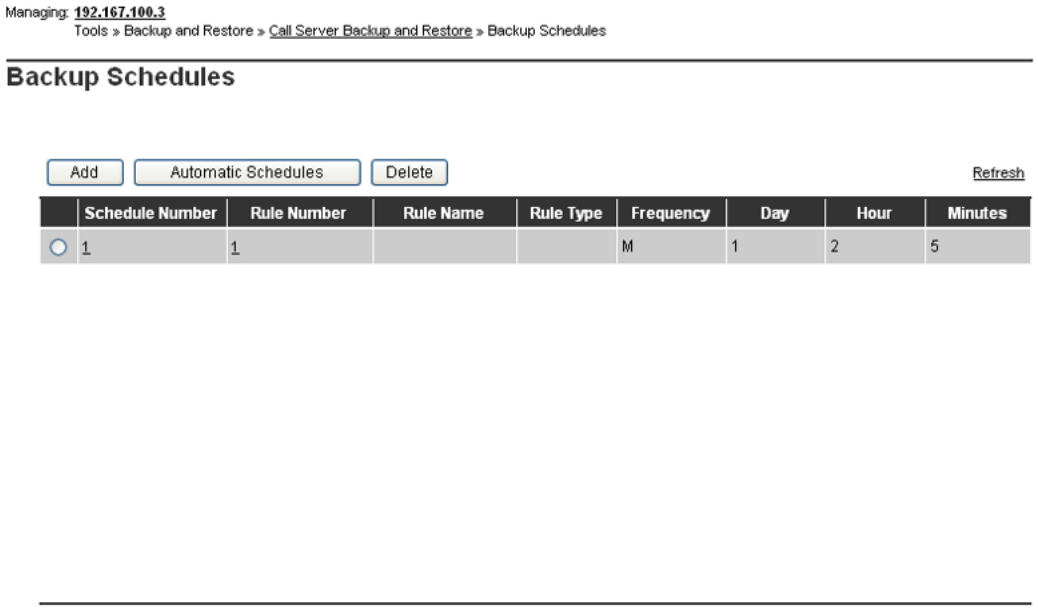


Figure 259: Backup Schedules Web page

To add a Backup Schedule, click **Add**. The Add Backup Schedule Web page opens. To edit a Backup Schedule, click the **Schedule Number**. The Edit Backup Schedule Web page opens, as shown in Figure 260: Edit Backup Schedule Web page on page 373.

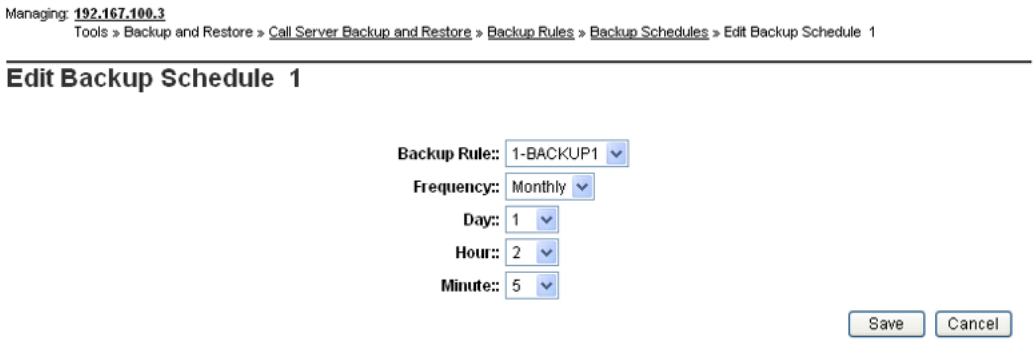


Figure 260: Edit Backup Schedule Web page

Each backup schedule defines a total of six associated parameters, as follows:

- **Backup Schedule Number** — up to ten backup schedules can be defined, numbered from one to ten.
- **Backup Rule** — specifies the backup rule number associated with this backup schedule. The backup rule number must be previously configured.
- **Frequency** — defines how often the scheduled backup operation occurs. The default is D. Not more than one backup schedule can be defined with Frequency set to the value A. Options are:
  - M (monthly)
  - W (weekly)
  - D (daily)
  - A (automatic — immediately after every EDD)
- **Day** — specifies the day on which the backup occurs with a default value of SU. When Frequency is M, the range is 1 to 31 with a default value of 1. This parameter does not apply when Frequency is set to either of the values D or A. When Frequency is W, the range is the days of the week as follows:
  - SU
  - MO
  - TU
  - WE
  - TH
  - FR

- SA

- **Hour** — specifies the hour in the day on which the backup occurs. The range is 0 to 23, with a default of 3. This parameter does not apply when FREQ is set to the value A.
- **Minute** — specifies the minute in the hour in the day on which the backup occurs. The range is 0 to 59.

To update Backup Schedules, click Automatic Schedules. The Update Backup Schedules Web page opens, as shown in Figure 261: Update Backup Schedules Web page on page 374.

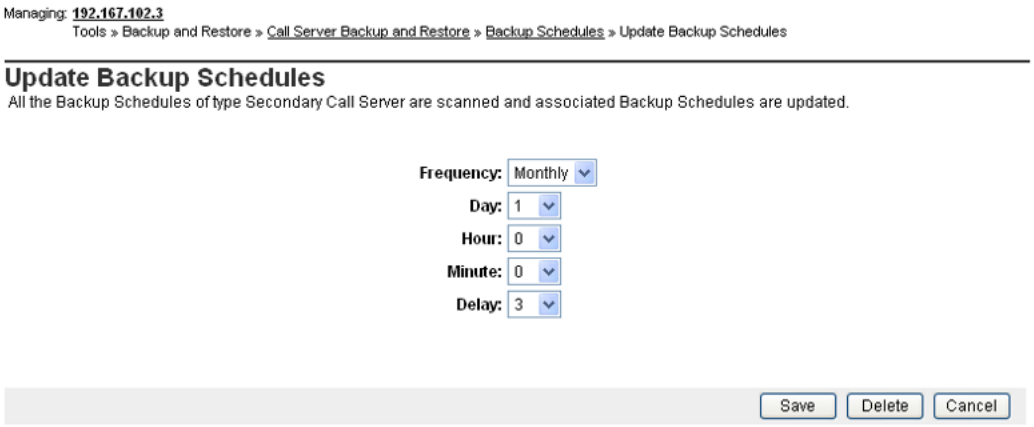


Figure 261: Update Backup Schedules Web page

Backup schedules are supported only on CP PIV and CP PM systems. A backup schedule can be created, modified, deleted, and printed by the respective command options **NEW, CHG, OUT**, and **PRT**.

Personal Directories Backup and Restore

To backup or restore Personal Directories click the **Backup and Restore > Personal Directories** link of the **Tools** branch of the Element Manager Navigator.

Note:

Element Manager always uses SFTP if it is enabled for the system. You must explicitly disable SFTP in order to perform backup and restore to FTP servers.

The Personal Directories Backup and Restore Web page opens and shown in the following figure.

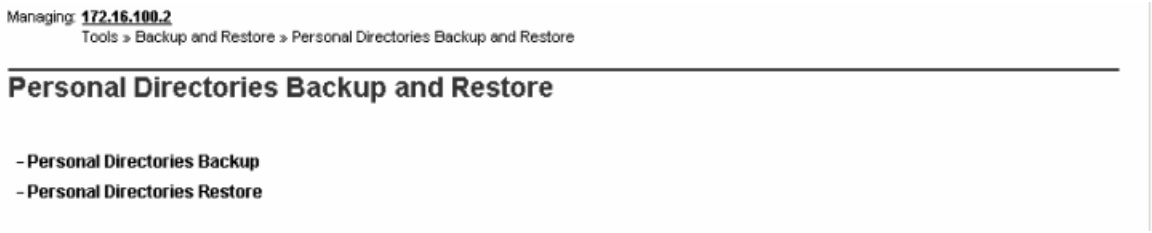


Figure 262: Personal Directories Backup and Restore Web page

To backup Personal Directories click the **Personal Directories Backup** link on the Personal Directories Backup and Restore Web page.

The Personal Directories Backup Web page opens as shown in the following figure.

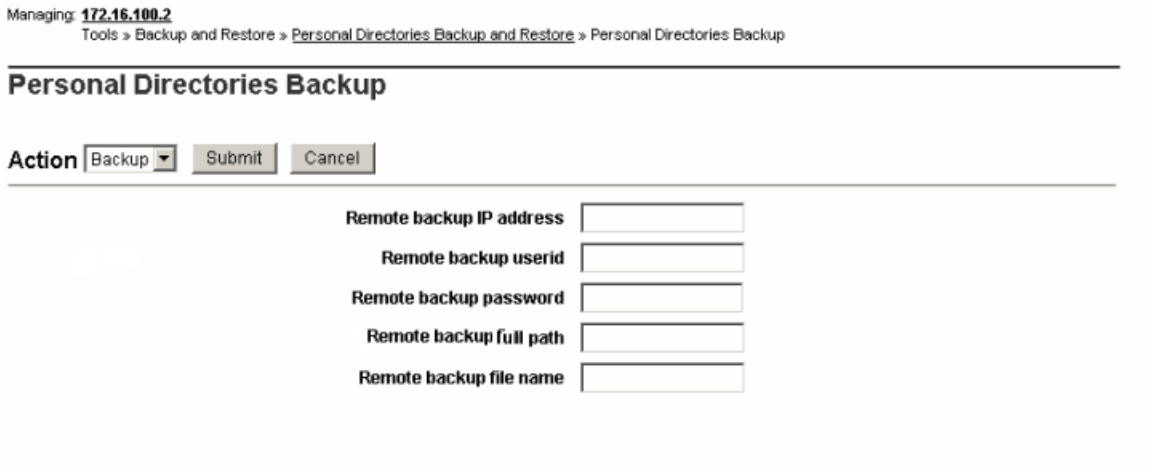


Figure 263: Personal Directories Backup Web page

To backup Personal Directories, enter the backup information and click **Submit** .

To restore Personal Directories click the **Personal Directories Restore** link on the Personal Directories Backup and Restore Web page.

The Personal Directories Restore Web page opens as shown in the following figure.

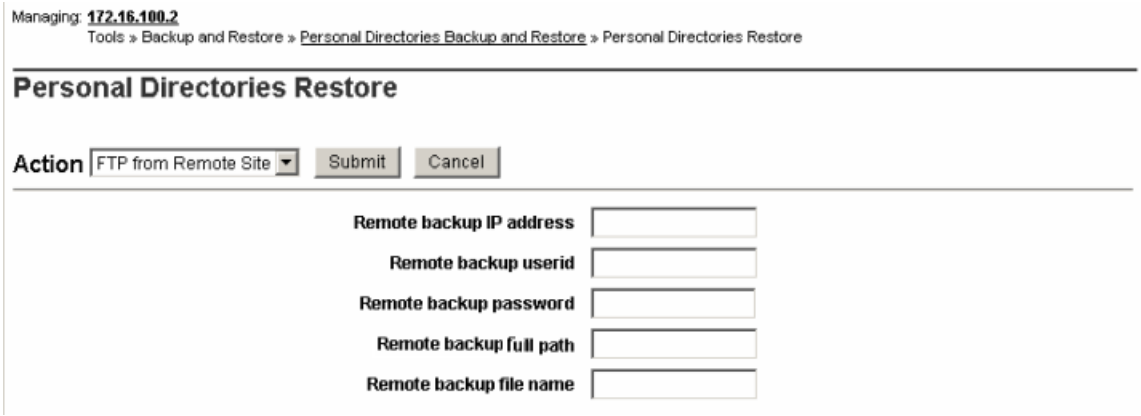


Figure 264: Personal Directories Restore Web page

To restore Personal Directories, enter the backup information to restore and click **Submit** .

For information on Backup and Restore functions of Personal Directories, Personal Directories on page 185.

Call Server Initialization

The Call Server Initialization page is used to invoke Call Server INI & Call Server SYSLOAD commands.

Click the **Call Server Initialization** link in the **Tools** branch of the Element Manager navigator. The Call Server Initialization Web page opens, as shown in Figure 265: Call Server Initialization Web page on page 376.

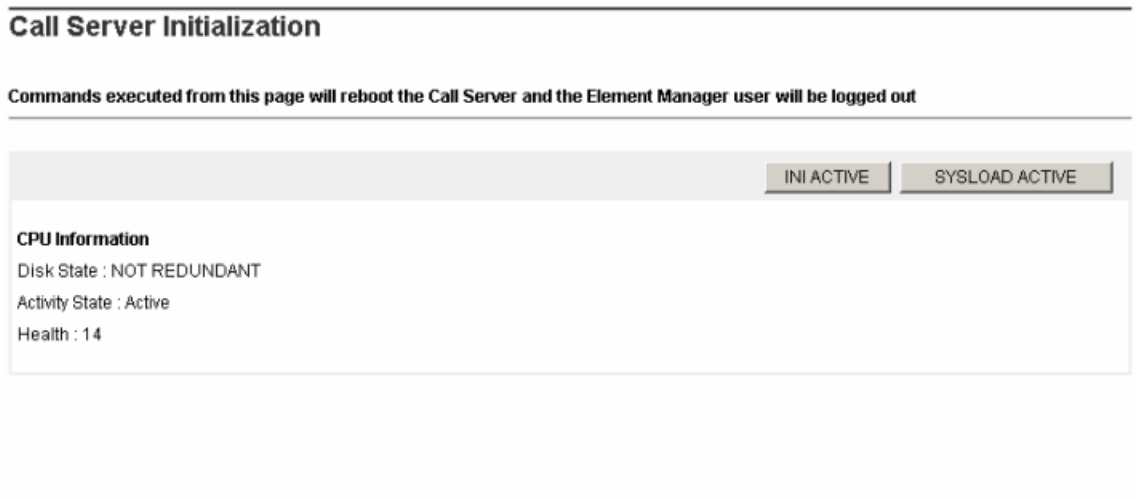


Figure 265: Call Server Initialization Web page

To check for the message displayed, roll the mouse over buttons displayed on the page.

If there is an INI command on the button, then the following message appears, “Restarts the Application Server”.

If it is a SYSLOAD command, then another message appears, “Restarts the Application Server as well as the Operating System”.

Call Server INI ACTIVE Command

The Call server is a Redundant System or a Split System on the Active side.

Initializing the INI ACTIVE command

1. Click **INI ACTIVE** .

   A confirmation message is displayed.
2. Click **OK** .

   The Call Server is rebooted and the Element Manager user is logged out.

Call Server INI INACTIVE Command

The Call server is Redundant System on the Inactive side.

Initializing the INI INACTIVE command

1. Click **INI INACTIVE** .

   A confirmation message is displayed.
2. Click **OK** .

   The inactive core reboots.

Call Server INI BOTH Command

The Call Server is a CPP Redundant System.

Initializing the INI BOTH command

1. Click **INI BOTH** .

   A confirmation message is displayed.
2. Click **OK** .

The Call Server is rebooted and the Element Manager user is logged out.

Call Server SYSLOAD ACTIVE

The Call server is a Redundant System or a Split System on the Active side.

Initializing the SYSLOAD ACTIVE command

1. Click **SYSLOAD ACTIVE** .

   A confirmation message appears.
2. Click **OK** .

   The Call Server reboots and the Element Manager user is logged out.

Call Server SYSLOAD INACTIVE Command

The Call server is Redundant System on the Inactive side.

Initializing the SYSLOAD INACTIVE command

1. Click **SYSLOAD INACTIVE** .

   A confirmation message appears.
2. Click **OK** .

   The inactive core goes for sysload.

Call Server SYSLOAD BOTH Command

The Call Server has a Redundant System.

Initializing the SYSLOAD BOTH command

1. Click **SYSLOAD BOTH** .

   A confirmation message appears.
2. Click **OK** .

   The Call Server reboots and the Element Manager user is logged out.

Note:

If the selected command is does not run successfully for any reason, such as an overlay conflict for example, the following error message appears, “The command was not executed successfully. Try again.”

Date and time

The date and time management covers the configuration of time synchronization options, as well as the setting of the actual date and time, and time zone related settings. An important concept is that there is a recommended configuration for any elements that are part of a CS 1000 system (these are running CS 1000 applications, such as CS, SS, SIPL, PD).

Timezone offsets for distributed phone subscribers is separately configurable through the Element Manger Branch Office zone configuration. In order to ensure that the configuration for a CS 1000 system is consistent, the configuration must be done using Element Manager.

The purpose of system-level coordination of the operating system date and time configuration for all elements of a single CS 1000 system is to facilitate the interpretation of system event and error messages generated by different elements.

The CS 1000 system level date and time management in Element Manager allows the configuration of Network Time Protocol (NTP) and Network Time Synchronization (NTS). The NTS client and NTP usage are mutually exclusive options for the CS 1000 system. A Call Server may be designated as the NTS master and utilize NTP to synchronize its own time.

In Element Manager, the configuration setting of NTP requires the systemadmin permissions, whereas setting of the actual date/time clock requires either systemadmin or timeadmin permissions.

For any other Linux servers that are not part of a CS 1000 system, configuration is done using Base Manager of UCM. See *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Configuration of time synchronization options performed from Element Manager overrides those previously performed by CLI, Base Manager, or the install tool on all system elements. Conversely, if changes are attempted later on at the individual element level that may interfere with the system time synchronization options chosen at the system level using Element Manager.

Avaya recommends that you use the ELAN interface for all NTP communication within a system. This would be to communicate to CS 1000 NTP primary and secondary servers. The CS 1000 NTP primary and secondary servers would normally communicate with external NTP clock sources using their TLAN connections. If TLAN is not available, then ELAN would be used. In all cases, it is necessary to ensure that appropriate routing is in place for communication between devices. This applies for communication to external sources and also for communication with CS 1000 NTP primary and secondary servers if the ELAN network interfaces of devices are on different subnets.

System time synchronization options

The following are the time synchronization options offered. Only one such option may be chosen. All configuration for these options is done solely by Element Manager and conveyed to all system elements.

- NTS client (Call Server as NTS client) can be configured to allow the Call Server to be synchronized from a ISDN digital trunk D-channel. The Call Server then pushes time directly to all system elements. An exception is standalone Element Manager, where Element Manager is not running on an element with any of the Call Server, SS, SIPL, or PD applications. In such as case, Base Manager must be used to set appropriate time synchronization, if required, on that element
- NTS Master (Call Server as NTS master) can be configured to allow the Call Server to act as the NTS Master. This Call Server provides time synchronization to other Call Servers set up as NTS slaves across MCDN. The system with Call Server as NTS master may use NTP configuration to maintain time from external time sources or internal hardware clock of the CS 1000 Primary NTP server.
- CS 1000 system level primary and, optionally, secondary NTP servers are configured on Linux system elements that are part of this CS 1000 system. The secondary NTP server would act as a backup for the primary NTP server, and normally synchronize time with the primary NTP server and then try with other external sources. The default is that the element on which Element Manager is running is set as the CS 1000 primary NTP server, but that can be altered. All other Linux system elements (including EM if applicable) will synchronize to these CS 1000 NTP servers. Configuration is done by EM and pushed to all Linux elements.

  The CS 1000 primary and secondary NTP servers can source their time in two ways:

  - The CS 1000 primary and secondary NTP servers use their internal hardware clocks. The date/time has to be set using Base Manager on the primary (assuming that the secondary NTP server will sync time from the primary NTP server in normal operation).
  - External NTP clock sources are used. The internal system primary and secondary NTP servers are synchronized from external clock sources, up to 10, with optional single key security. The secondary NTP server would normally synchronize with the primary NTP server, and only synchronized with the external sources if the primary is not available.

If you use NTP security, all the clock source servers need to have the same private key. This means that an internal primary NTP server can not use a different key to access an external server than that which is used for servicing requests from internal clients. The implication is that if the external connection is to be secured, the internal connections would also have to be secured using the same single key as the external connections. Also, all the external servers

need to have the same private key to service the requests from the internal servers or other Linux NTP clients.

Note:

In previous releases, the Call Server supported configuration of two external clock sources with different private keys for each, but only a single private key is supported in Communication Server 1000 from Release 6.0.

When NTP configuration is done using EM, the ELAN IP addresses of system elements are obtained from UCM element information and used for the configuration of such elements as primary or secondary NTP servers.

When NTP is utilized, you must configure each element with time zone and daylight saving adjustments. Element Manager supports Windows-style selection of time zones. The time zone you select determines the time zone regions and subregions to be used on Linux system elements. The configuration associated with the time zone you select is applied to all system elements

System Date and Time

The System Date and Time Web page offers configuration of the following:

- The ability to configure the Date and Time for the system
- The ability to configure the Time Zone
- The option to configure Network Time Protocol for the system
- The option to configure Network Time Synchronization for the system

Note:

If there are no time synchronization options currently chosen (i.e., neither NTP nor NTS are configured) then a warning appears.

Click the **Date and Time** link in the **Tools** branch of the Element Manager navigator. The System Date and Time Web page opens, as shown in Figure 266: System Date and Time Web page on page 382.

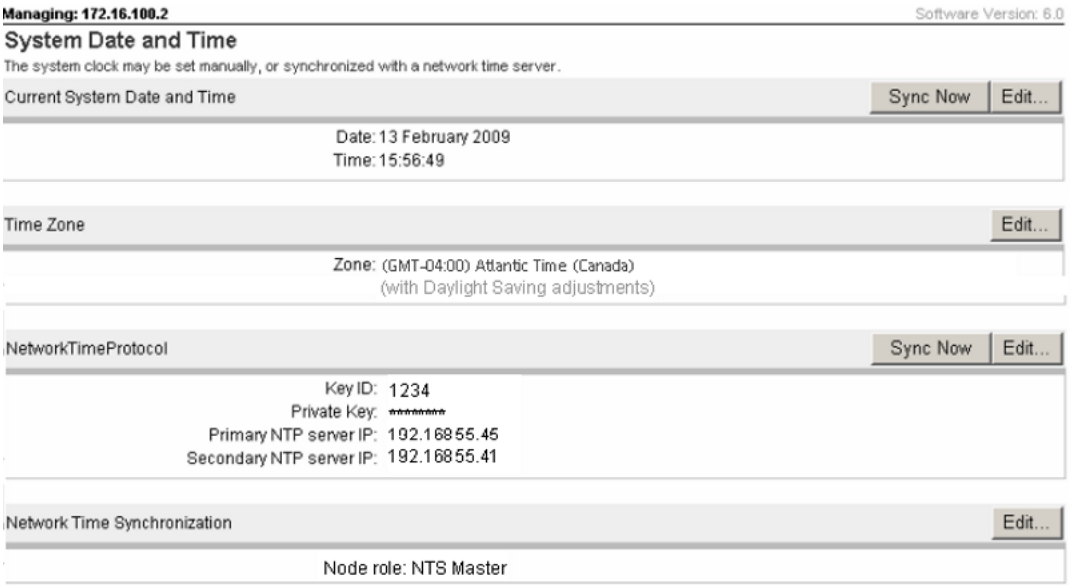


Figure 266: System Date and Time Web page

Note:

If NTP is disabled the **Sync Now** button is disabled, as shown in the following figure:

Figure 267: System Date and Time — Sync Now disabled

The System Date and Time Web page summarizes the following sections:

- Current System Date and Time: The time displayed is always the Call Server time.
- Time zone: The time zone configured for the CS 1000 system is displayed
- Network Time Protocol: The NTP server (Primary/Secondary) details are displayed. If security is configured then the key id and private key are shown (masked), otherwise a message is displayed with “Not configured".
- NTS configuration is displayed (NTS Master/NTS Slave/NTS Stand-alone).

Current System Date and Time

The Current System Date and Time section displayed on the System Date and Time Web page displays the current date and time on the CS 1000 Call Server. When you select **Edit**, you can manually configure the date and time on the Call Server or NTP server. Manual configuration of the date and time is not an operation that you would normally perform in the cases where either NTP or NTS were configured because manual adjustments would be overwritten.

The **Sync Now** button initiates re-application of the date and time configuration to all elements. If NTP is in use on the system this results in an immediate synchronization with external NTP sources and/or the CS 1000 primary NTP server. If NTP is not in use the **Sync Now** button is disabled.

If NTP is in use and the Primary NTP server is joined to the security domain, you are redirected to Base Manager to configure the date and time on the internal Primary NTP server. If NTS is in use, configure the date and time on the Call Server (in the case of a Linux-based Call Server, you are redirected to Base Manager).

Use the **Edit** button in the following scenarios:

- If the system is running as NTS slave then time is set on the Call Server. For a VxWorks Call Server clicking **Edit** brings up a new page to set the time. For the CP PM Co-Resident CS & SS on Linux, the Base Manager of the CS server is opened in a new window.
- If the system is using NTP and the Primary NTP server is not joined to the security domain, clicking **Edit** causes the following message to appear:

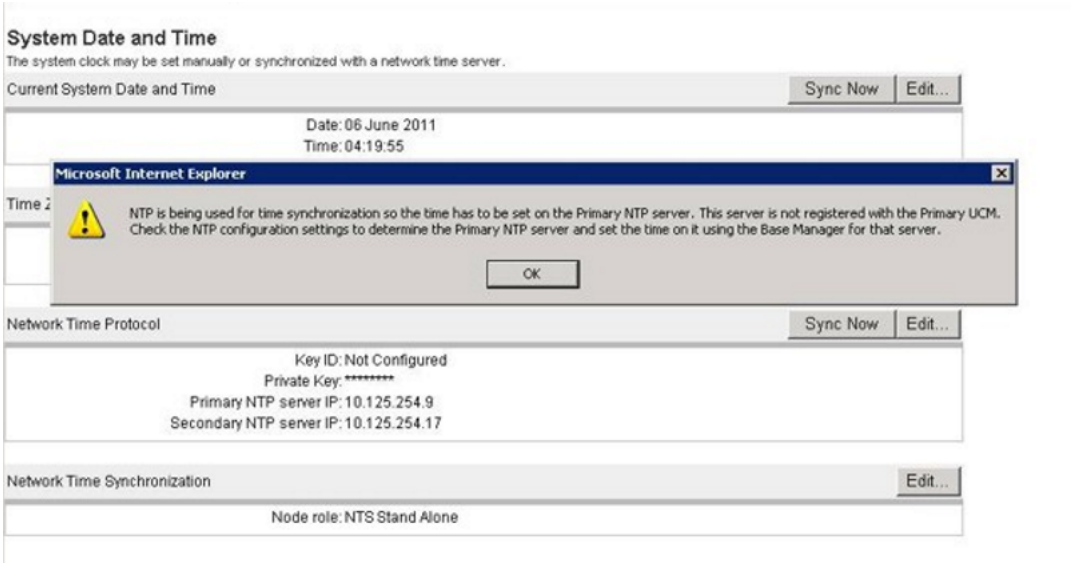


Figure 268: NTP time synchronization message

- If the system is using NTP and the Primary NTP server is joined to the security domain, clicking **Edit** opens the Base Manager time page of the Primary NTP server.
- In the case of NTS master or NTS stand-alone (i.e., NTS disabled), then if NTP is in use clicking **Edit** opens the Base Manager time page.
- If time synchronization is not configured, a warning is normally given when accessing the page. Clicking **Edit** allows the time on the Call Server to be set. For a VxWorks Call Server clicking Edit brings up a new page to set the time. For the CP PM Co-Resident CS & SS on Linux, the Base Manager of the CS server is opened in a new window.

If NTP is being used on the system, then after setting the time, click **Sync Now**, to immediately start time synchronization to all elements.

For more information about configuring Date and Time using Base Manager, refer to *Avaya Linux Platform Base and Applications Installation and Commissioning, NN43001-315*.

Editing date and time on a VxWorks Call Server

1. Click **Edit** in the Current System Date and Time section of the System Date and Time Web page.

   The Edit Date and Time Web page opens, as shown in Figure 269: Edit Date and Time Web page on page 385
2. Enter the **Date** and **Time** in the appropriate fields.
3. If necessary enter the value for the **Daily Time Adjustment** to compensate for a fast or slow system clock.
4. Click **Save** .

The System Date and Time Web page opens with the new time settings.

5. If NTP is being used on the system, click **Sync Now** to immediately start time synchronization to all elements.

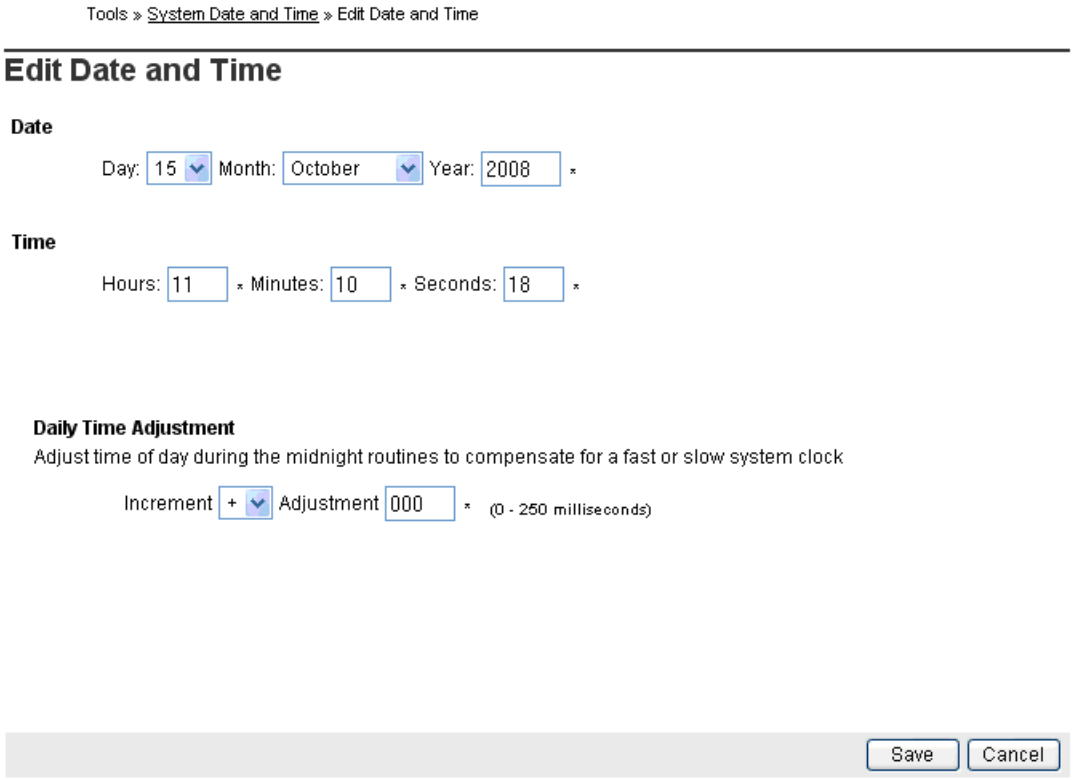


Figure 269: Edit Date and Time Web page

Time Zone

The Time Zone Web page displays the time zones and lists all the supported zones and UTC values. The time zone selected is used to set the time on the Call Server and Linux elements. For the case of a VxWorks Call Server internal mapping is also done of the offset from UTC and Daylight Saving time start and end dates. For a VxWorks Call Server, the Daylight Saving time start and end dates will be configured on the Call Server using the internally mapped values. For Linux devices, the Linux time region Daylight Saving time information is used.

If the time zone selected has automatic Daylight Saving adjustments built in, the text on the screen indicates that as “(with Daylight Saving adjustments)”, otherwise the text indicates “(no Daylight Saving adjustments)". Some time zones (e.g., currently those associated with Jerusalem and Tehran) have Daylight Saving dates that vary each year. These are not handled and you must manually change the time zones for these regions upon entering or leaving the Daylight Saving calendar period. When such time zones are selected, the text on the screen

indicates “(manual time zone change required when entering or leaving Daylight Saving period)”.

Editing the Time Zone

1. Click **Edit** in the **Time Zone** section of the System Date and Time Web page.

   The Time Zone Web page opens as shown in the following figure.
2. Select the Time Zone from the list.
3. Click **Save** .

   The System Date and Time Web page opens with the new time zone setting.

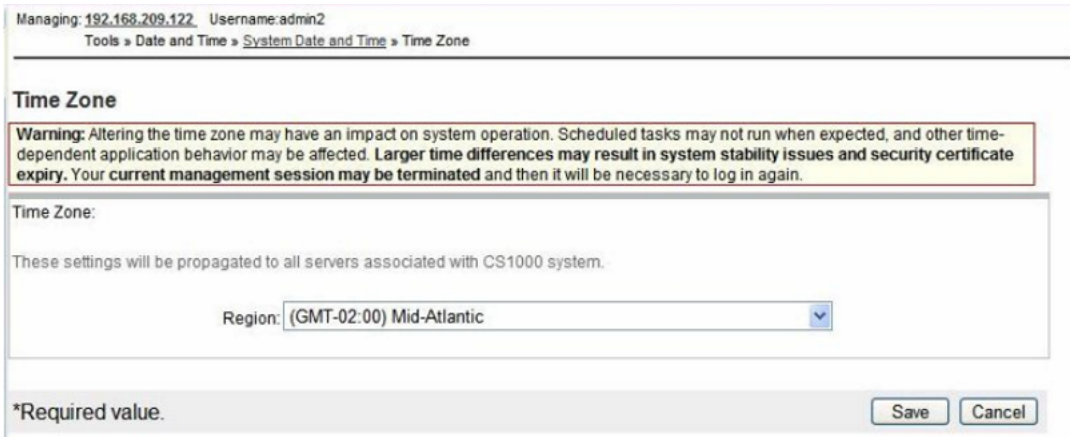


Figure 270: Time Zone Web page

Network Time Protocol

Prior to CS 1000 Release 6.0, Element Manager used overlay configuration of the Call Server (CS) on VxWorks to support system level NTP configuration. The NTP configuration only applied to the CS and all of the VxWorks based Communication Server 1000 system elements derived their time from the CS through a pbxLink.

You must use Element Manager to configure time synchronization settings that are used on the Call Server as well as all other system elements. Some settings for polling interval, query offset, and alarms which were applicable for VxWorks based CS are not offered now, since the Call Server now synchronizes only with internal system primary or secondary NTP servers, and not with external clock sources. These settings are hardcoded now and ten minutes for polling is the mid-range of Linux NTP clients.

If this is the first time that NTP is being configured, after you select the **Synchronize System Clock with NTP** check-box, the UI loads with a default configuration. The default configuration has the server running Element Manager selected as the internal Primary NTP server, and internal clock sources (hardware clock on this server) is used. If NTP had been previously

configured on the system, but subsequently disabled then the previous configuration is displayed.

The default selection for transfer mode is “Secure”. This selection requires the operator to enter the Key ID and Private key. Only a single key is supported to be applied for NTP protocol security between external clock sources as well as between internal system NTP servers and other system Linux elements. Only MD5 authentication is supported for NTP security. Selecting insecure transfer mode disables the fields for Key ID and Private key and the key data is not removed.

When you click the **Sync Now** button in the **Network Time Protocol** section, a ntpconfig command is sent to the Linux element with the pre-configured NTP details.

CS 1000 Linux System Elements

The NTP Configurations propagate into all Linux elements associated with the CS 1000 system. Default configuration shows the list of Linux elements registered with the CS 1000 system. Linux elements that are not associated with the CS 1000 system can be added and removed manually and updates the same for CS 1000 system-level NTP servers.

CS 1000 system-level NTP server(s)

The selection of a primary internal NTP server is mandatory, whereas a secondary internal NTP server is optional, but recommended when there are two or more Linux based elements configured in the CS 1000 system.

The secondary internal NTP server's NTP client normally gets its time source from the primary internal NTP Server. If the Primary internal NTP server does not respond to the Secondary, then the Secondary gets its time source from the first external NTP server which responds to polling by the Secondary.

NTP clients running on Linux base elements which are "Not a clock server", as well as on the VxWorks-based Call Server, get their time source from the Primary internal NTP server, or from the Secondary internal NTP server, if the Primary does not respond to polling by the other NTP clients in the CS 1000 system.

If NTP has not already been configured for the CS 1000 system, the default value for is the ELAN address Element Manager for the system. The drop down boxes for primary and secondary server IP addresses provide the choice of any Linux server associated with the given CS 1000 system. ELAN IP’s are always shown even if the hostname is on TLAN.

Note:

The Primary and Secondary IP addresses must be different and the system validates the IP addresses before they are accepted.

External Servers

The selection of External server(s) enables the additional fields labeled “NTP server IP” thereby allowing the operator to enter the IP addresses of one to ten external clock sources. The internal system primary and secondary NTP servers are Synchronized with these servers. The list is an ordered list, such that the first external source listed is contacted first, and if that fails then move on down the list. If the list is not in correct order then it may be necessary to delete sources and re-add in desired order. A newly added external server IPs is added to the end of the list.

If necessary to reach external servers then IP routing configuration may have to be performed on devices. This would not normally be required for devices that reach external sources by the TLAN, since the default route for most devices uses the TLAN. An IP route is required if the ELAN has to be used to reach an external source. The IP routes would have to be performed on the primary and secondary servers if required, and Base Manager can be used for this configuration. If external servers are not provided, the primary NTP server will derive its system clock from its internal hardware clock.

Note:

The maximum number of Network Time Protocol server IP addresses is ten entries and these are validated for uniqueness.

Network Time Protocol for High Scalability systems

Note:

The information in this section applies only to Communication Server 1000 High Scalability systems, which use Element Manager for High Scalability.

High Availability systems are managed by one instance of Element Manager for High Scalability. When you select a High Availability system, the navigation menu displays the option to configure the time synchronization parameters for that system. These parameters include the time zone, Network Time Protocol configuration, and Network Time Synchronization configuration.

You must configure Network Time Protocol separately for each core as the configuration settings are not included with common data. Redundant systems with Element Manager for

High Scalability and High Availability systems with local Element Manager both support Network Time Protocol configuration.

Note:

During Communication Server 1000 software upgrades, NTP configuration settings are retained only for Element Manager to Element Manager upgrades and not for Element Manager to Element Manager for High Scalability upgrades.

By default, the Network Time Protocol status for the Primary and Secondary NTP Servers is not configured. You must choose the Primary and Secondary NTP servers from the list of automatically generated system elements or the list of elements that have been added manually. The Element Manager for High Scalability system is not selected by default. If required, you must add it to the list manually.

For each High Availability system of High Scalability, you must configure the external NTP clock sources and any security keys separately.

If you use the local Element Manager to configure a core belonging to a High Availability system, the configuration is consistent with CS 1000 Network Time Protocol configuration, as described in Network Time Protocol configuration on page 389.

Network Time Protocol configuration

To configure Network Time Protocol, click the **Date and Time** link in the **Tools** branch of the Element Manager navigator. The System Date and Time Web page opens.

Configuring Network Time Protocol

1. Click **Edit** in the Network Time Protocol section of the System Date and Time Web page.

   The Network Time Protocol Web page opens as shown in Figure 271: Network Time Protocol Web page on page 391.

2. Select the **Synchronize System Clock with NTP** box.

   Note:

   Clicking this box enables Network Time Protocol configuration otherwise only synchronization is available.

3. Select **Secure** .

   Secure is the default setting.

4. Enter the **Key ID** and **Private Key**.

5. Select **Primary** and **Secondary IP** addresses from the lists.

   The drop down boxes for primary and secondary server IP addresses provide the choice of any Linux server associated with the given CS 1000 system.

Note:

If NTP has not been configured for the CS 1000 system, the default value for the primary server IP address is the ELAN address of the server hosting Element Manager for the system.

6. To select an external server as a clock source select the **External server(s)** box.

   Selecting External server(s) enables the additional fields labeled “NTP server IP” which allows you to enter the IP addresses of one to ten external clock sources.

   Note:

   Specifying an external NTP clock sources are optional, and if configured, are used by the local Primary and Secondary NTP servers. If external servers are not configured then the internal hardware clocks are used on the primary and secondary NTP servers.

7. Enter an external clock source and click **Add** .

   You can add up to ten external clock sources. The list is an ordered list, such that the first external source listed is contacted first, and if that fails then the next on the list is used.

   Note:

   You may have to perform IP routing configuration to reach external servers. This would not normally be required for devices that reach external sources by the TLAN, since the default route for most devices uses the TLAN. Base Manager can be used for IP route configuration.

8. Click **Save** .

   The parameters are transferred to all system Linux elements.

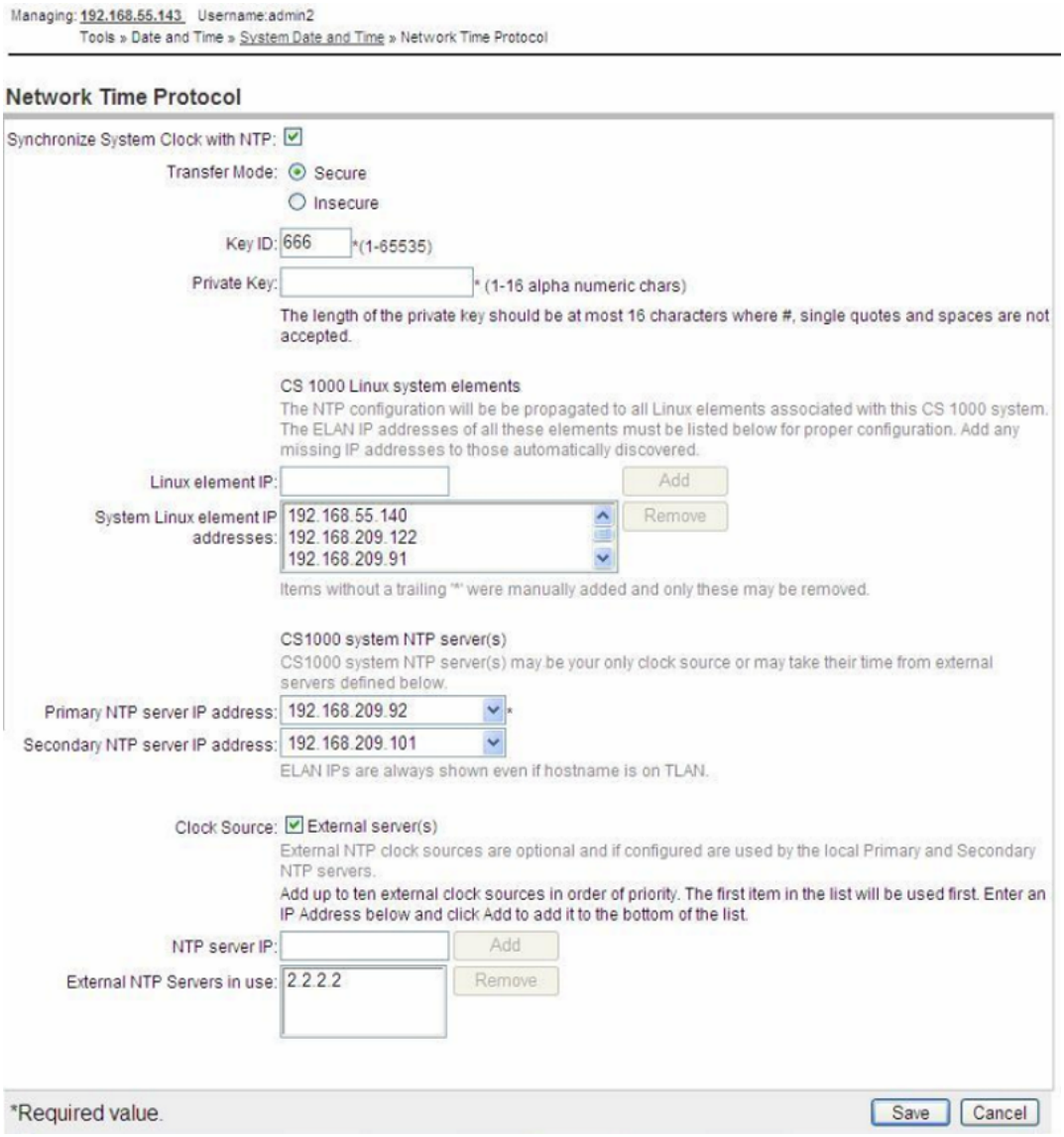


Figure 271: Network Time Protocol Web page

Network Time Synchronization

The clock synchronization feature is designed to work on ISDN networks, using D channel messages. NTS helps to synchronize time across different zones with different time zones for each. The Call Server is configured in master/stand-alone/slave modes for these zones. The stand-alone Call Server doesn't sync up with the master but the slave does sync up with the master. NTS enables the CS 1000 Call Server to derive its system clock from a Digital Trunk Signaling Link (DTRL). All of the other Signaling Servers, Media Gateway Controllers, and

Voice Gateway Media Cards associated with the CS 1000 system derive their system clock from the Call Server by signaling over the PBXLink. protocol.

Support for NTS has been included in the deployment of Linux based servers. If the CS 1000 Call Server NTS Node Role is set as NTS slave then NTP and NTS configurations are mutually exclusive. For roles like stand-alone and master user can configure NTP for the elements to get time synced from the NTP servers. The Time Delta time adjustment factor keeps the Call Server at a difference with the master Call Server. This allows the slave Call Server to keep CS 1000 system time for its local timezone. If there are DST differences between the master NTS and slave NTS then manual adjustments may be required of the offset as the DST starts/ ends.

You set the customer of the node and Local Virtual DN in charge of synchronizing the switch (that customer makes and receives the calls to and from the Master/Backup switch). That customer must already exist, prior to referencing it

If NTS is disabled and NTP is not in effect, then an warning message is shown to the user.

The Network Time Synchronization feature ensures that all time stamps in a network are synchronized from one source.

Configuring Network Time Synchronization

1. Click Edit in the Network Time Synchronization section of the System Date and Time Web page.

   The Network Time Synchronization Web page opens, as shown in Figure 272: Network Time Synchronization Web page on page 393.
2. Select the Node Role form the list.
3. Select the Customer from the list.
4. Enter the Local Virtual DN.
5. Enter the Master/Backup Time Synchronization Number.
6. Choose the mode: Background (BKGD) or Daily Services Routine (DVCS).
7. If there are Daylight Saving Time (DST) differences between the master NTS and slave NTS then manual adjustments may be required of the offset as the DST starts or ends. Enter the Time Adjustment factor with clock on Master values
8. Click Save.

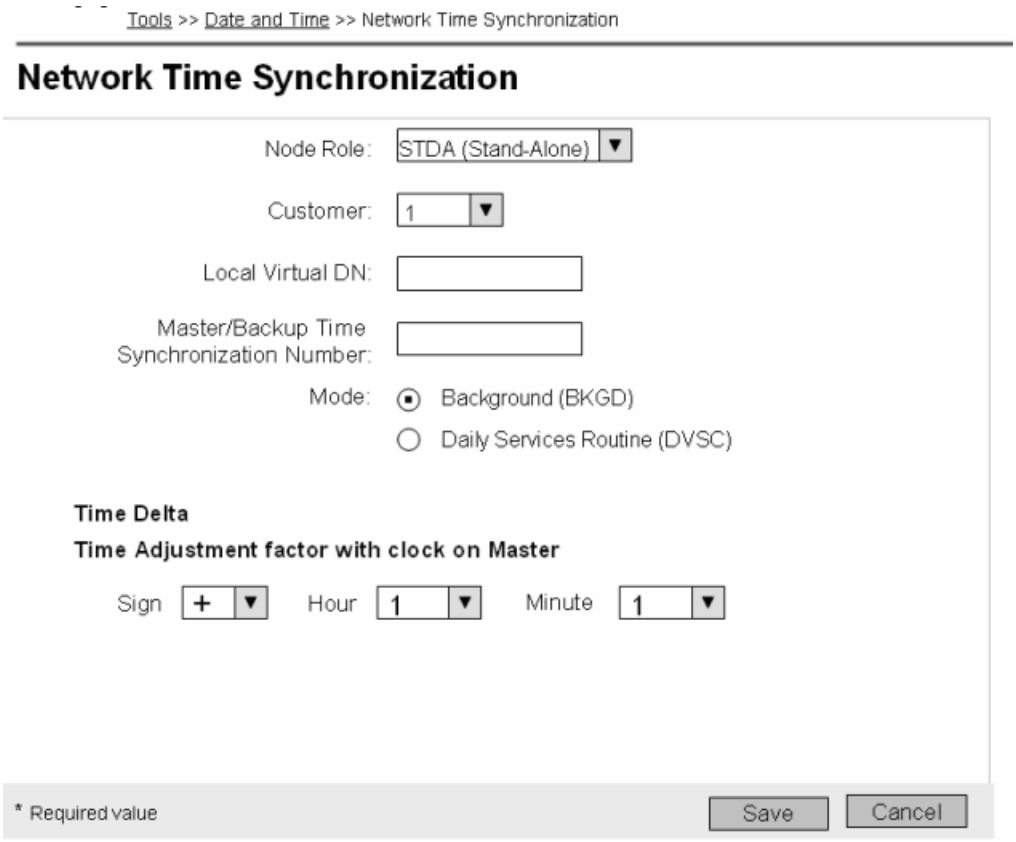


Figure 272: Network Time Synchronization Web page

Logs and Reports

To access IP Telephony Node Maintenance Reports click the **Logs and Reports > IP Telephony Nodes** link in the **Tools** branch of the Element Manager navigator. The Node Maintenance and Reports Web page appears.

For information on IP Telephony Node Maintenance and Reports, see Nodes: Servers, Media Cards on page 139.

In addition, information about the database status and synchronization are available under the Reports tab in NRS Manager. For more information on these reports, refer to *Avaya IP Peer Networking Installation and Commissioning, NN43001-313* .

To display information on all IP Phones configured in the system, click the **Logs and Reports > IP Phone Location** link in the **Tools** branch of the Element Manager navigator. The IP Phone Location Web page opens, as shown in Figure 273: IP Phone Location Web page on page 394.

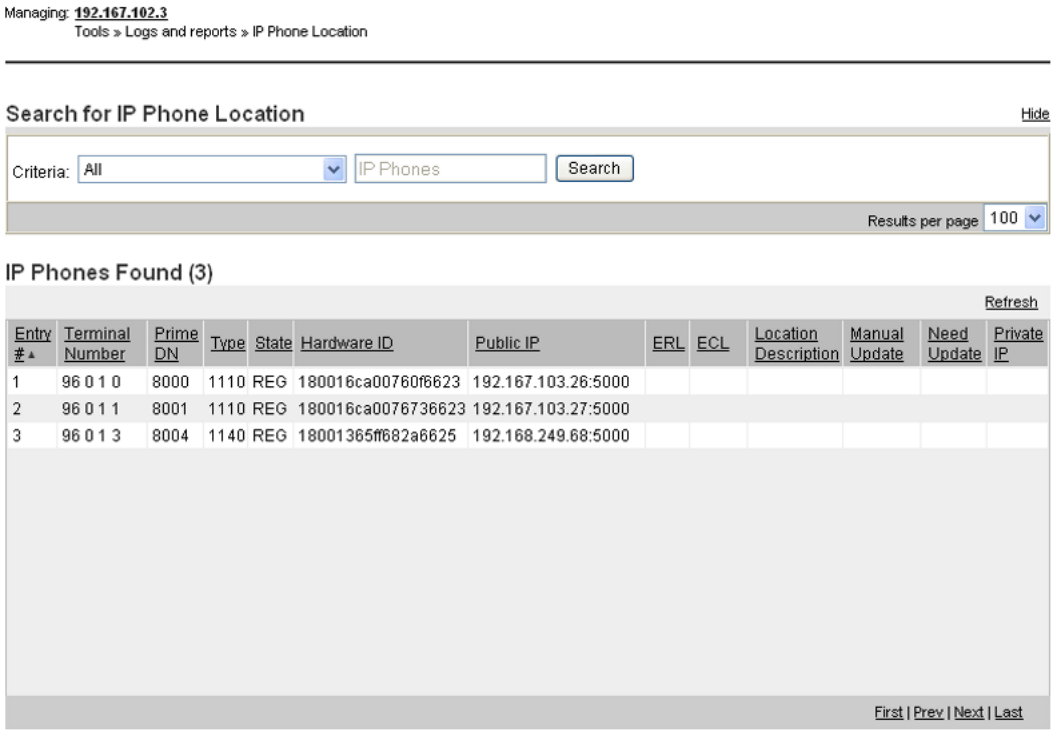


Figure 273: IP Phone Location Web page

Enter the search criteria in the Search for IP Phone Location section and click **Search**. The results matching the criteria entered are displayed in the IP Phones Found section.

Call Server Report

To access the Call Server Report Web page, click the **Logs and Reports > Call Server Report** link in the **Tools** branch of the Element Manager navigator. The Call Server Report Web page opens as shown in the following figure.

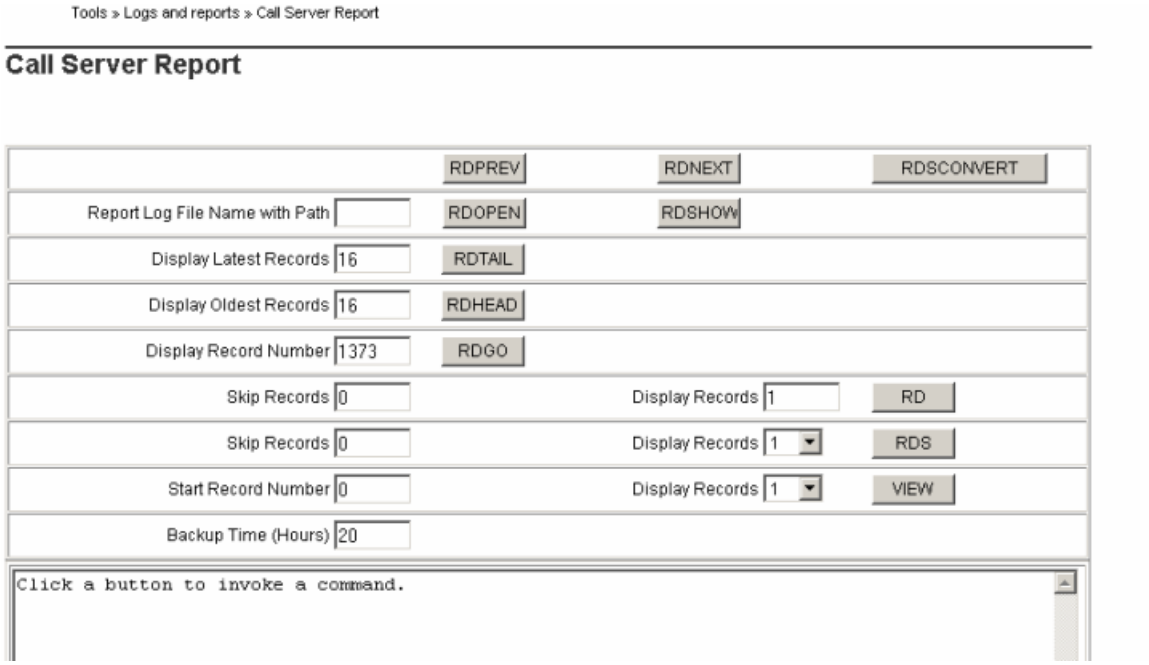


Figure 274: Call Server Report Web page

The following buttons provide one-click access to the following functions:

- RDSCONVERT — Convert a report log file to text
- RDPREV — Open the previous log file
- RDNEXT — Open the next log file
- RDOPEN — Open the latest report file
- RDSHOW — Show a summary of the report file
- RDTAIL — Show x records up to the newest record in the report file (where x is the configured display size).
- RDHEAD — Show x records starting from the oldest record in the report file (where x is the configured display size).

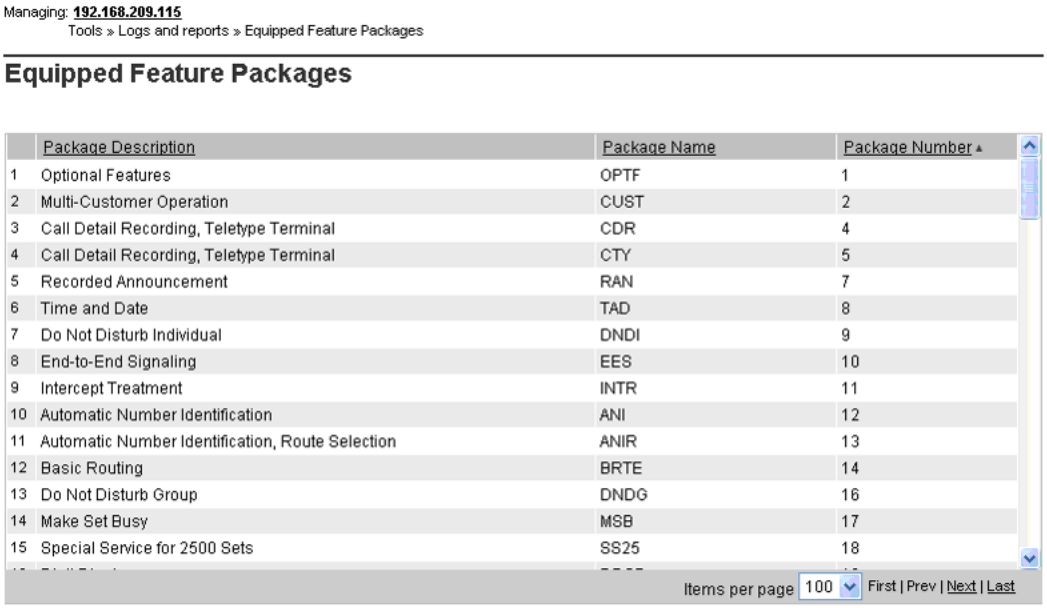
To view selected detail data on records in the report file, use the text boxes, the drop-down lists, and the following buttons:

- RDGO — Displays the record specified in the adjacent text box (where -1 is the oldest record and 1000 is the most recent).
- RD — Browses the report records. Enter the number of records to skip and the number of records to display in the adjacent text boxes.

- RDS — Browses the report records with (symbolic) memory dump. Enter the number of records to skip, and select the number of records to display using the adjacent text box and drop-down list.
- VIEW — Views selected records. Enter a starting record number and select the number of records to view using the adjacent text box and drop-down list. Negative numbers indicate records previous to the starting record.

Equipped Feature Packages

To view a list of software feature packages, click the **Logs and Reports > Equipped Feature Packages** link in the **Tools** branch of the Element Manager navigator. The Equipped Feature Packages List Web page opens as shown in Figure 275: Equipped Feature Packages List Web page on page 396.


Managing: 192.168.209.115
Tools » Logs and reports » Equipped Feature Packages

Equipped Feature Packages

	Package Description	Package Name	Package Number
1	Optional Features	OPTF	1
2	Multi-Customer Operation	CUST	2
3	Call Detail Recording, Teletype Terminal	CDR	4
4	Call Detail Recording, Teletype Terminal	CTY	5
5	Recorded Announcement	RAN	7
6	Time and Date	TAD	8
7	Do Not Disturb Individual	DNDI	9
8	End-to-End Signaling	EES	10
9	Intercept Treatment	INTR	11
10	Automatic Number Identification	ANI	12
11	Automatic Number Identification, Route Selection	ANIR	13
12	Basic Routing	BRTE	14
13	Do Not Disturb Group	DNDG	16
14	Make Set Busy	MSB	17
15	Special Service for 2500 Sets	SS25	18

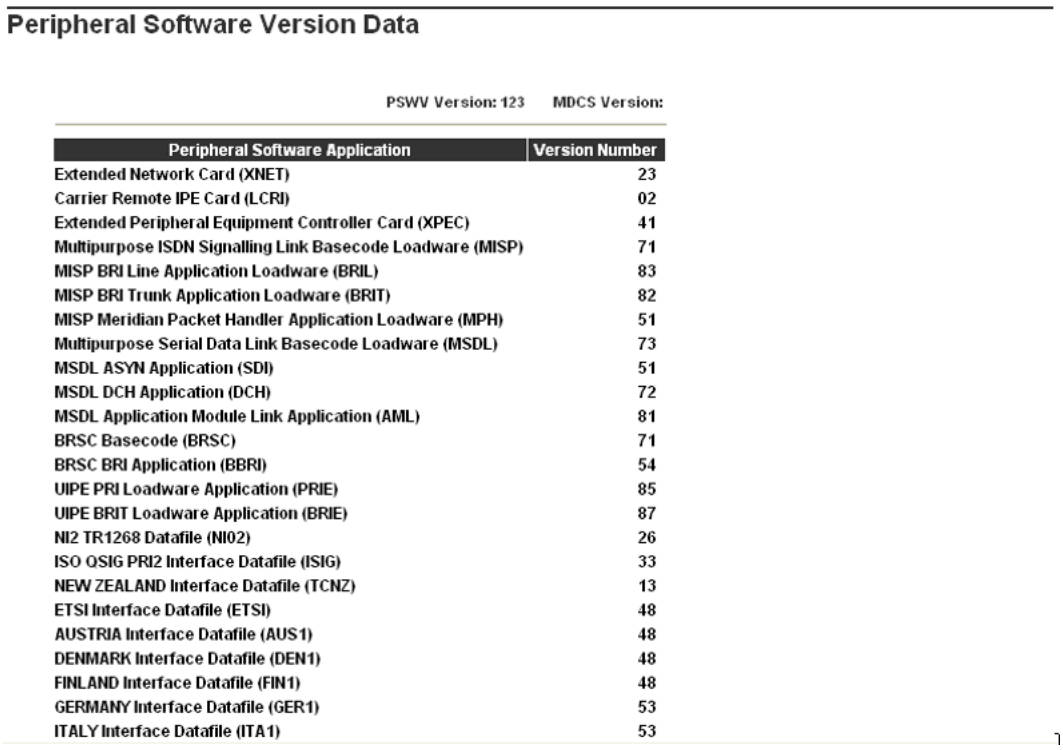
Items per page 100 First | Prev | Next | Last

Figure 275: Equipped Feature Packages List Web page

Peripheral Software Version Data

To view a list of Peripheral Software Version Data, including the loadware version of the Media gateway Controller (MGC) card, click the **Logs and Reports > Peripheral Software Version Data** link in the **Tools** branch of the Element Manager navigator. The Peripheral Software

Version Data Web page opens as shown in Figure 276: Peripheral Software Version Data Web page on page 397.



Peripheral Software Version Data

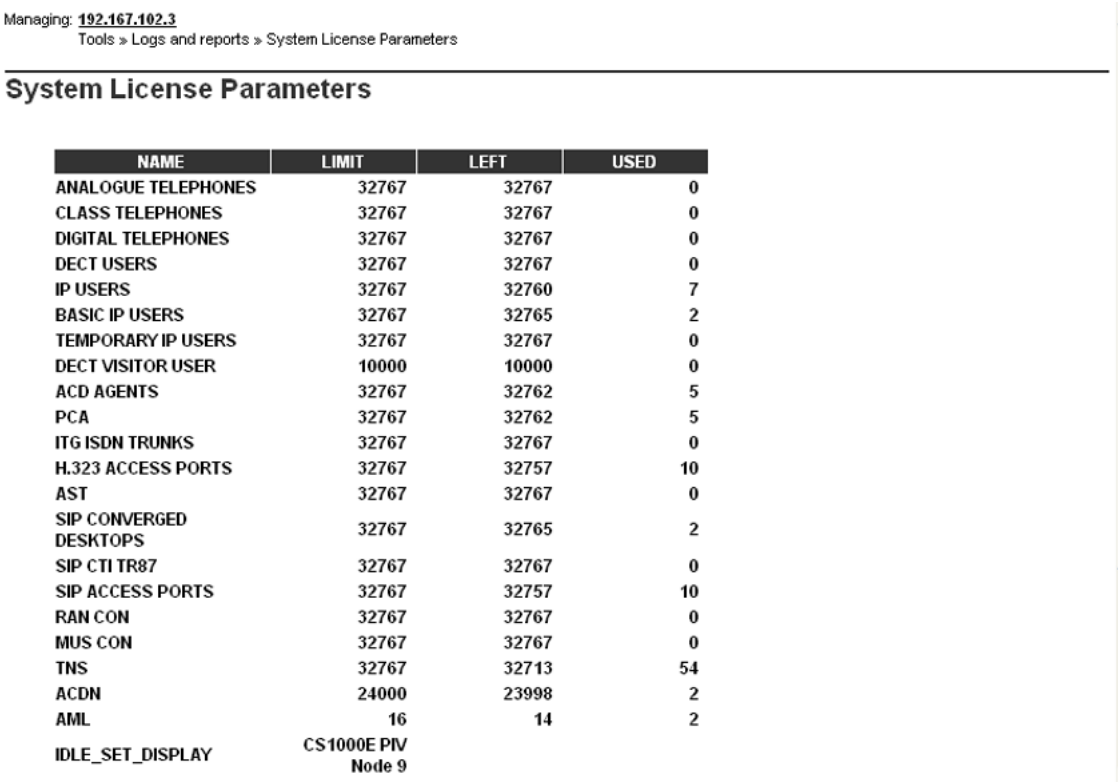
PSWV Version: 123 MDCS Version:

Peripheral Software Application	Version Number
Extended Network Card (XNET)	23
Carrier Remote IPE Card (LCRI)	02
Extended Peripheral Equipment Controller Card (XPEC)	41
Multipurpose ISDN Signalling Link Basecode Loadware (MISP)	71
MISP BRI Line Application Loadware (BRIL)	83
MISP BRI Trunk Application Loadware (BRIT)	82
MISP Meridian Packet Handler Application Loadware (MPH)	51
Multipurpose Serial Data Link Basecode Loadware (MSDL)	73
MSDL ASYN Application (SDI)	51
MSDL DCH Application (DCH)	72
MSDL Application Module Link Application (AML)	81
BRSC Basecode (BRSC)	71
BRSC BRI Application (BBRI)	54
UIPE PRI Loadware Application (PRIE)	85
UIPE BRIT Loadware Application (BRIE)	87
NI2 TR1268 Datafile (NI02)	26
ISO QSIG PRI2 Interface Datafile (ISIG)	33
NEW ZEALAND Interface Datafile (TCNZ)	13
ETSI Interface Datafile (ETSI)	48
AUSTRIA Interface Datafile (AUS1)	48
DENMARK Interface Datafile (DEN1)	48
FINLAND Interface Datafile (FIN1)	48
GERMANY Interface Datafile (GER1)	53
ITALY Interface Datafile (ITA1)	53

Figure 276: Peripheral Software Version Data Web page

System License Parameters

To view a list of System License Parameters, click the **Logs and Reports > System License Parameters** link in the **Tools** branch of the Element Manager navigator. The System License Parameters Web page opens as shown in the following figure.



Managing: 192.167.102.3
Tools » Logs and reports » System License Parameters

System License Parameters

NAME	LIMIT	LEFT	USED
ANALOGUE TELEPHONES	32767	32767	0
CLASS TELEPHONES	32767	32767	0
DIGITAL TELEPHONES	32767	32767	0
DECT USERS	32767	32767	0
IP USERS	32767	32760	7
BASIC IP USERS	32767	32765	2
TEMPORARY IP USERS	32767	32767	0
DECT VISITOR USER	10000	10000	0
ACD AGENTS	32767	32762	5
PCA	32767	32762	5
ITG ISDN TRUNKS	32767	32767	0
H.323 ACCESS PORTS	32767	32757	10
AST	32767	32767	0
SIP CONVERGED DESKTOPS	32767	32765	2
SIP CTI TR87	32767	32767	0
SIP ACCESS PORTS	32767	32757	10
RAN CON	32767	32767	0
MUS CON	32767	32767	0
TNS	32767	32713	54
ACDN	24000	23998	2
AML	16	14	2
IDLE_SET_DISPLAY	CS1000E PIV Node 9		

Figure 277: System License Parameters Web page

Operational Measurements

Element Manager provides users with regularly scheduled reports on system traffic. Perform this procedure to access reports.

Procedure steps

In the Element Manager navigator tree, open the following folders: **Tools, Logs and Reports, Operational Measurements**.

The Figure 278: Operational Measurements on page 399 web page appears.

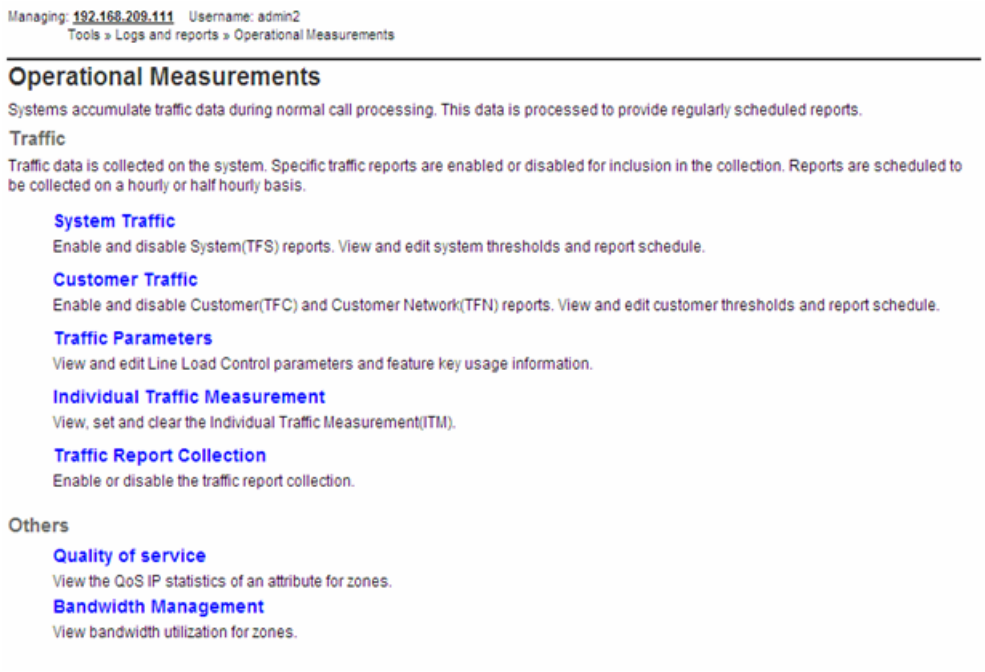


Figure 278: Operational Measurements

System Traffic

Perform this procedure to enable or disable system traffic (TFS) reports. You can also view and edit system thresholds and reports schedule.

Procedure steps

1. Click System Traffic.

   The Figure 279: System Traffic on page 400 web page appears.

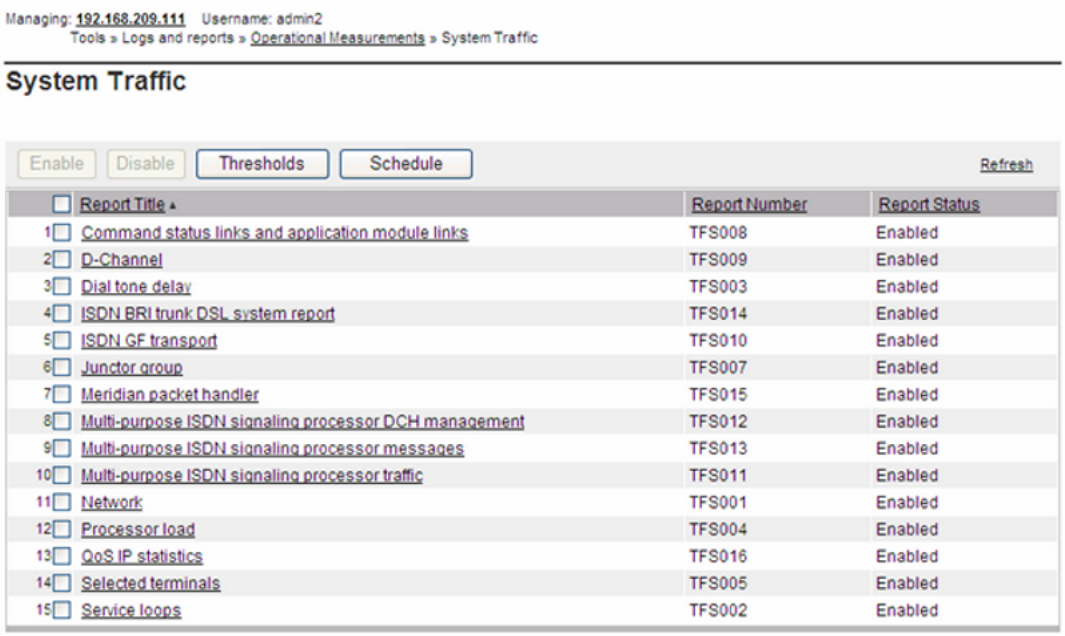


Figure 279: System Traffic

2. To view the report, click **Report Title**. The report window appears.
3. To enable a report, select a report.
4. Click **Enable**. The report is enabled.
5. To disable a report, select the report.
6. Click **Disable**. The report is disabled.
7. To configure Threshold information, click **Thresholds**. The Thresholds screen appears.
8. To configure report schedules, click **Schedules**. The Report Schedule screen appears.

   For more information about report schedules, see Call Server Traffic Collection Schedule on page 404.

Customer Traffic

Perform this procedure to enable and disable customer (TFC) and customer network (TFN) reports. You can also view and edit customer thresholds and display details of the traffic reports for each customer configured in the system.

Procedure steps

1. Click Customer Traffic.

   The Figure 280: Customer Traffic on page 401 web page appears.

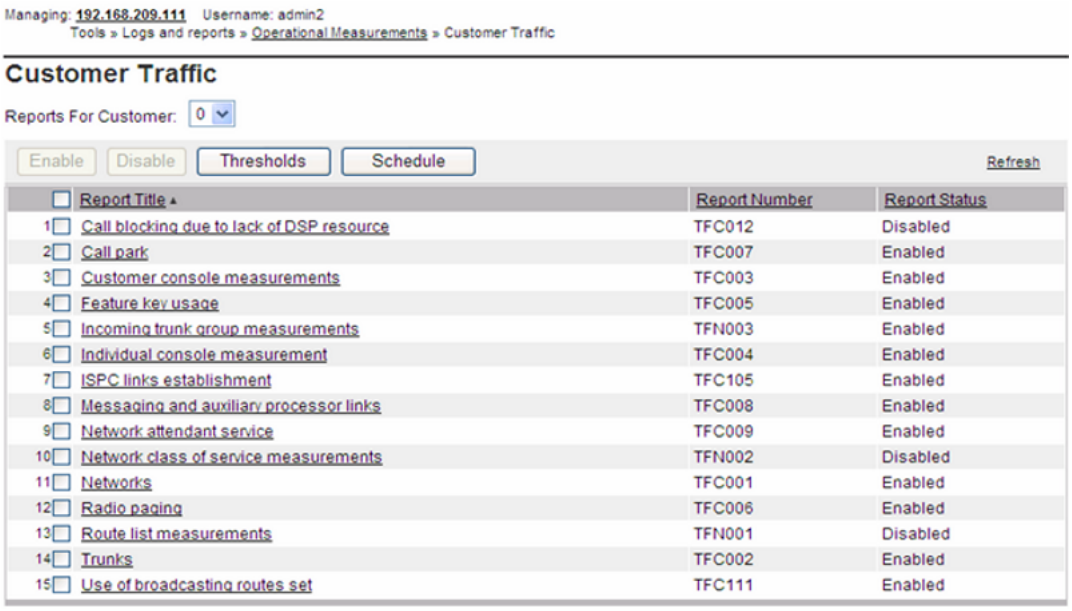


Figure 280: Customer Traffic

2. To display traffic reports for a customer, select a customer from the **Reports For Customer** list.
3. To enable a report for the selected customer, select the report.
4. Click **Enable**.
5. To disable a report for the selected customer, select the report.
6. Click **Disable**.
7. To configure threshold information for the selected customer, click Thresholds. The Thresholds screen appears.
8. To configure report schedules for the selected customer, click Schedules. The Report Schedule screen appears.

   For more information about report schedules, see Call Server Traffic Collection Schedule on page 404.

Traffic Parameters

Perform this procedure to view and edit line board control parameters and key feature usage information for a system.

Procedure steps

1. Click **Traffic Parameters**.

   The Figure 281: Edit Traffic Parameters on page 402 web page appears.

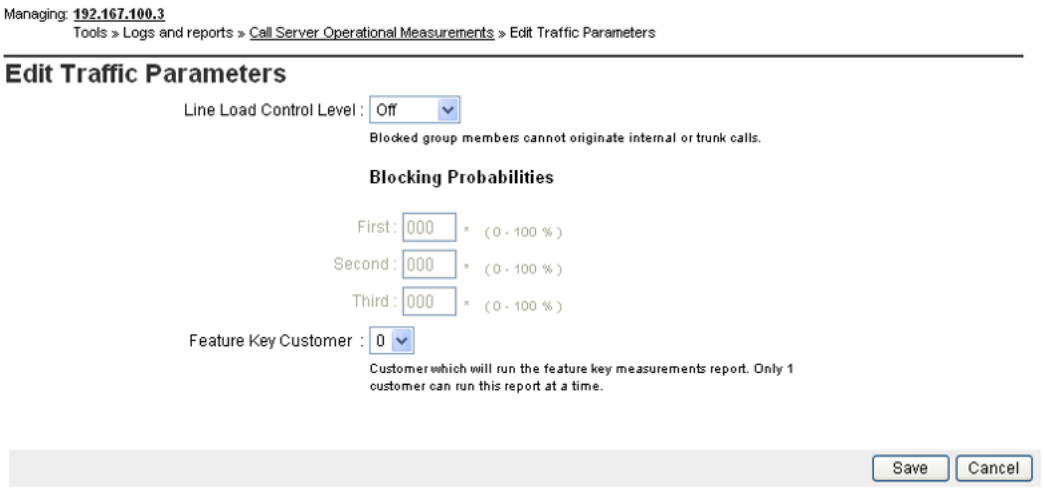


Figure 281: Edit Traffic Parameters

2. Select a **Line Load Control Level** from the list.
3. Enter the Blocking Probabilities.
4. Choose a customer from the **Feature Key Customer** list.

Important:

If the line load control level is set to off, the blocking probabilities are disabled.

5. Click **Save**.

Individual Traffic Measurement

Perform this procedure to view and edit the individual traffic measurement (ITM).

Procedure steps

1. To configure lines and trunks for Individual Traffic Measurement, click **Individual Traffic Measurement**.

   The Figure 282: Individual Traffic Measurement on page 403 web page opens.

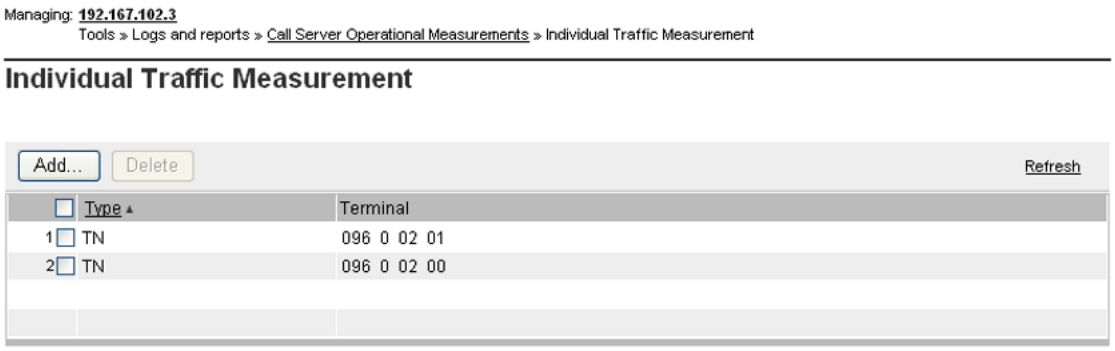


Figure 282: Individual Traffic Measurement

2. To add a terminal for individual traffic measurement, click **Add**. The Figure 283: Add TN on page 403 web page appears.

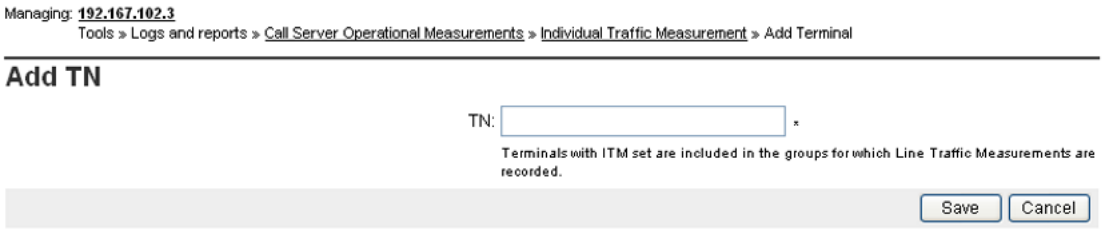


Figure 283: Add TN

3. To add TNs, type the TN in the **TN** field.

Important:

You can enter up to five TNs and must be separated by a comma.

4. Click **Save**.

Traffic Report Collection

Perform this procedure to enable or disable the traffic report collection.

Important:

By default, traffic reports are collected every 30 minutes and are stored locally. Each traffic report table in the database can hold a maximum of 3 000 records. Once this limit is reached, old data is deleted so that new reports may be added.

1. Click **Traffic Report Collection**. The Figure 284: Traffic Report Collection on page 404 web page appears.

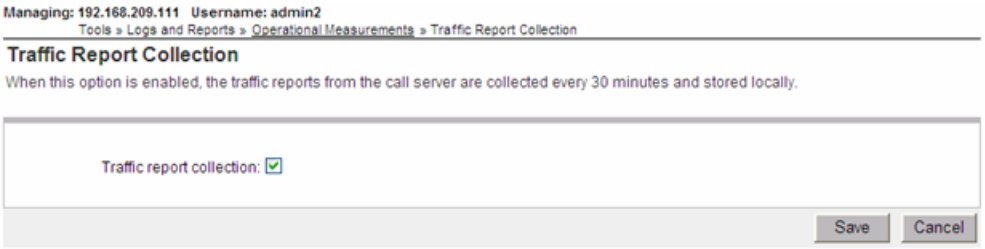


Figure 284: Traffic Report Collection

2. To enable traffic report collection, select the **Traffic Report Collection** check box. The traffic report collection is enabled.
3. To disable traffic report collection, clear the **Traffic Report Collection** check box. The traffic report collection is disabled.
4. Click Save to save the changes.

Call Server Traffic Collection Schedule

Perform this procedure to configure report schedules for a selected system or a customer.

Procedure steps

1. Click **Schedule**.

   The Figure 285: Report Schedule on page 405 web page appears.

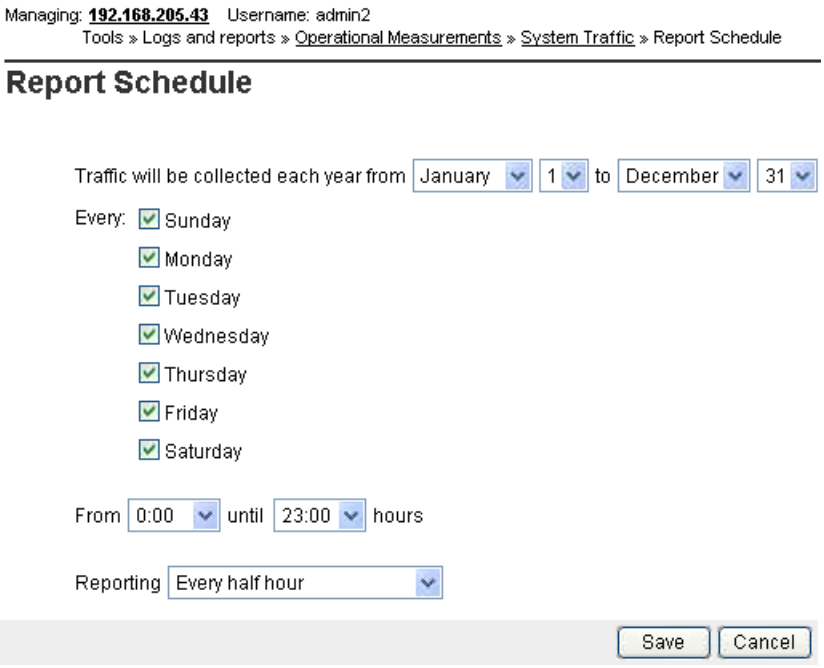


Figure 285: Report Schedule

2. Select the report collection duration in year.
3. Select the days check boxes.
4. From the **From** and **until** lists, select the hours for report collection.
5. From the **Reporting** list, select the time.
6. Click **Save**.

Viewing historic and current traffic reports for system traffic

Perform this procedure to view the historic and current traffic reports of each system or network, configured in the system.

Procedure steps

1. To view the system report, click **System** . The Figure 286: System Traffic on page 406 web page appears.

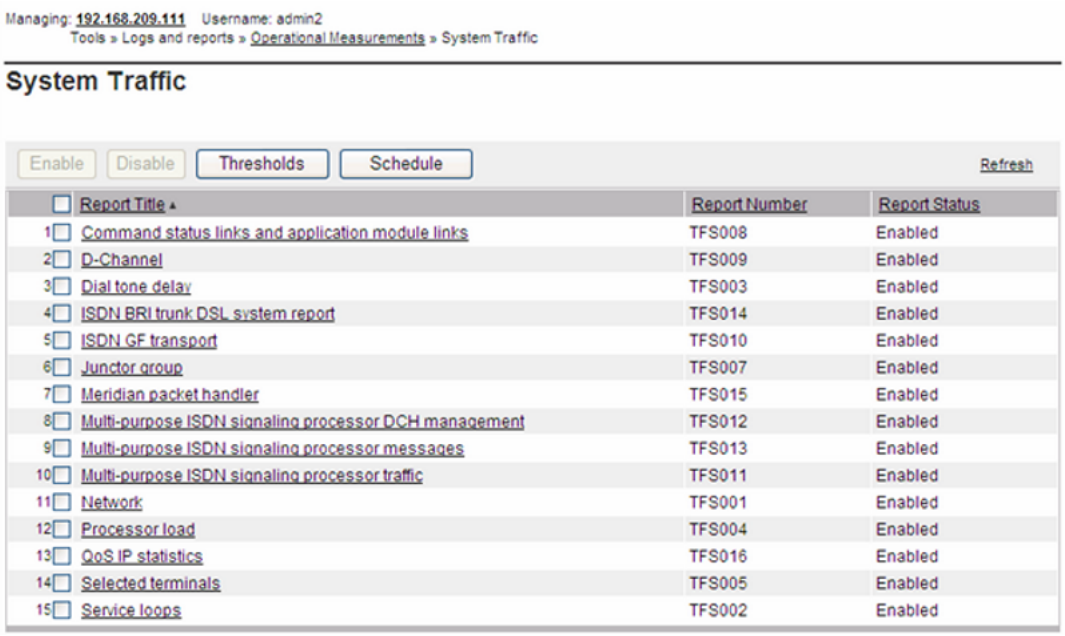


Figure 286: System Traffic

2. Click a **Report Title**. The Figure 287: System Networks Report on page 406 window appears displaying the current data with the current date and time.

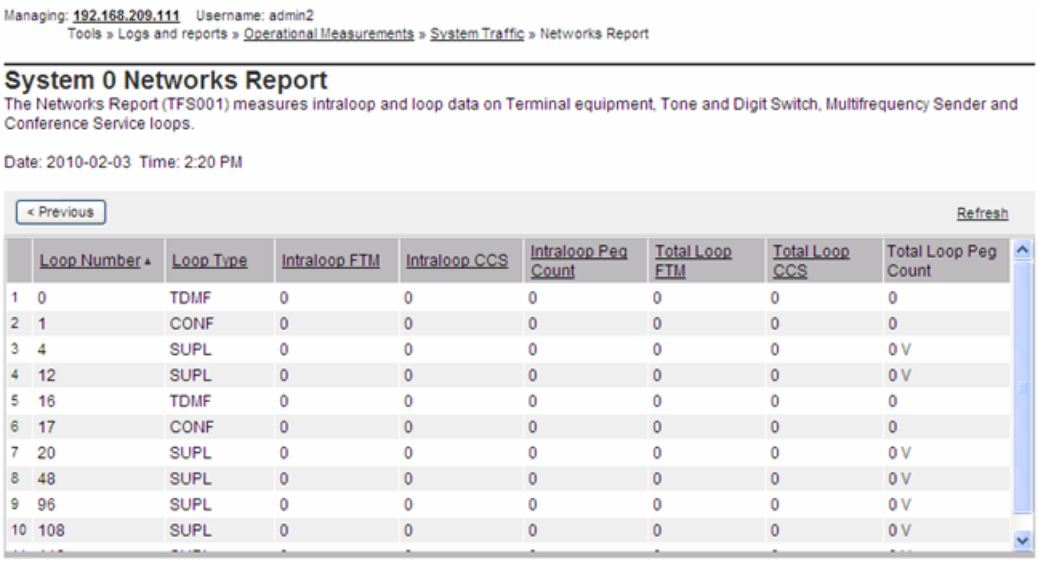
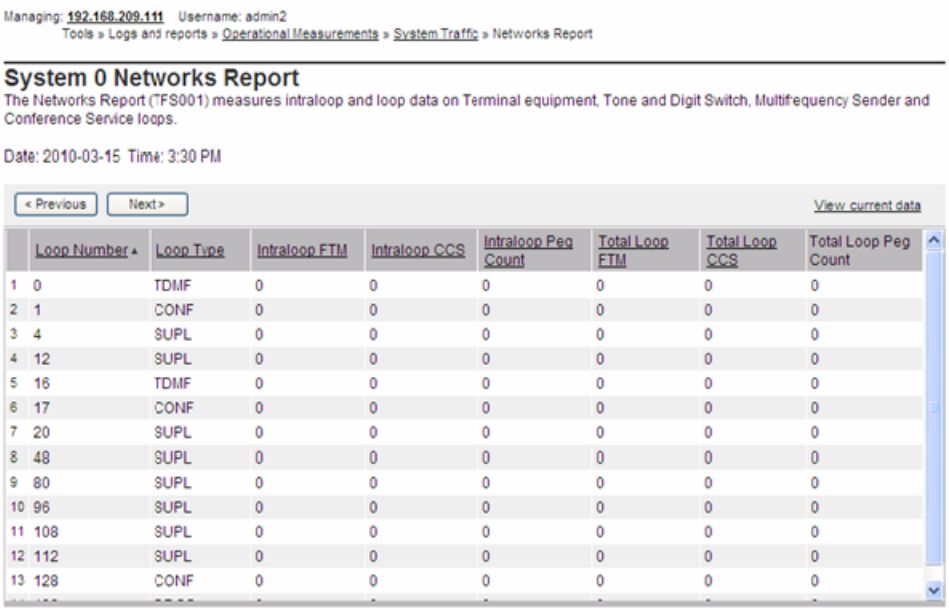


Figure 287: System Networks Report

3. Click **Previous**, to view the historic data of a particular report type.
4. Click **Next**, to traverse between the records.


Managing: 192.168.209.111 Username: admin2
Tools » Logs and reports » Operational Measurements » System Traffic » Networks Report

System 0 Networks Report

The Networks Report (TFS001) measures intraloop and loop data on Terminal equipment, Tone and Digit Switch, Multifrequency Sender and Conference Service loops.

Date: 2010-03-15 Time: 3:30 PM

< Previous | Next > | View current data

	Loop Number	Loop Type	Intraloop FTM	Intraloop CCS	Intraloop Peg Count	Total Loop FTM	Total Loop CCS	Total Loop Peg Count
1	0	TDMF	0	0	0	0	0	0
2	1	CONF	0	0	0	0	0	0
3	4	SUPL	0	0	0	0	0	0
4	12	SUPL	0	0	0	0	0	0
5	16	TDMF	0	0	0	0	0	0
6	17	CONF	0	0	0	0	0	0
7	20	SUPL	0	0	0	0	0	0
8	48	SUPL	0	0	0	0	0	0
9	80	SUPL	0	0	0	0	0	0
10	96	SUPL	0	0	0	0	0	0
11	108	SUPL	0	0	0	0	0	0
12	112	SUPL	0	0	0	0	0	0
13	128	CONF	0	0	0	0	0	0

Figure 288: System Networks Report

Important:

The date and time displays the report generated by the call server, which is stored and retrieved from the database.

5. To view the current data, click **View current data**.

Viewing historic and current traffic reports for customer traffic

Perform this procedure to view the historic and current traffic reports of a customer, configured in the system.

Procedure steps

1. To view the customer report, click **Customer Traffic**. The Figure 289: Customer Traffic on page 408 web page appears.

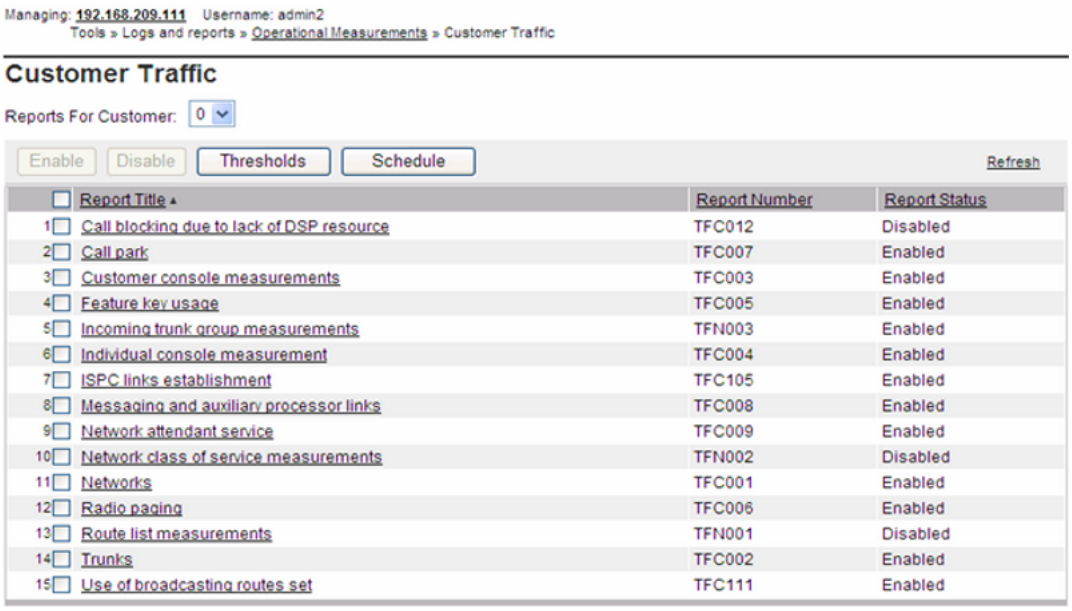


Figure 289: Customer Traffic

2. Click a **Report Title** in one of the reports. The Figure 290: System Customer Feature Key Usage Report on page 408 window appears displaying the current data with the current date and time.

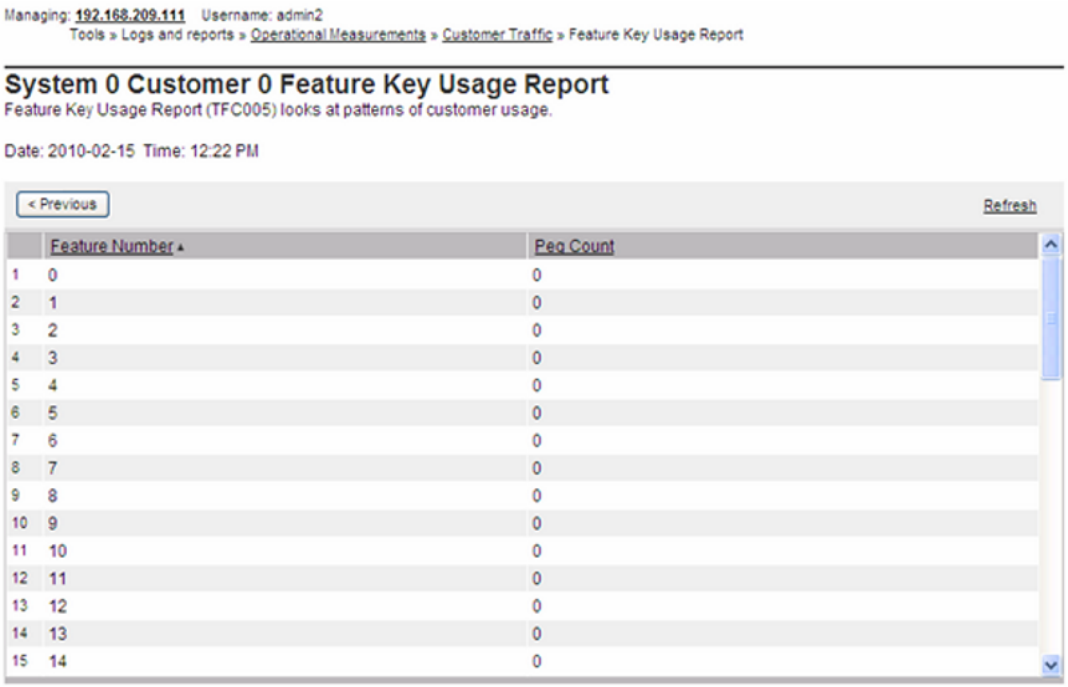


Figure 290: System Customer Feature Key Usage Report

3. Click **Previous**, to view the historic data of a particular report type.
4. Click **Next**, to traverse between the records.

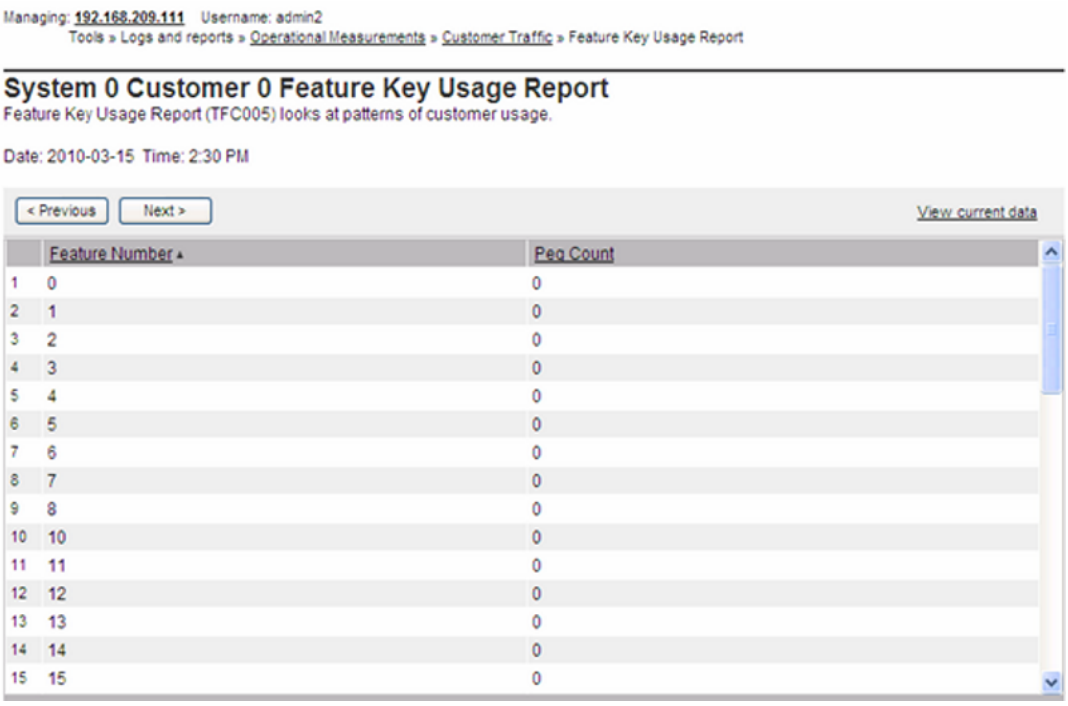


Figure 291: System Customer Feature Key Usage Report

Important:

The date and time displays the report generated by the call server, which is stored and retrieved from the database.

5. To view the current data, click **View current data**.

Quality of Service

Perform this procedure to view the QoS IP statistics of an attribute for a zone.

Procedure steps

To view the Ethernet Quality of Service Diagnostics web page, click **Quality of service**. For more information, see Ethernet Quality of Service Diagnostics on page 83.

Bandwidth Management

Perform this procedure to view bandwidth utilization for zones.

Procedure steps

To open the Maintenance Commands for Zones web page, click Bandwidth Management. For more information, see Zone Diagnostics on page 106.

Chapter 13: Security

The following links are provided under the Security branch of Element Manager:

- Passwords
  - System Passwords
  - Customer Passwords
- Policies
  - Media
  - System Keys
  - File Transfer
  - Port Access Restrictions
- Login Options
  - Shell Login
  - Access Warning

All information about the Security features available in Element Manager is covered and maintained in *Avaya Security Management Fundamentals, NN43001-604*.

Chapter 14: Certificate Management

Contents

This chapter contains information about the following topics:

Overview

When accessing Element Manager Certificate Management is provided by the Unified Communication Management (UCM) Common Services. For more information, see *Avaya Unified Communications Management Common Services Fundamentals, NN43001-116* .

This section contains information about the Element Manager SSL/TLS Service Management Wizard, which guides users through the certificate management and Transportation Layer Security (TLS) configuration process.

Creating a new certificate request

When Element Manager is first deployed, no certificate is installed. The TLS service for the Element Manager is disabled.

Follow the steps in Creating a new certificate request on page 414 to create a new certificate request.

Creating a new certificate request

1. Log in using the non-secure mode.
2. Click **Configure**.

   The Server Certificate Web page appears.
3. Select the **Create a new certificate request to be signed by Certificate Authority** radio button and click **Next**.

   The Name and Security Settings Web page appears.
4. Enter a **Friendly Name** for the certificate.
5. Select a bit length from the **Bit length** list.
6. Click **Next**.

   The Organization Information Web page appears.
7. Enter an **Organization** and **Organization Unit** and click **Next**.

   The Your Server's Common Name Web page appears
8. Enter a **Common Name** and click **Next**.

   The Geographical Information Web page appears.
9. Enter a **Country/Region**.
10. Enter a **State/Province**.
11. Enter a **City/Locality**.
12. Click **Next**.

    The Certificate Request Summary Web page appears.
13. Click **Commit** to download the certificate request to a local file.

    The X.509 Certificate Request Web page appears.
14. Click **Close** to close the wizard.

Processing a pending certificate response

The certificate request file is submitted to a Certificate Authority. The Certificate Authority sends a response in a text file.

Follow the steps in Processing a pending certificate response on page 415 to process the pending certificate response file.

Processing a pending certificate response

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Web page appears.
2. Select the **Process the pending request and install the certificate** option button and click **Next**.

   The Process a Pending Request Web page appears.
3. Copy the contents of the text file received from the certificate authority.
4. Click **Commit**.

   The Certificate Summary Web page appears.
5. Click **Finish**.

To verify that the Certificate Authority is trusted by Internet Explorer, choose **Tools > Internet Options > Content > Certificates**. The Trusted Certificate Authority List Web page appears.

If the Certificate Authority is not in the trusted Certificate Authority list of Internet Explorer, a Security Alert Web page appears when accessing Element Manager using SSL or TLS.

The user must then log in using the secure mode.

Deleting a pending certificate request

Follow the steps in Deleting a pending certificate request on page 415 to delete a pending certificate request.

Deleting a pending certificate request

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Web page appears.
2. Select the **Delete the pending request** option button and click **Next**.

The Delete a Pending Request Web page appears.

3. Click **Finish**.

Creating a self-signed certificate

Follow the steps in Creating a self-signed certificate on page 416 to create a self-signed certificate.

Creating a self-signed certificate

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Web page appears.
2. Select the **Create a new self-signed certificate** option button and click **Next**.

   The New Self-Signed Certificate Web page appears.
3. Click **Next**.

   The Name and Security Settings Web page appears.
4. Enter a **Friendly Name** for the certificate.
5. Select a bit length from the **Bit length** list.
6. Click **Next**.

   The Organization Information Web page appears.
7. Enter an **Organization** and **Organization Unit** and click **Next**.

   The Your Server's Common Name Web page appears.
8. Enter a **Common Name** and click **Next**.

   The Geographical Information Web page appears.
9. Enter a **Country/Region**.
10. Enter a **State/Province**.
11. Enter a **City/Locality**.
12. Click **Next**.

    The Certificate Request Summary Web page appears.
13. Click **Commit**.

    The **X.509 Certificate Request** Web page appears.
14. Click **Close** to close the wizard.

    If the Security Alert Web page appears, click **Yes**.

Note:

The user can also export the self-signed certificate and distribute it into the trusted Certificate Authority list of Internet Explorer.

Assigning an existing certificate

To assign an existing certificate to the Element Manager's Web site, follow the steps in Assigning an existing certificate on page 417.

Assigning an existing certificate

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Web page appears.
2. Select the **Assign an existing certificate** option button and click **Next**.

   The Available Certificate Web page appears.
3. Select a certificate from the list of available certificates and click **Next**.

   The Certificate Summary Web page appears.
4. Click **Finish**.

Importing a certificate and its private key

Follow the steps in Importing a certificate and its private key on page 417 to import a certificate and its private key.

Importing a certificate and its private key

1. On the **SSL/TLS Service Configuration** Web page, click **Configure**.

   The Server Certificate Web page appears.
2. Select the **Import a certificate and its private key from a PEM encoded file** option button and click **Next**.

   The Import Certificate Password Web page appears.
3. Enter the password of the certificate file and click **Commit**.

   The Import Certificate Web page appears.
4. Copy the contents of the text file received from the certificate authority.
5. Click **Commit**.

The Certificate Summary Web page appears.

6. Click **Finish**.

Creating a certificate renew request for the current certificate

The X.509 certificate has an expiration date. A warning message is shown if the expiration date is less than one month away. To create a certificate renewal request, follow the steps in Creating a certificate renew request on page 418.

Creating a certificate renew request

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Web page appears.

2. Select the **Create a certificate renew request** option button and click **Next**.

   The Certificate Request Summary Web page appears.

3. Click **Commit** to download the certificate request to a local file.

   The X.509 Certificate Request Web page appears.

4. Click **Close** to close the wizard.

Removing the current certificate

To remove a current certificate, follow the steps in Removing the current certificate on page 418.

Removing the current certificate

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Web page appears.

2. Select the **Remove the current certificate** option button and click **Next**.

   The Remove a Certificate Web page appears.

3. Click **Finish**.

Note:

All client sessions must be terminated before the removing operation can take effect.

Replacing the current certificate

To replace the current certificate, follow the steps in Replacing the current certificate on page 419.

Note:

The security context of the Web SSL service will change to the new certificate when there is no active HTTPS connection.

Replacing the current certificate

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Configuration Wizard Web page appears.
2. Select the **Replace the current certificate** option button and click **Next**.

   The Available Certificate Web page appears.
3. Select a certificate from the list and click **Next**.

   The Certificate Summary Web page appears.
4. Click **Close** to close the wizard.

Exporting the current self-signed certificate

When the current certificate is self-signed, it can be exported. Using SSL and TLS protocol, the certificate file can be used to set up a trust relationship between different parties.

To export the current self-signed certificate, follow the steps in Exporting the current self-signed certificate on page 419.

Exporting the current self-signed certificate

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Configuration Wizard Web page appears.
2. Select the **Export the current self-signed certificate** option button and click **Next**.

   The Export Self-signed Certificate Summary Web page appears.
3. Click **Download**.

   The Certificate Content Web page appears. Copy the contents of the text box and save it as a plain text file. When exporting the self-signed certificate, name the file

with extension .cer. The file can then be installed in the trusted certificate list of the client.

4. Click **Close** to close the wizard.

Exporting the current certificate and its private key

The current certificate and its private key can be exported. A password is required to encrypt the file. Use the same password that was used to import the file.

Follow the steps in Exporting the current certificate on page 420 to export the current certificate and its private key.

Exporting the current certificate

1. On the SSL/TLS Service Configuration Web page, click **Configure**.

   The Server Certificate Configuration Wizard Web page appears.

2. Select the **Export the current certificate and its private key** option button and click **Next**.

   The Export Certificate Password Web page appears.

3. Enter the password and click **Next**.

   The Export Current Certificate and Private Key Summary Web page appears.

4. Click **Download**.

   The Certificate Content Web page appears. When exporting the certificate and private key, import the file to another server.

5. Click **Close** to close the wizard.

SSL/TSL security configuration

When a certificate is installed on Element Manager, the SSL/TLS usage rule is set to "Always" by default.

If "Always" is selected, all user traffic must use SSL/TLS. If "UserChoice" is selected, users can choose between secure and non-secure sessions when they log in.

The user can configure the TCP port used by the SSL and TLS service by entering a value in the **SSL/TLS** field. The default value is 443.

Chapter 15: Support

Contents

This chapter contains information about the following topics:

Introduction

The following Support features can be accessed through Element Manager:

- Help
- Release Notes

Help

Element Manager provides context-sensitive online Help. To access Help, click the **Help** link located in the top right corner of the Element Manager Web pages. The Help Web page shown in Figure 292: Help Web page on page 422 appears.

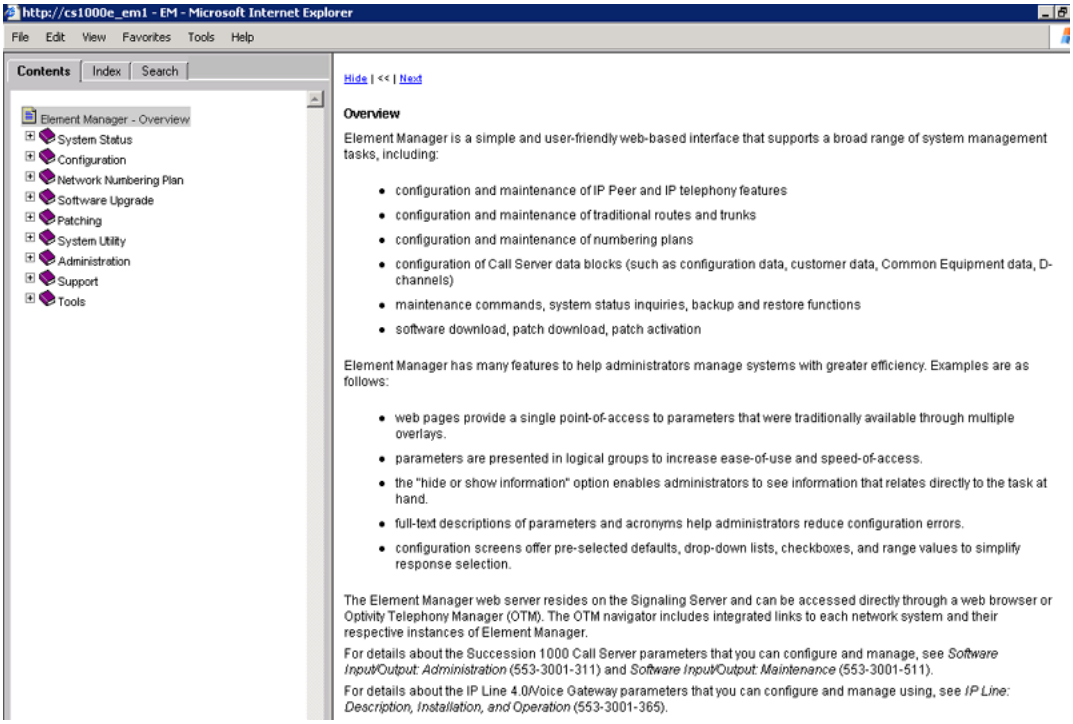


Figure 292: Help Web page

Release Notes

A Release Note can describe a design change or a product feature that was discovered after market release. Often, a Release Note describes how to work around a product limitation. Click the **Release Notes** link to access the Web-based Helmsman Express application.

Chapter 16: Appendix A

⚠ Warning:

Do not contact Red Hat for technical support on your Avaya version of the Linux base operating system. If technical support is required for the Avaya version of the Linux base operating system, contact Avaya technical support through your regular channels

This section governs the use of the Red Hat Software and any updates to the Red Hat Software, regardless of the delivery mechanism and is governed by the laws of the state of New York in the U.S.A. The Red Hat Software is a collective work under U.S. Copyright Law. Subject to the following terms, Red Hat, Inc. (“Red Hat”) grants to the user (“Customer”) a license to this collective work pursuant to the GNU General Public License. Red Hat Enterprise Linux (the “Red Hat Software”) is a modular operating system consisting of hundreds of software components. The end user license agreement for each component is located in the component's source code. With the exception of certain image files identified below, the license terms for the components permit Customer to copy, modify, and redistribute the component, in both source code and binary code forms. This agreement does not limit Customer's rights under, or grant Customer rights that supersede, the license terms of any particular component. The Red Hat Software and each of its components, including the source code, documentation, appearance, structure and organization are owned by Red Hat and others and are protected under copyright and other laws. Title to the Red Hat Software and any component, or to any copy, modification, or merged portion shall remain with the aforementioned, subject to the applicable license. The “Red Hat” trademark and the “Shadowman” logo are registered trademarks of Red Hat in the U.S. and other countries. This agreement does not permit Customer to distribute the Red Hat Software using Red Hat's trademarks. If Customer makes a commercial redistribution of the Red Hat Software, unless a separate agreement with Red Hat is executed or other permission granted, then Customer must modify any files identified as “REDHAT-LOGOS” and “anaconda-images” to remove all images containing the “Red Hat” trademark or the “Shadowman” logo. As required by U.S. law, Customer represents and warrants that it: (a) understands that the Software is subject to export controls under the U.S. Commerce Department’s Export Administration Regulations (“EAR”); (b) is not located in a prohibited destination country under the EAR or U.S. sanctions regulations (currently Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria); (c) will not export, re-export, or transfer the Software to any prohibited destination, entity, or individual without the necessary export license(s) or authorizations(s) from the U.S. Government; (d) will not use or transfer the Red Hat Software for use in any sensitive nuclear, chemical or biological weapons, or missile technology end-uses unless authorized by the U.S. Government by regulation or specific license; (e) understands and agrees that if it is in the United States and exports or transfers the Software to eligible end users, it will, as required by EAR Section 740.17(e), submit semi-annual reports to the Commerce Department’s Bureau of Industry & Security (BIS), which include the name and address (including country) of each transferee; and (f) understands that countries other than the United States may restrict the import, use, or export of encryption products and that it shall be solely responsible for compliance with any such import, use, or export restrictions. Red Hat may distribute third party software programs with the Red Hat Software that are not part of the Red Hat Software. These third party programs are subject to their own license terms. The license terms either accompany the programs or can be viewed at http://www.redhat.com/licenses/. If Customer does not agree to abide by the applicable license terms for such programs, then Customer may not install them. If Customer wishes to install the programs on more than one system or transfer the programs to another party, then Customer must contact the licensor of the programs. If any provision of this agreement is held

to be unenforceable, that shall not affect the enforceability of the remaining provisions.

Chapter 17: Appendix B

Configuring the IPMG in Element Manager

The following procedure describes how to configure the IPMG in Element Manager.

Configuring the IPMG (Element Manager)

1. In Element Manager, select **IP Network > Media Gateways**.
2. On the Add IPMG page, configure the appropriate Superloop Number and Shelf, and then click **Add**.

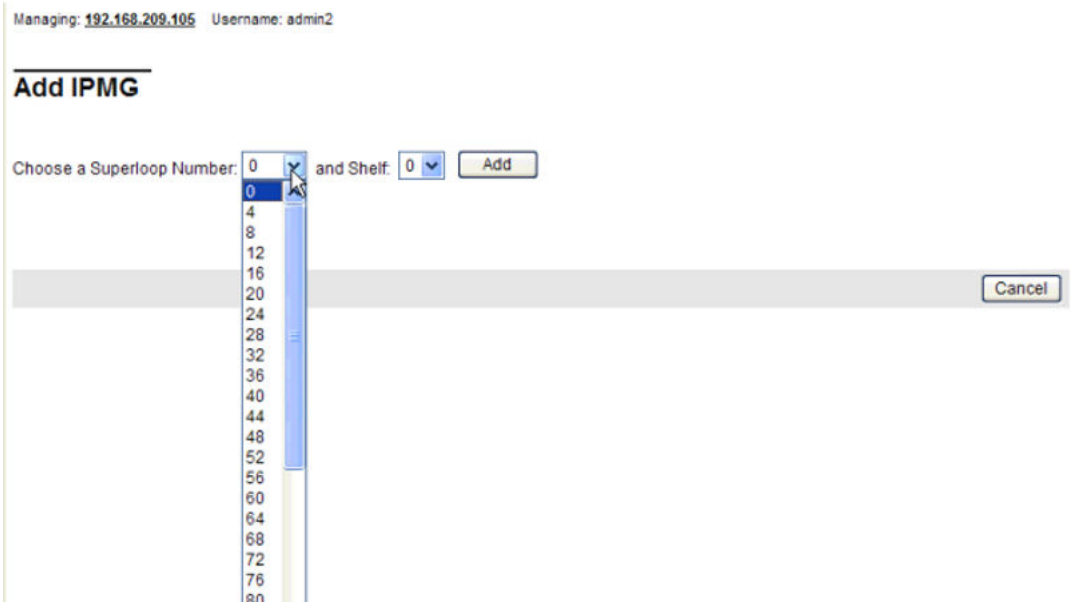


Figure 293: Add IPMG

3. Configure the IP address, zone number, and the Media Gateway type (in this case, a Media Gateway Controller), and then click **Save**.

   You can select MGC to automatically fill in the remaining fields.

   Note:

   The IP address that you configure here is the same IP address as the one configured on the MGC in an earlier procedure.

   The IPMG Media Gateway Controller (MGC) Configuration Web page appears.

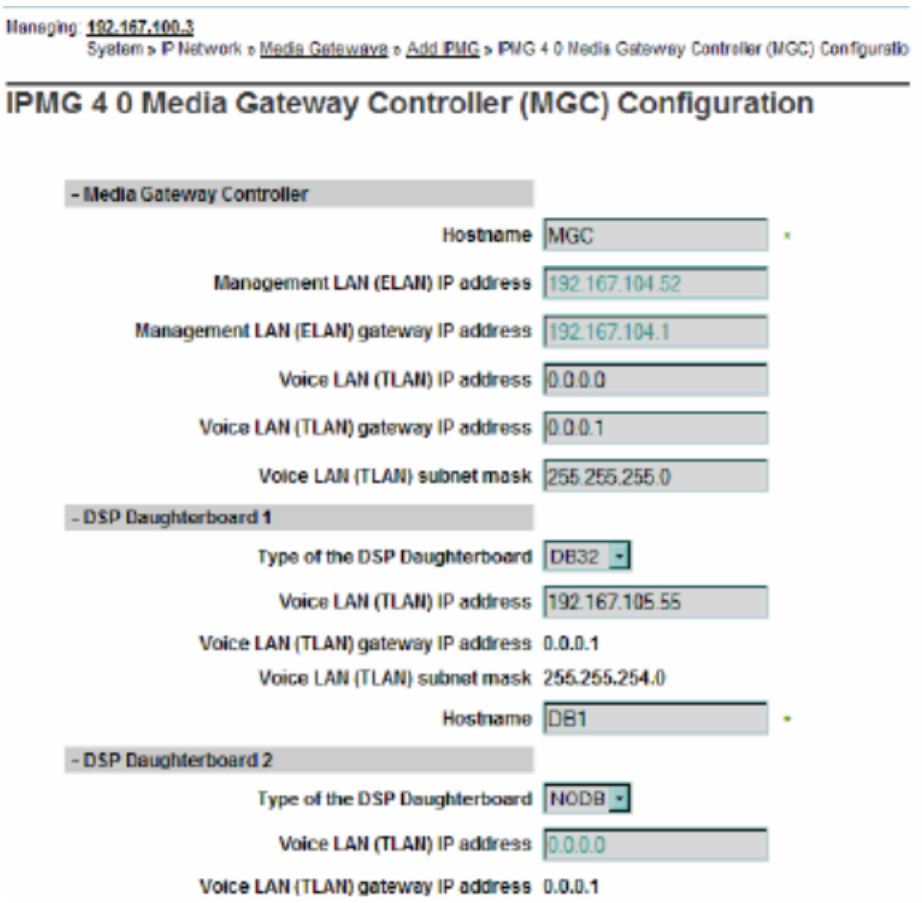


Figure 294: IPMG Media Gateway Controller (MGC) Configuration Web page

4. Configure the Gateway IP addresses and Voice LAN IP addresses. If the MGC has DSP daughterboards connected, select the type and enter the IP addresses.

   After the configuration is complete the following figure appears.

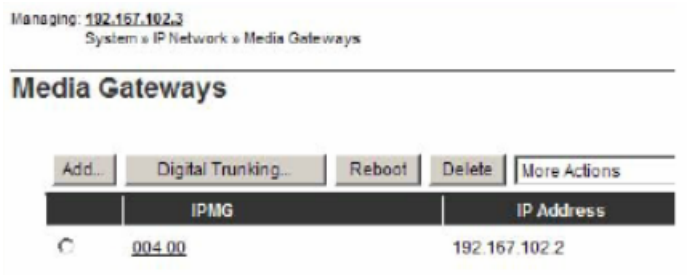


Figure 295: Media Gateways

   The Media Gateways screen lists the superloop and shelf numbers, IP address, zone, and type of the recently configured MGC.

5. Click the radio-button next to the superloop, and then from the list, select **Add VGW channels**.

The Add VGW channels Web page appears as shown below.

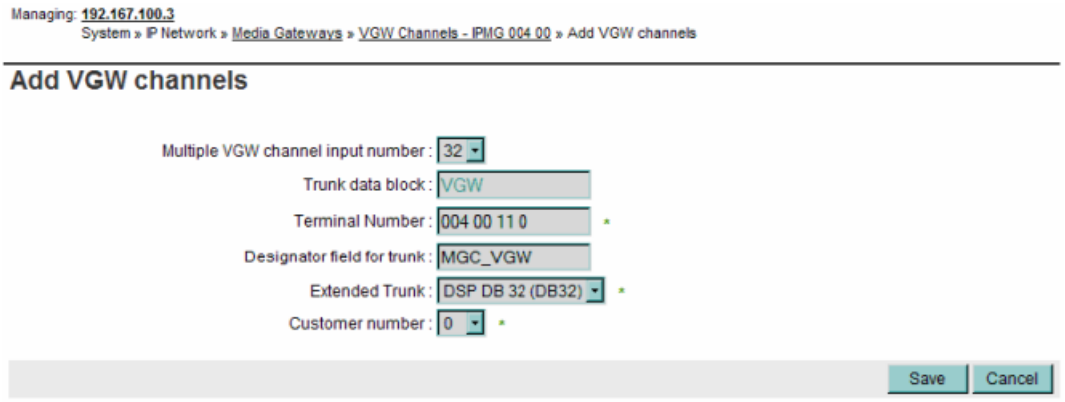


Figure 296: Add VGW channels Web page

6. On this page, configure the number of required channels, the Terminal Number (the superloop and shelf numbers of the MGC, the card number, and the unit). Provide a name and the daughterboard and customer type. Click **Save**.

   The VGW Channels IPMG Web page appears. The MGC is added to the list.

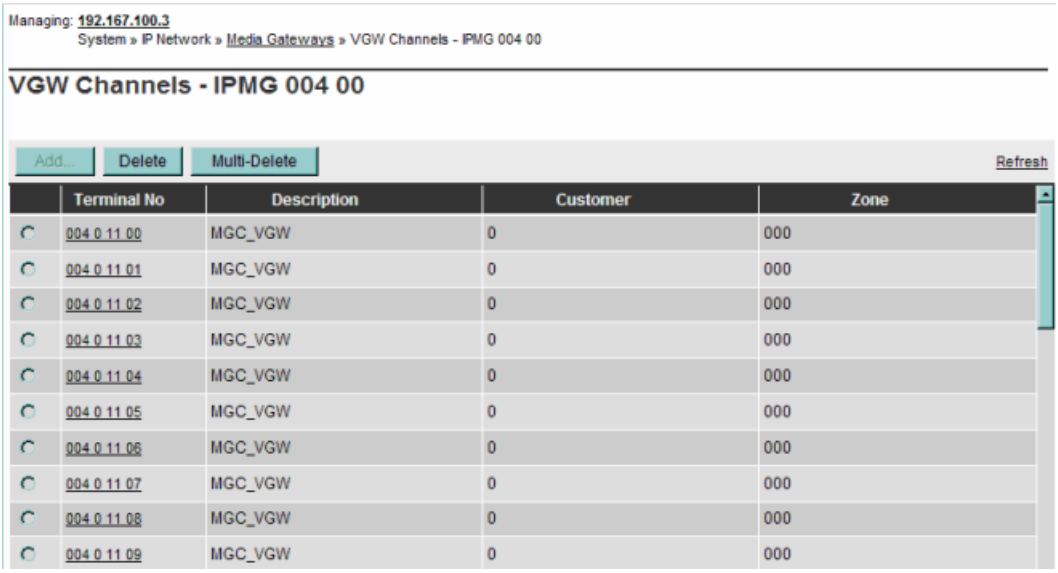


Figure 297: VGW Channels IPMG Web page

Configuring conference TDS

To configure conference TDS for IPMG using Element Manager, complete the following procedure.

Configuring conference TDS

1. In the Element Manager screen, select **IP Network > Media Gateways**.

   The Media Gateway Web page appears, as shown in the following figure.

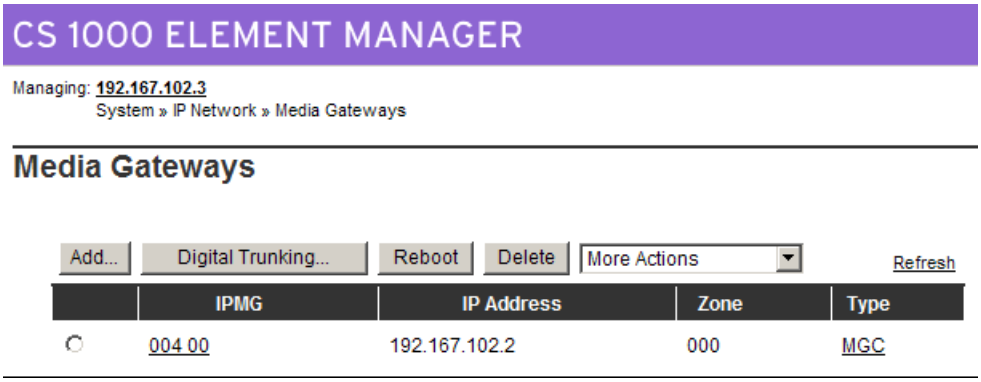


Figure 298: Media Gateways Web page

2. On the Media Gateway Web page, select the IPMG superloop and then click **Digital Trunking**.

   The Digital Trunking Web page appears, as shown in the following figure.

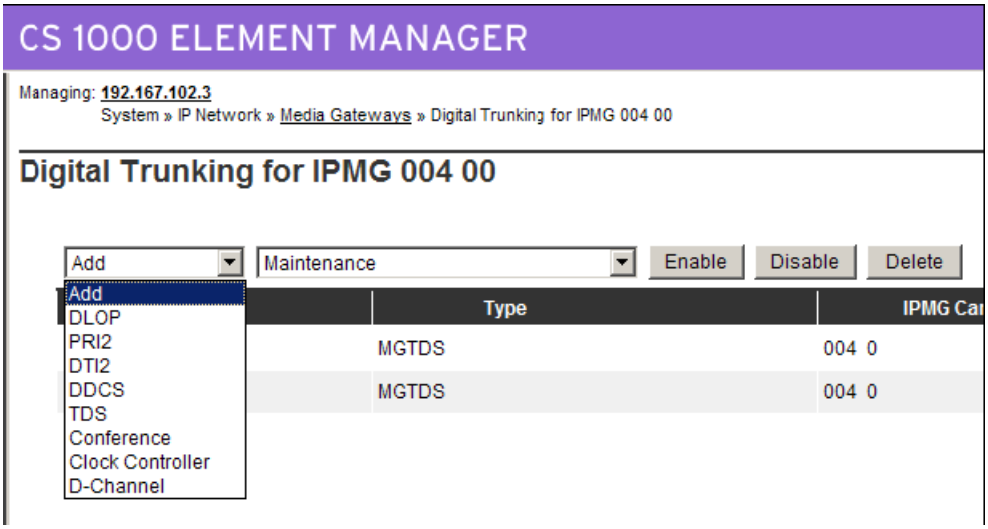


Figure 299: Digital Trunking for IPMG Web page

3. From the first menu, select TDS to add a TDS loop.

   The IPMG TDS Web page appears as shown in the following figure.

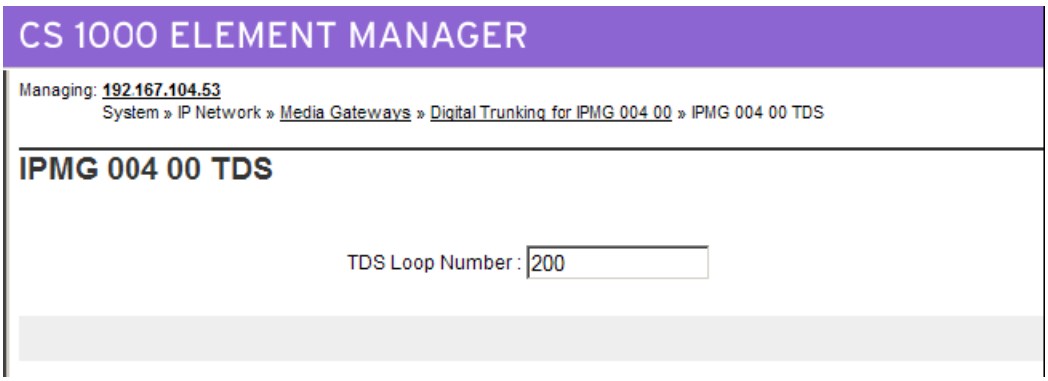


Figure 300: IPMG TDS Web page

4. Type the TDS loop number (0 — 255).
5. Click **Save**.

   The TDS loop is not available until after you type a loop number and press TAB to move the cursor.
6. On the confirmation box, click **OK** to complete the configuration.

   The updated loop configuration page appears and the new Conference loop appears.

Configuring DSP Daughterboard Voice gateway channels

If the MGC has DSP daughterboards connected, select the type daughterboard and configure the IP addresses on the IPMG Media Gateway Controller (MGC) Configuration Web page.

Chapter 18: Appendix C

Avaya 1110 IP Deskphone

The following figure shows the Avaya 1110 IP Deskphone layout.

Figure 301: Avaya 1110 IP Deskphone layout

Avaya 1110 IP Deskphone Display Areas

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed.

That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

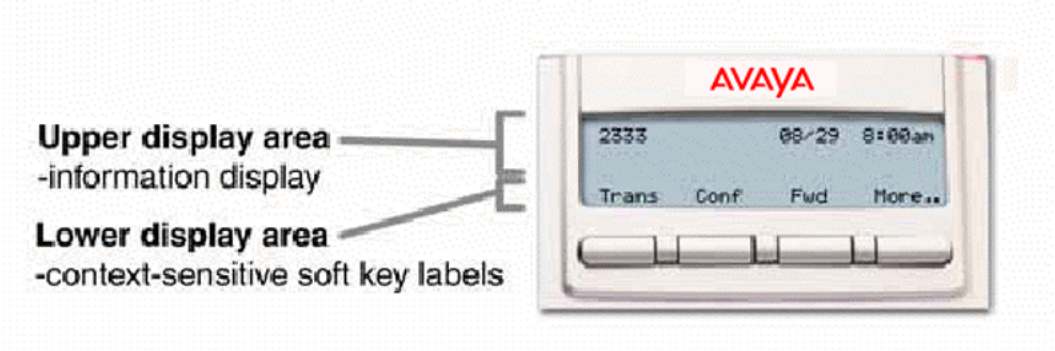


Figure 302: Avaya 1110 IP Deskphone Display Areas

Avaya 1110 IP Deskphone with Soft Keys 17-19

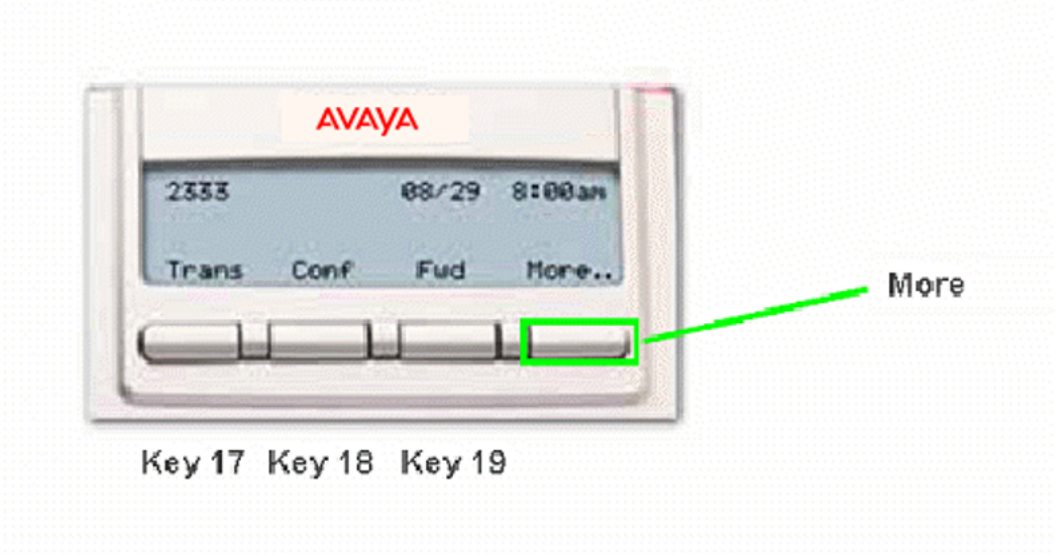


Figure 303: Avaya 1110 IP Deskphone with Soft Keys 17-19

Press the More key to access Soft Keys 20-22.

Avaya 1110 IP Deskphone with Soft Keys 20-22

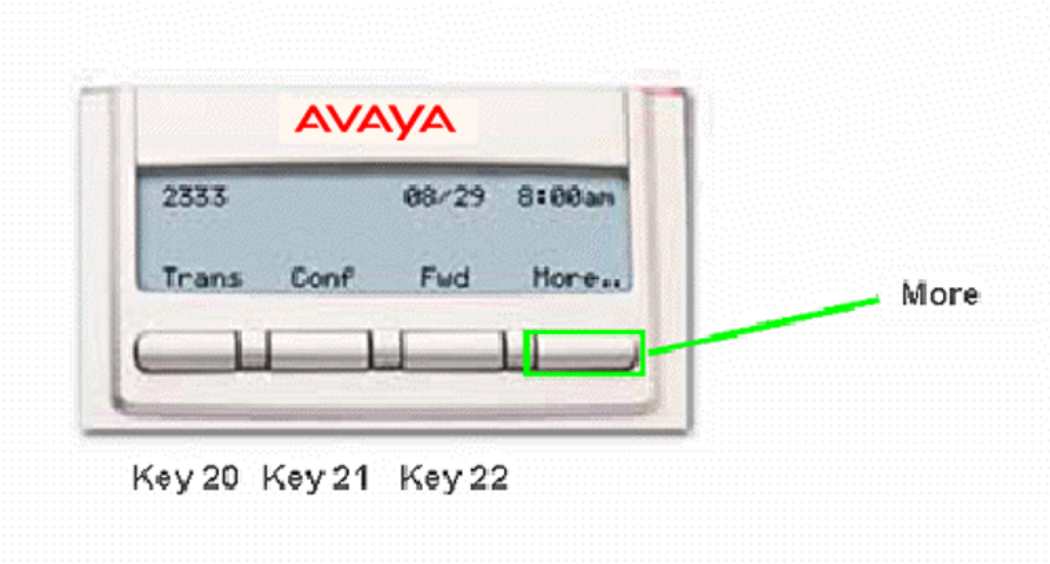


Figure 304: Avaya 1110 IP Deskphone with Soft Keys 20-22

Press the More key to access the Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

Avaya 1110 IP Deskphone Default Key Values

Table 5: Default Key Values

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)

Key No	Value
26	Calling Party Number (CPN)

Avaya 1120E IP Deskphone

The following figure shows the Avaya 1120E IP Deskphone layout.

Figure 305: Avaya 1120E IP Deskphone Layout

Avaya 1120E IP Deskphone Display Areas

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

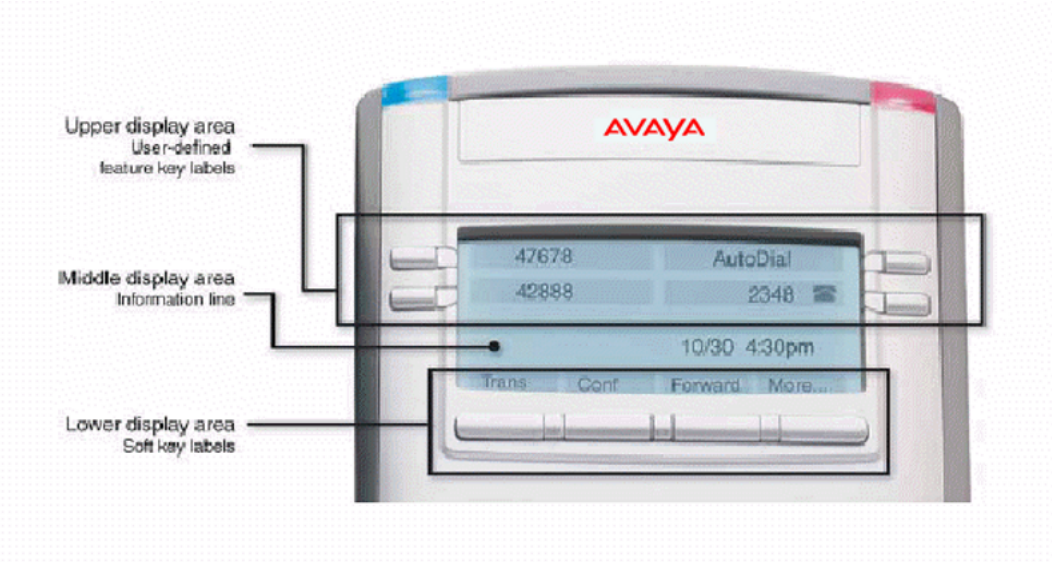


Figure 306: Avaya 1120E IP Deskphone Display Areas

Avaya 1120E IP Deskphone with Feature Keys 0-3 and Soft Keys 17-19

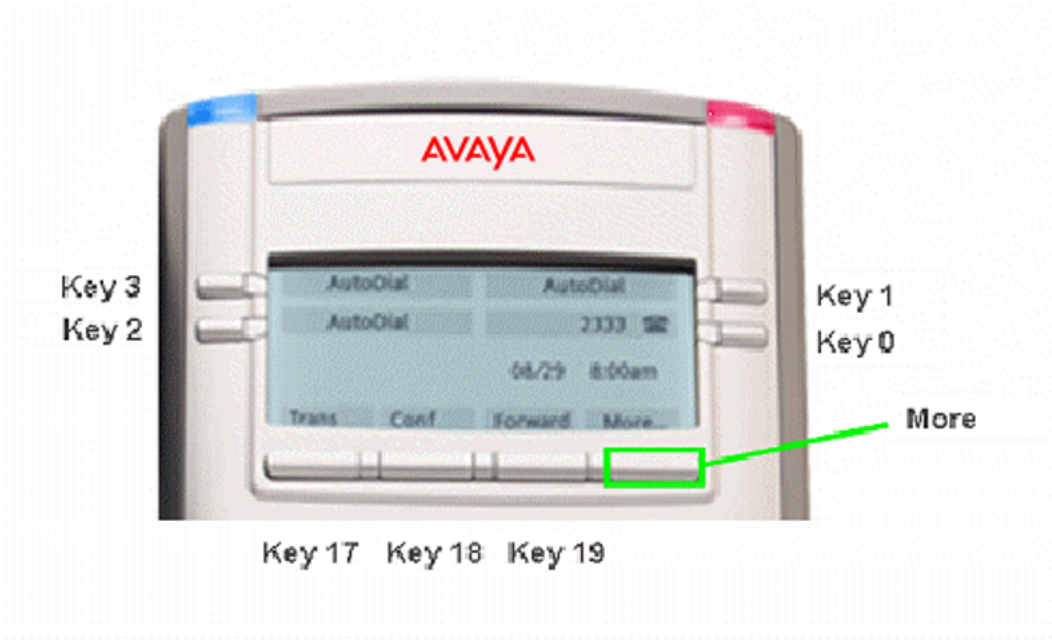


Figure 307: Avaya 1120E IP Deskphone with Soft Keys 17-19

Press the More key to access Soft Keys 20-22.

Avaya 1120E IP Deskphone with Soft Keys 20-22

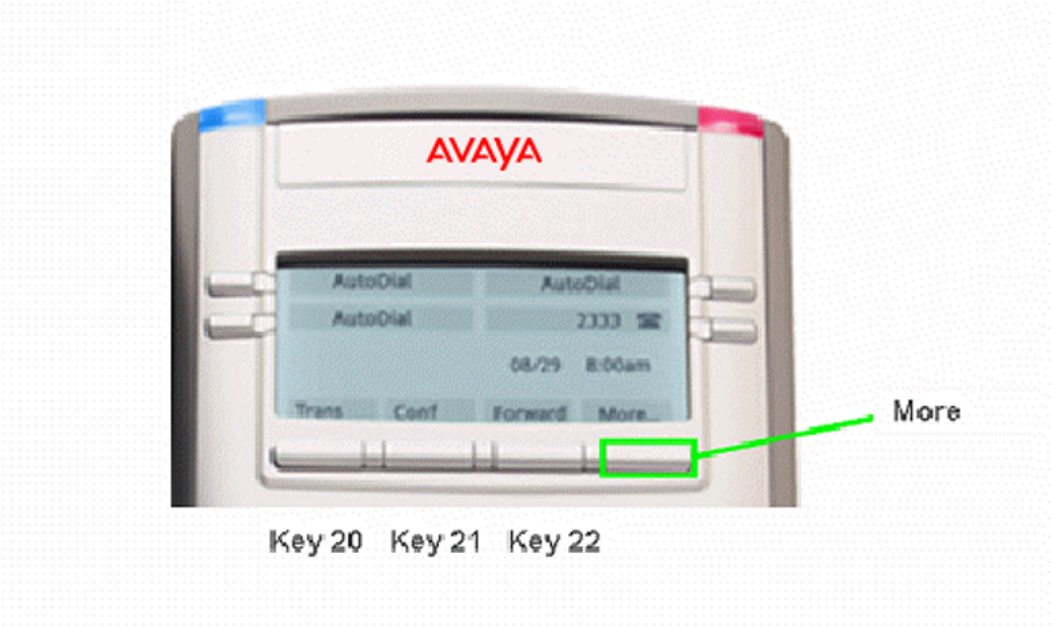


Figure 308: Avaya 1120E IP Deskphone with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

Avaya 1120E IP Deskphone Expansion Module 1 with Keys 32-49

The Avaya 1120E IP Deskphone can have up to three Expansion Modules which provides up to 54 additional line/feature keys.

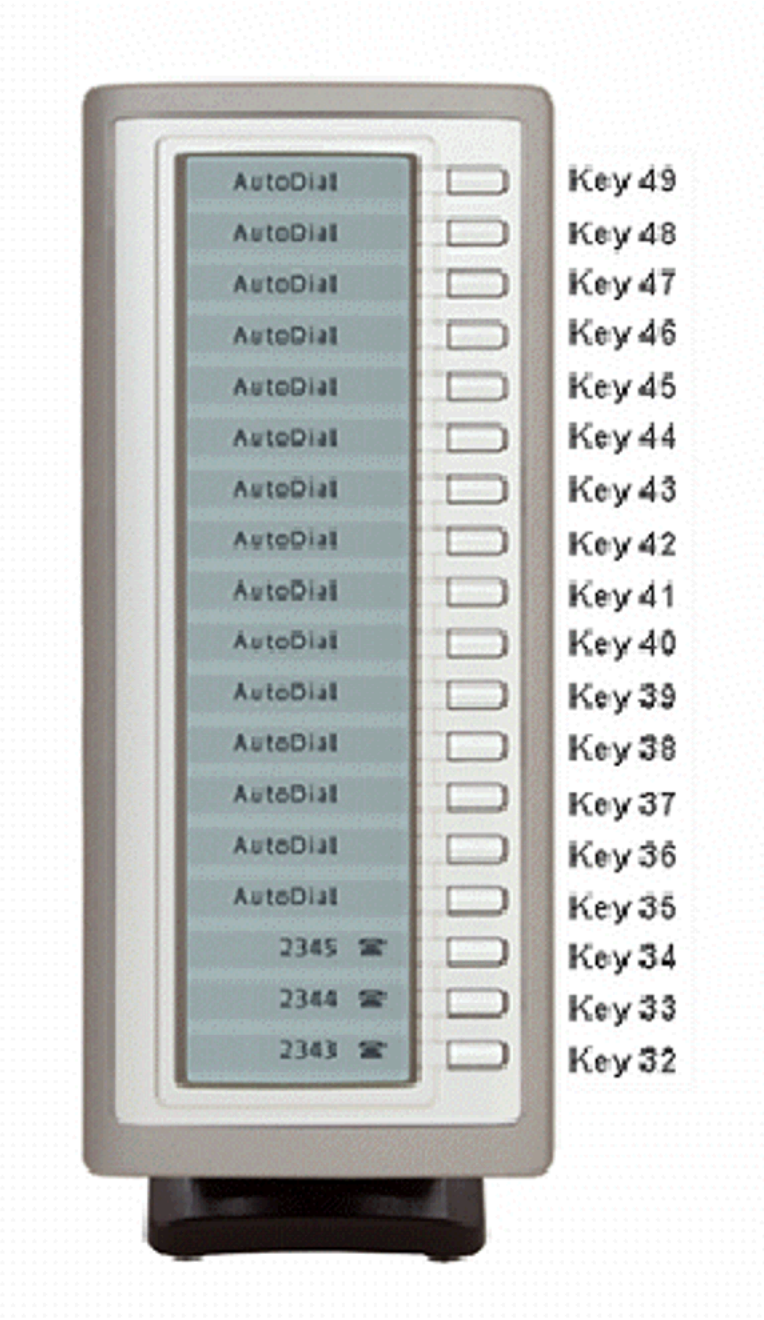


Figure 309: Avaya 1120E IP Deskphone Expansion Module 1 with Keys 32-49

Expansion Module 2 contains keys 50-67 and Expansion Module 3 contains keys 68-85.

Avaya 1120E IP Deskphone Default Keys Value

Table 6: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 1140E IP Deskphone

The following figure shows the Avaya 1140E IP Deskphone layout.

Figure 310: Avaya 1140E IP Deskphone Layout

Avaya 1140E IP Deskphone Display Areas

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

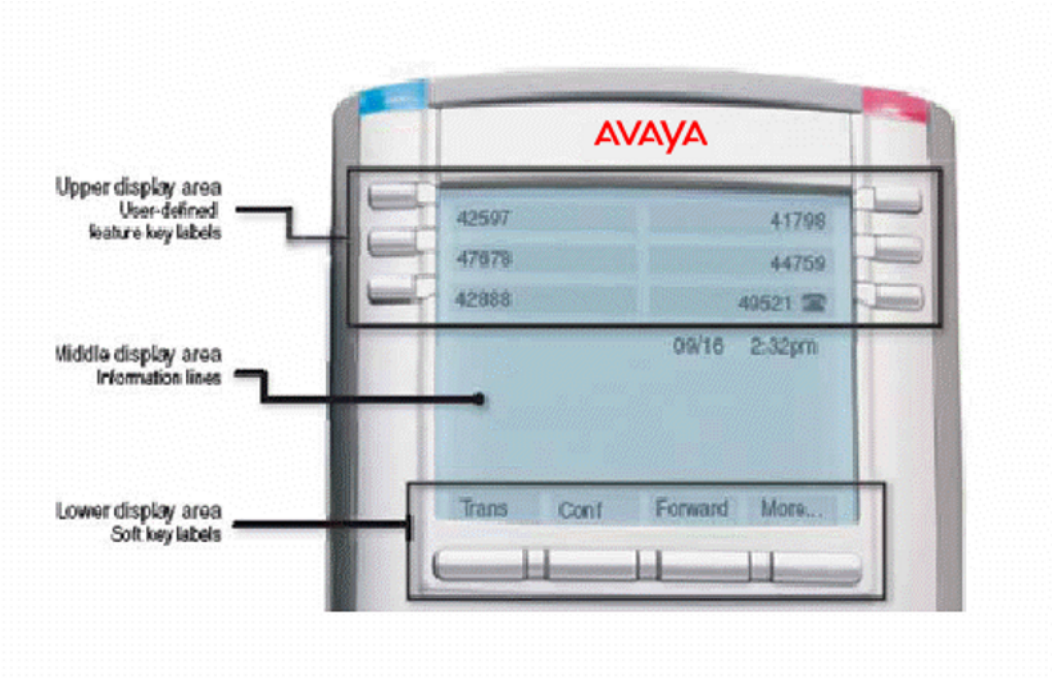


Figure 311: Avaya 1140E IP Deskphone Display Areas

Avaya 1140E IP Deskphone with Feature Keys 0-5 and Soft Keys 17-19

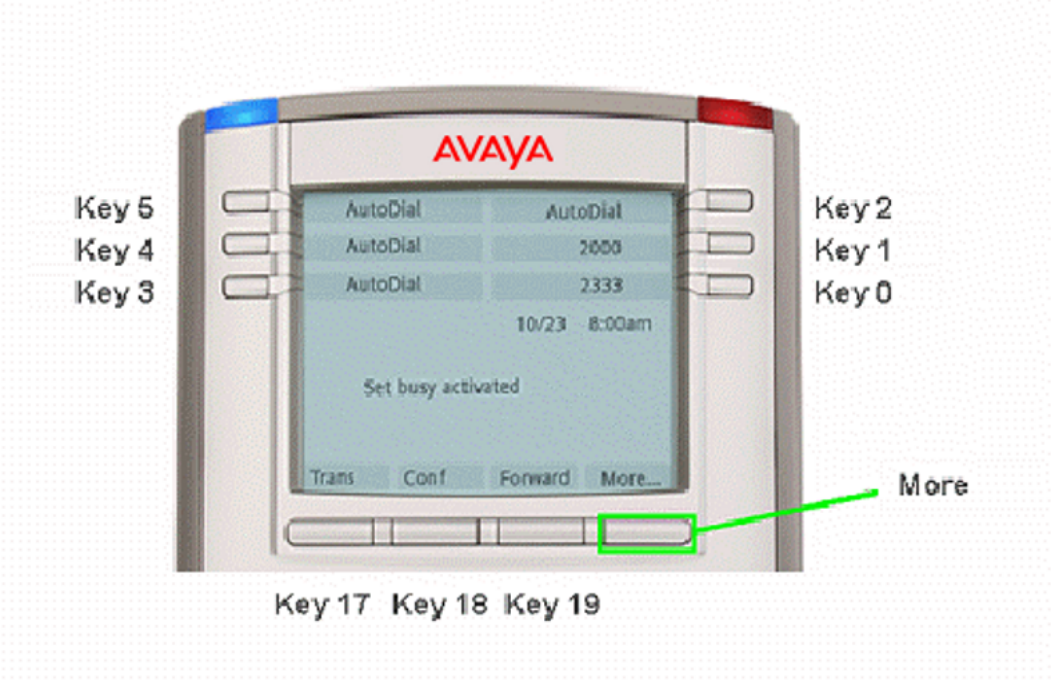


Figure 312: Avaya 1140E IP Deskphone with Soft Keys 17-19

Press the Shift/Outbox key to access Feature Keys 6-11.

Press the More key to access Soft Keys 20-22.

Avaya 1140E IP Deskphone with Soft Keys 20-22

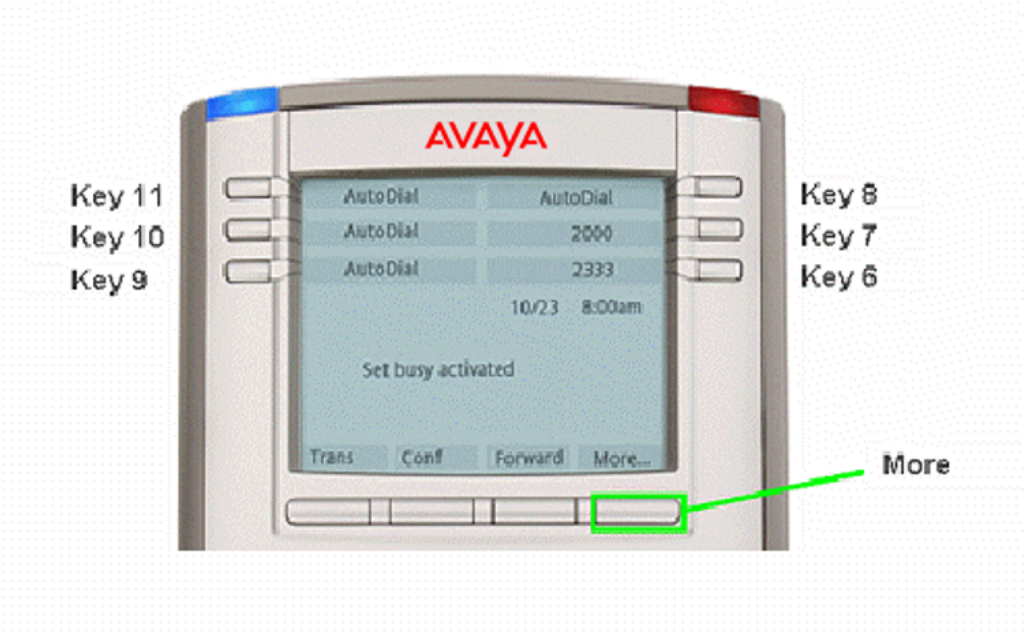


Figure 313: IP Phone 1140E with Soft Keys 20-22

Press the Shift/Outbox key to return to Feature Keys 0-5

Press the More key to access Soft Keys 20-22.

Avaya 1140E IP Deskphone with Soft Keys 20-22

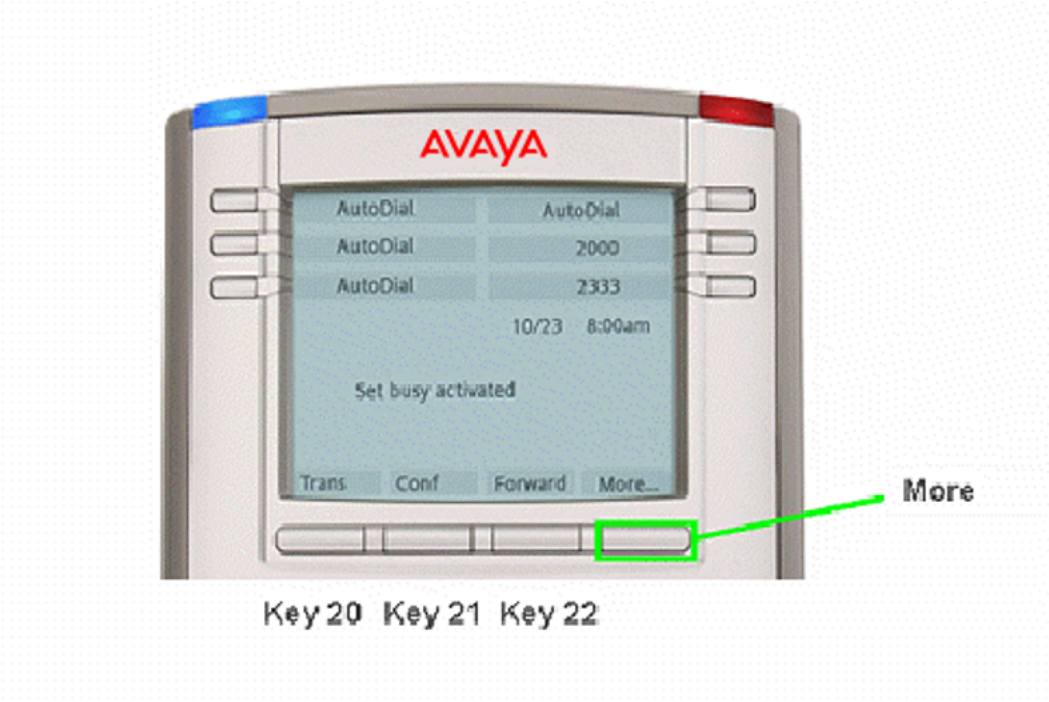


Figure 314: IP Phone 1140E with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

Avaya 1140E IP Deskphone Expansion Module 1 with Keys 32-49

The Avaya 1140E IP Deskphone can support up to 54 additional line/feature keys with 3 Expansion Modules. Using the Shift key functionality and one Expansion Module, it can provide up to 36 additional line/feature keys. With more than one Expansion Module connected, the Shift key functionality does not affect the Expansion Module since the maximum number of line/feature keys is already available.

Expansion Module 2 contains keys 50-67 and Expansion Module 3 contains keys 68-85.

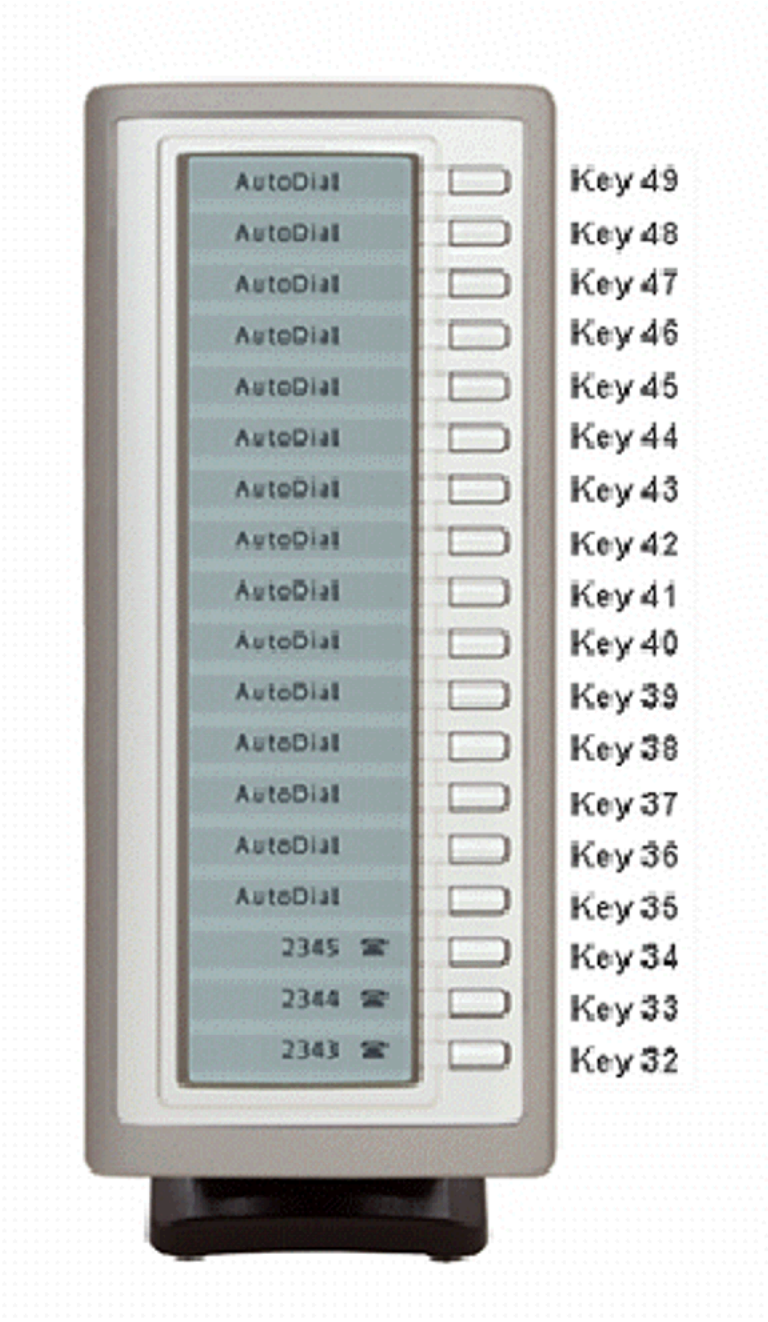


Figure 315: IP Phone 1140E Expansion Module 1 with Keys 32-49

Expansion Module 2 contains keys 50-67 and Expansion Module 3 contains keys 68-85.

Avaya 1140E IP Deskphone Default Keys Value

Table 7: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 1150E IP Deskphone

The following figure shows the Avaya 1150E IP Deskphone Default Agent Key Configuration.

Figure 316: Avaya 1150E IP Deskphone Default Agent Key Configuration

Avaya 1150E IP Deskphone Supervisor Key Configuration

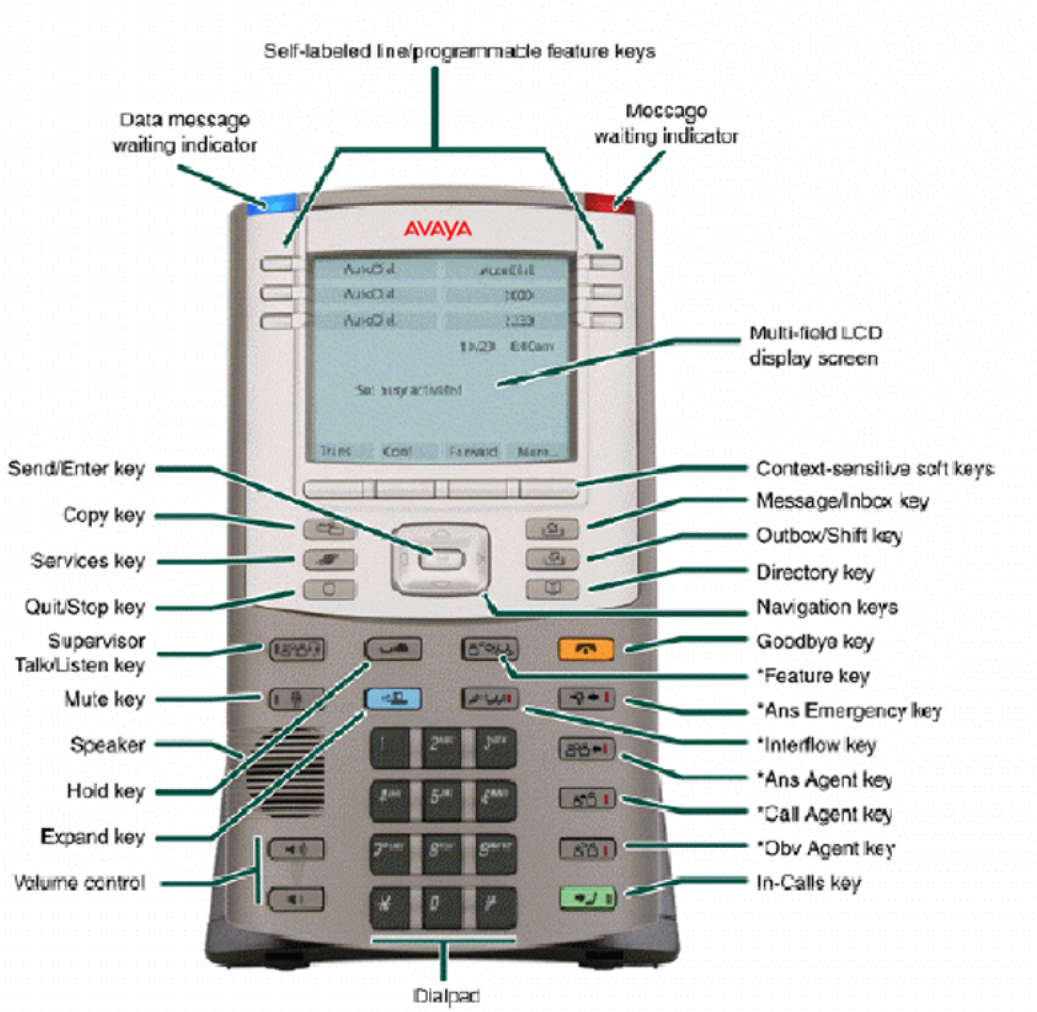


Figure 317: Avaya 1150E IP Deskphone Supervisor Key Configuration

Avaya 1150E IP Deskphone Display Areas

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

Key numbers 12-15 are used for the ACD fixed features but they can be programmed for different functions.

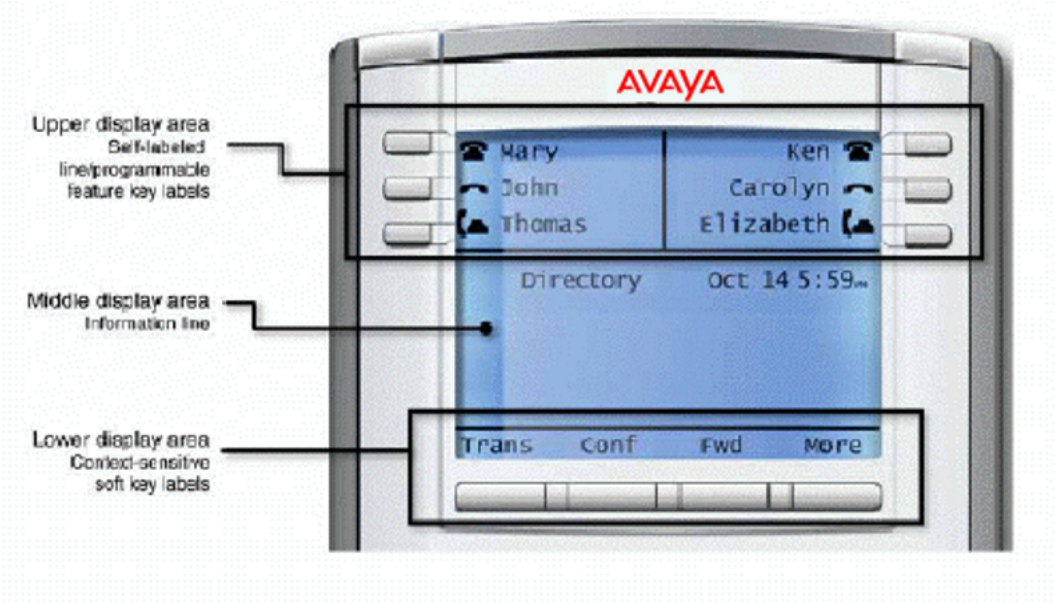


Figure 318: Avaya 1150E IP Deskphone Display Areas

ACD default Agent fixed feature keys

Key number	Response	Description
Key 12	NRD	Not Ready
Key 13	MSB	Make Set Busy
Key 14	ASP	Call Supervisor
Key 15	EMR	Emergency

Supervisor fixed feature keys

Key number	Response	Description
Key 12	OBV	Observe Agent
Key 13	RAG	Call Agent
Key 14	AAG	Answer Agent
Key 15	AMG	Answer Emergency

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

Avaya 1150E IP Deskphone with Feature Keys 0-5 and Soft Keys 17-19

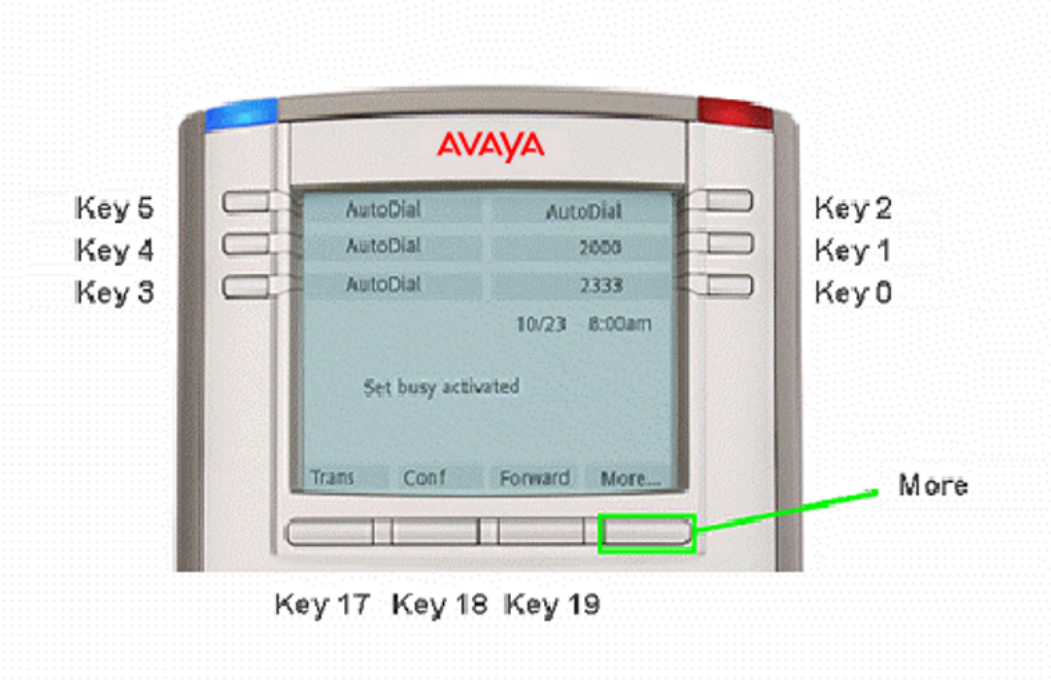


Figure 319: Avaya 1150E IP Deskphone with Soft Keys 17-19

Press the Shift/Outbox key to access Feature Keys 6-11.

Press the More key to access Soft Keys 20-22.

Avaya 1150E IP Deskphone with Soft Keys 6-11

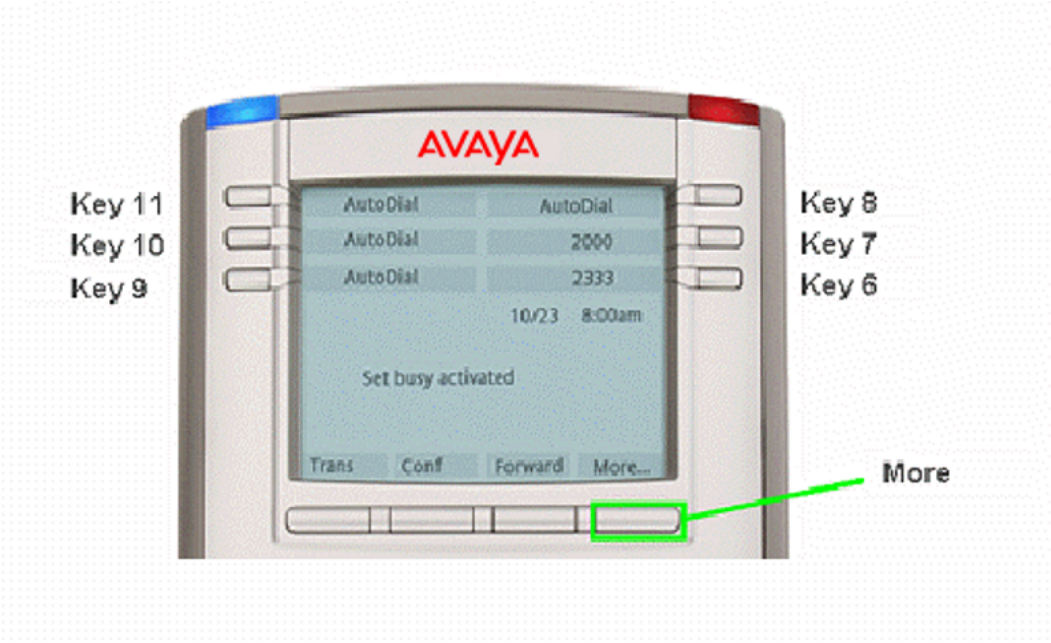


Figure 320: Avaya 1150E IP Deskphone with Soft Keys 6-11

Press the Shift/Outbox key to return to Feature Keys 0-5

Press the More key to access Soft Keys 20-22.

Avaya 1150E IP Deskphone with Soft Keys 20-22

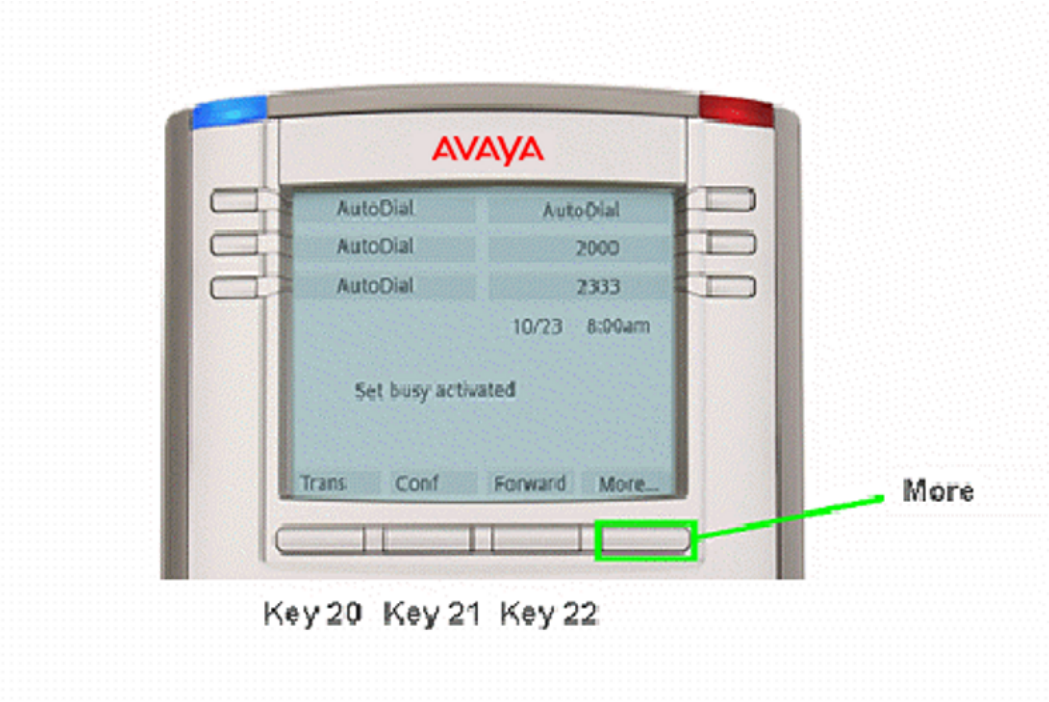


Figure 321: Avaya 1150E IP Deskphone with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

Avaya 1150E IP Deskphone Expansion Module 1 with Keys 32-49

The Avaya 1150E IP Deskphone can support up to 54 additional line/feature keys with 3 Expansion Modules. Using the Shift key functionality and one Expansion Module, it can provide up to 36 additional line/feature keys. With more than one Expansion Module connected, the Shift key functionality does not affect the Expansion Module since the maximum number of line/feature keys is already available.

Expansion Module 2 contains keys 50-67 and Expansion Module 3 contains keys 68-85.

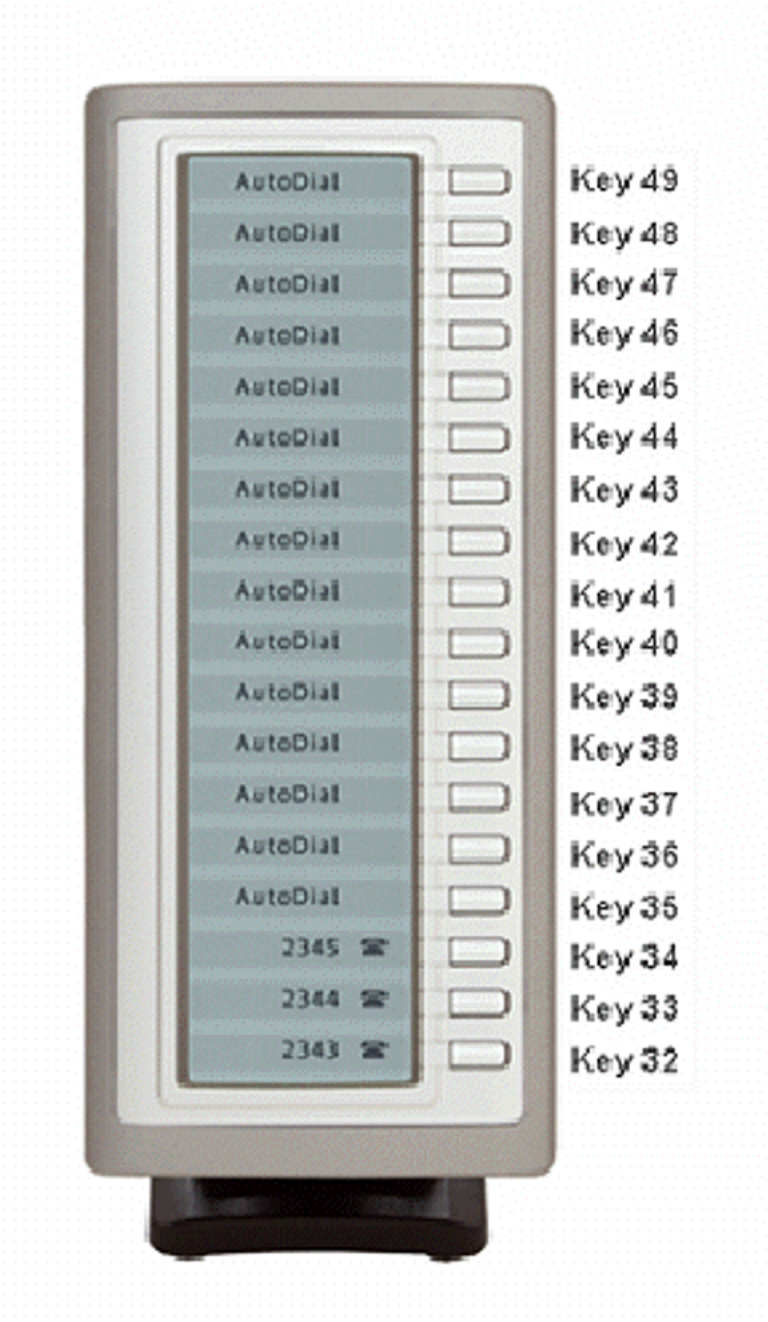


Figure 322: Avaya 1150E IP Deskphone Expansion Module 1 with Keys 32-49

Expansion Module 2 contains keys 50-67 and Expansion Module 3 contains keys 68-85.

Avaya 1150E IP Deskphone Default Keys Value

Table 8: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 1210 IP Deskphone

The following figure shows the Avaya 1210 IP Deskphone layout.

Figure 323: Avaya 1210 IP Deskphone Layout

The Avaya 1210 IP Deskphone has five fixed call-processing keys (hold, goodbye, handsfree, headset, mute), four context-sensitive soft keys, and two specialized fixed keys (Services and Message).

Context-sensitive soft keys are below the display area. The LCD label above each key changes based on the active feature.

The Services key is used to access various phone options, such as changing the ring type.

Double-press the Services key to access the Local Tools menu, and use the navigation keys to make a selection.

Press the Navigation keys to scroll through menus and lists that appear on the display screen. The outer part of this key cluster rocks for up, down, left, and right movements.

Press the Enter key, at the center of the Navigation key cluster, to confirm menu selections.

In most menus, you can press the Enter key instead of the Select soft key.

Avaya 1210 IP Deskphone Default Keys Value

Table 9: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 1220 IP Deskphone

The following figure shows the Avaya 1220 IP Deskphone layout.

Figure 324: Avaya 1220 IP Deskphone Layout

The Avaya 1220 IP Deskphone has six specialized fixed keys (quit, directory, message, redial, services, and applications), six fixed call-processing keys (hold, goodbye, handsfree, headset, mute, and conference), and four context-sensitive soft keys. The Avaya 1220 IP Deskphone also has six programmable DN/feature keys.

The keys on either side of the display area are programmable keys with labels on the LCD display. The system administrator programs these keys as memory, line, or intercom keys.

Avaya 1220 IP Deskphone Programmable/DN Feature keys

Figure 325: Avaya 1220 IP Deskphone Programmable/DN Feature keys

Context-sensitive soft keys are located below the display area. The LCD label above each key changes based on the active feature.

The Services key is used to access various phone options, such as changing the ring type. Double-press the Services key to access the Local Tools menu, and use the navigation keys to make a selection.

Press the Navigation keys to scroll through menus and lists that appear on the display screen. The outer part of this key cluster rocks for up, down, left, and right movements

Press the Enter key, at the center of the Navigation key cluster, to confirm menu selections.

In most menus, you can press the Enter key instead of the Select soft key.

The Avaya 1220 IP Deskphone supports up to four LCD 12- Key Self-Labeling Expansion Modules.

LCD Expansion Module:12-Key Self-Labeling

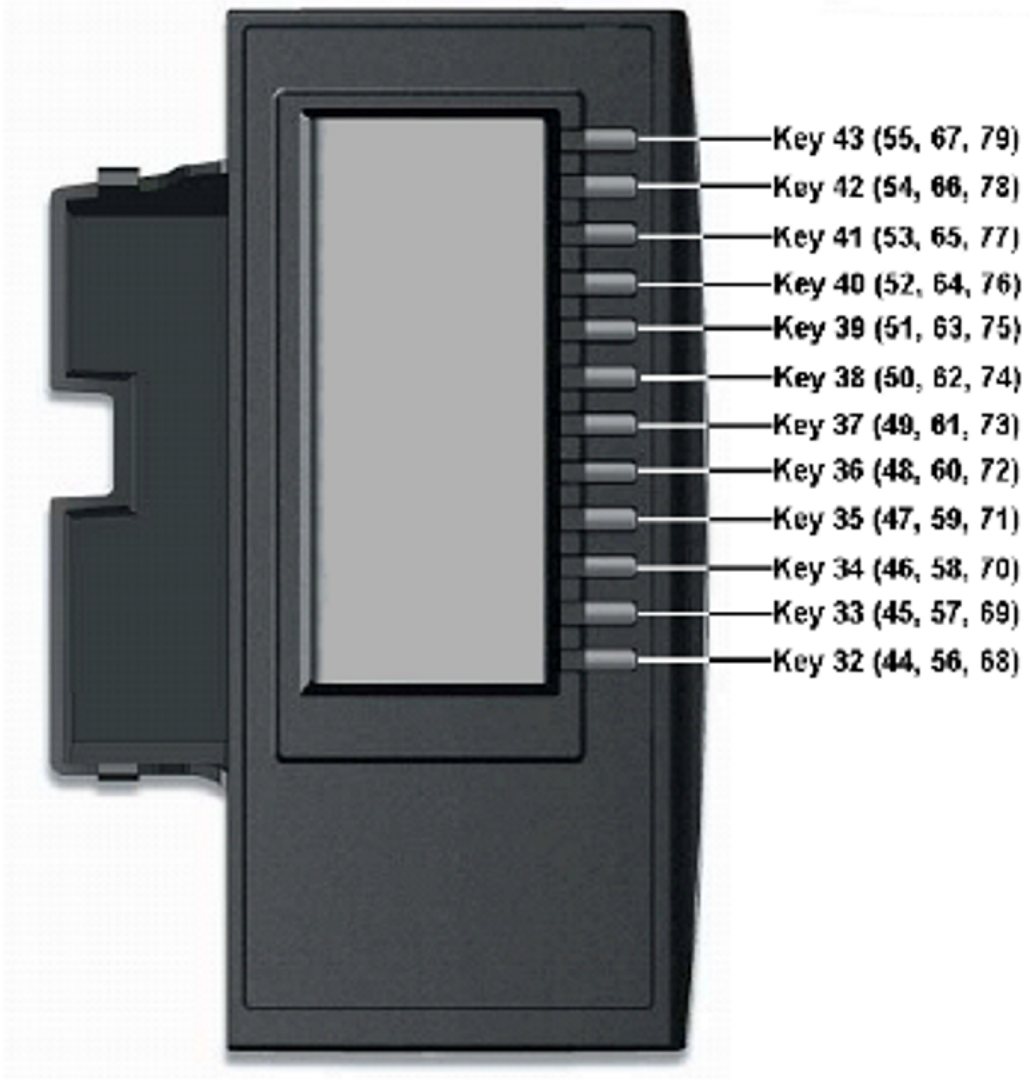


Figure 326: LCD Expansion Module:12-Key Self-Labeling

Avaya 1220 IP Deskphone Default Keys Value

Table 10: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 1230 IP Deskphone

The following figure shows the Avaya 1230 IP Deskphone layout.

Figure 327: Avaya 1230 IP Deskphone layout

The Avaya 1230 IP Deskphone has six specialized fixed keys (quit, directory, message, redial, services, and applications), six fixed call-processing keys (hold, goodbye, handsfree, headset, mute, and conference), and four context-sensitive soft keys. The Avaya 1230 IP Deskphone also has twenty programmable feature keys: ten keys for user-defined feature key labels and ten lines/features that can be accessed through Second Page Functionality.

The keys on either side of the display area are programmable keys with labels on the LCD display. The system administrator programs these keys as memory, line, or intercom keys.

Programmable/DN Feature keys

First page of programmable/DN feature keys.

Figure 328: Programmable/DN feature keys (first page)

Second page of programmable/DN feature keys.

Figure 329: Programmable/DN feature keys (second page)

Context-sensitive soft keys are below the display area. The LCD label above each key changes based on the active feature. The Services key is on the bottom left of the display area and is used to access various phone options, such as changing the ring type.

Double-press the Services key to access the Local Tools menu, and use the navigation keys to make a selection

Press the Navigation keys to scroll through menus and lists that appear on the display screen. The outer part of this key cluster rocks for up, down, left, and right movements.

Press the Enter key, at the center of the Navigation key cluster, to confirm menu selections. In most menus, you can press the Enter key instead of the Select soft key.

The 10 keys on either side of the LCD are self-labeled line/programmable feature keys, with labels on the LCD. These keys also function as line (DN) keys. These keys are numbered 0 — 9 for the first feature key page. Press the Left or Right arrow keys to access the second page of feature keys (Second Page Functionality). The keys on the second feature key page

are numbered from 10 — 15, and the last four are numbered 27 — 30. Keys 17 — 26 are reserved for soft keys.

Key 0 is the primary DN key. Keys 1 — 15 and 27 — 30 can be configured with any DN or feature key supported on IP phones except for Message Waiting, which must be configured on Key 16.

The Avaya 1230 IP Deskphone supports up to four LCD 12-Key Self-Labeling Expansion Modules.

LCD Expansion Module:12-Key Self-Labeling

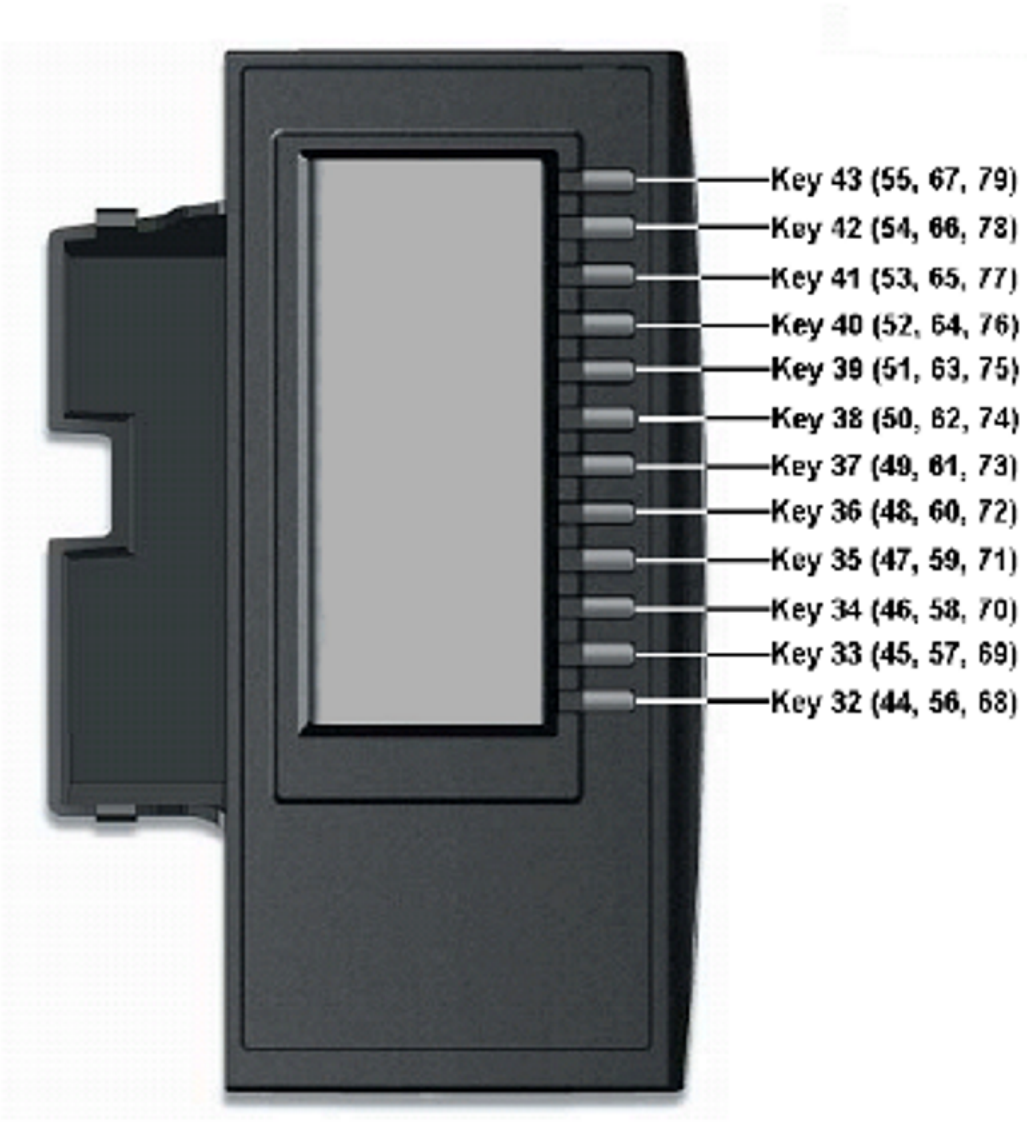


Figure 330: LCD Expansion Module:12-Key Self-Labeling

Avaya 1230 IP Deskphone Default Key Values

Table 11: Default Key Values

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

IP Phone 2001

The following figure shows the IP Phone 2001 layout.

Figure 331: IP Phone 2001 Layout

IP Phone 2001 Display Areas

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

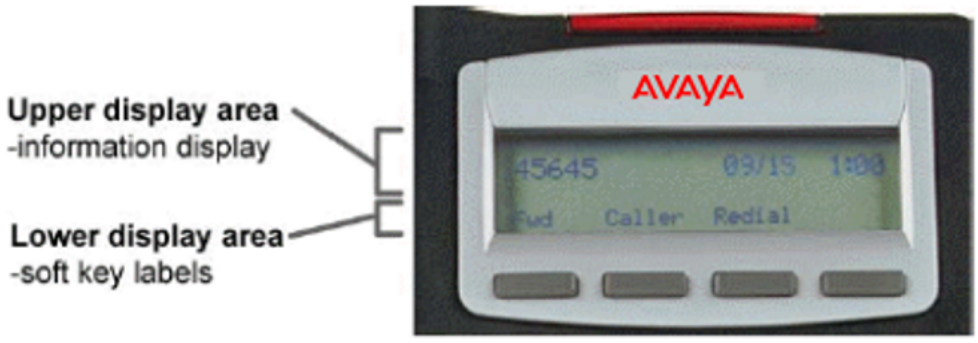


Figure 332: IP Phone 2001 Display Areas

IP Phone 2001 with Soft Keys 17-19

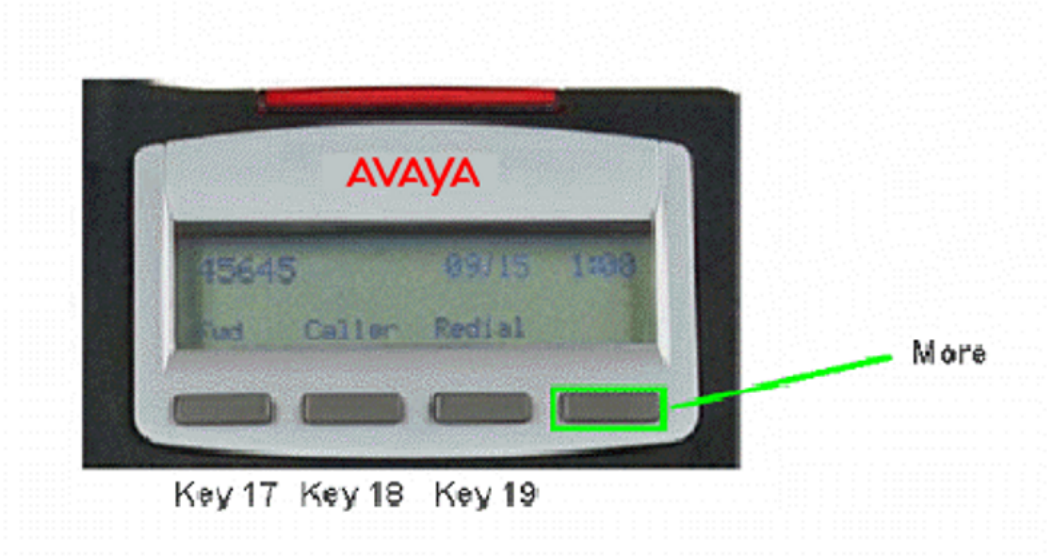


Figure 333: IP Phone 2001 with Soft Keys 17-19

Press the More key to access Soft Keys 20-22.

IP Phone 2001 with Soft Keys 20-22

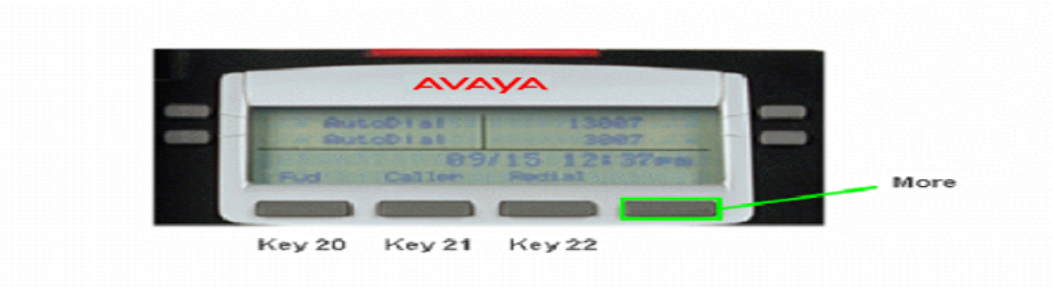


Figure 334: IP Phone 2001 with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

IP Phone 2001 Default Keys Value

Table 12: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

IP Phone 2002

The following figure shows the IP Phone 2002 layout.

Figure 335: IP Phone 2002 Layout

IP Phone 2002 Programmable Line (DN)/Feature Key and Soft Key Labels

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

Figure 336: IP Phone 2002 Programmable Line (DN)/Feature Key and Soft Key Labels

IP Phone 2002 with Feature Keys 0-3 and Soft Keys 17-19

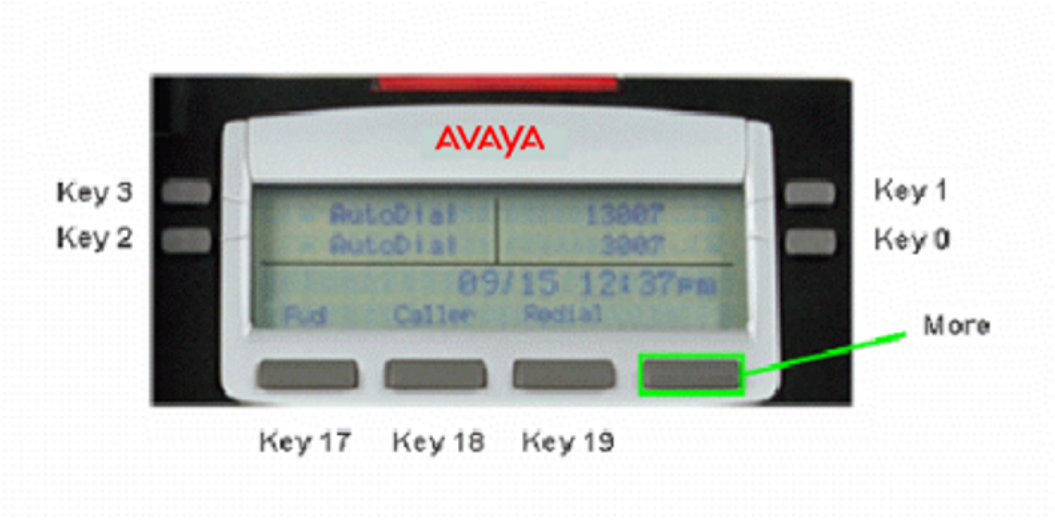


Figure 337: IP Phone 2002 with Feature Keys 0-3 and Soft Keys 17-19

Press the More key to access Soft Keys 20-22.

IP Phone 2002 with Soft Keys 20-22

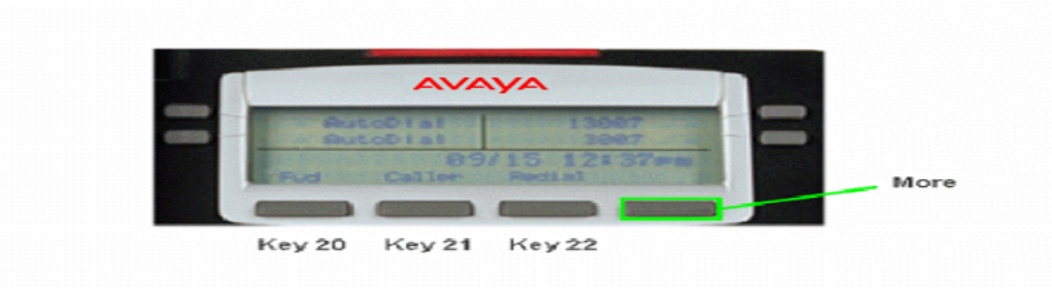


Figure 338: IP Phone 2002 with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

IP Phone 2002 Key Expansion Module 1 with Keys 32-55

Figure 339: IP Phone 2002 Key Expansion Module 1 with Keys 32-55

The IP Phone 2002 can have up to 54 additional line/feature keys with 3 IP Phone Key Expansion Modules (KEM). The IP Phone 2002 does not support Shift key functionality

KEM 2 contains keys 56-79

IP Phone 2002 Default Keys Value

Table 13: Default Keys Value

Key No	Value
16	Message Waiting (MWK)

Key No	Value
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

IP Phone 2004

The following figure shows the IP Phone 2004 layout.

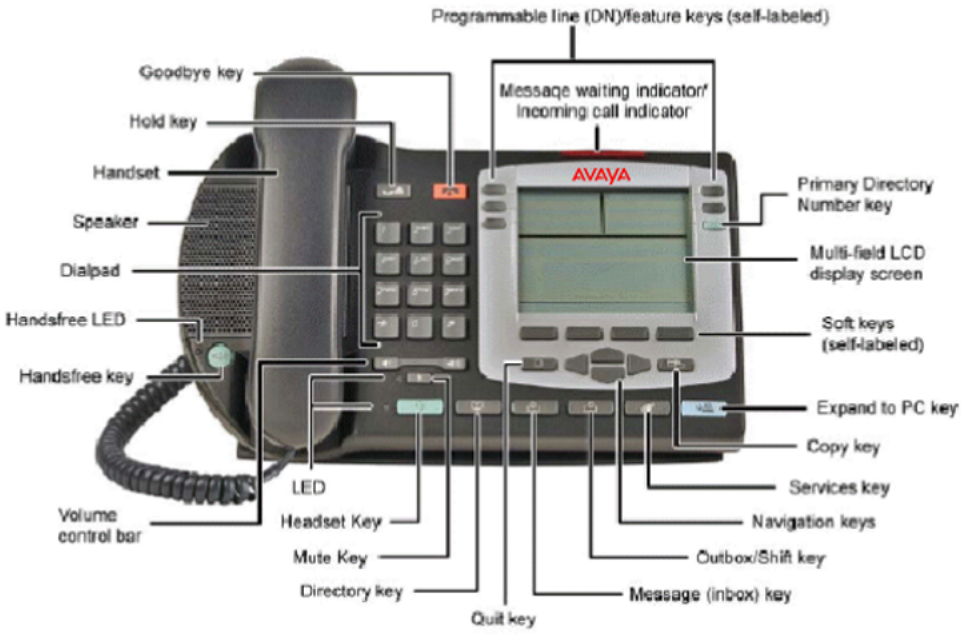


Figure 340: IP Phone 2004 Layout

IP Phone 2004 Programmable Line (DN)/Feature Key and Soft Key Labels

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

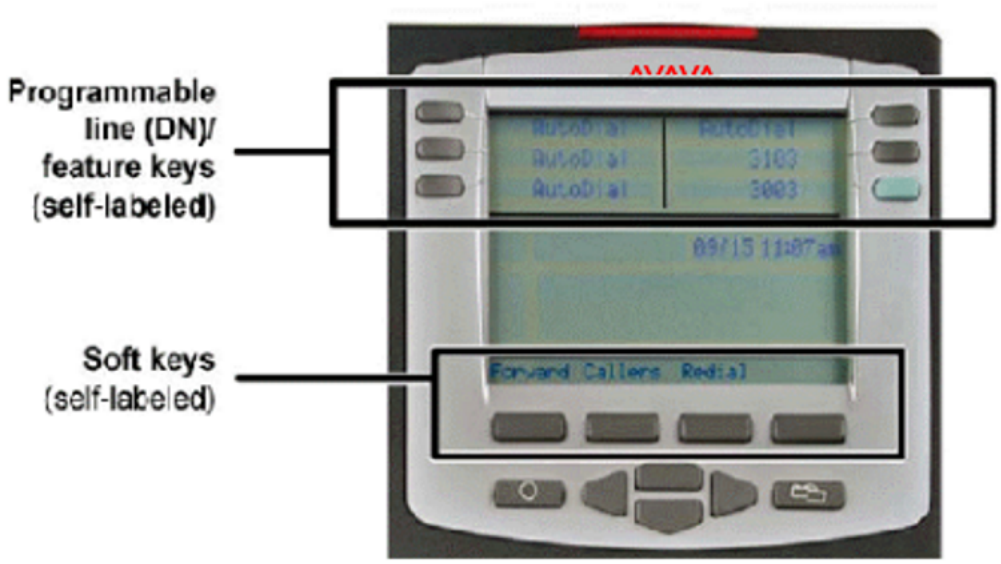


Figure 341: IP Phone 2004 Programmable Line (DN)/Feature Key and Soft Key Labels

IP Phone 2004 with Feature Keys 0-5 and Soft Keys 17-19

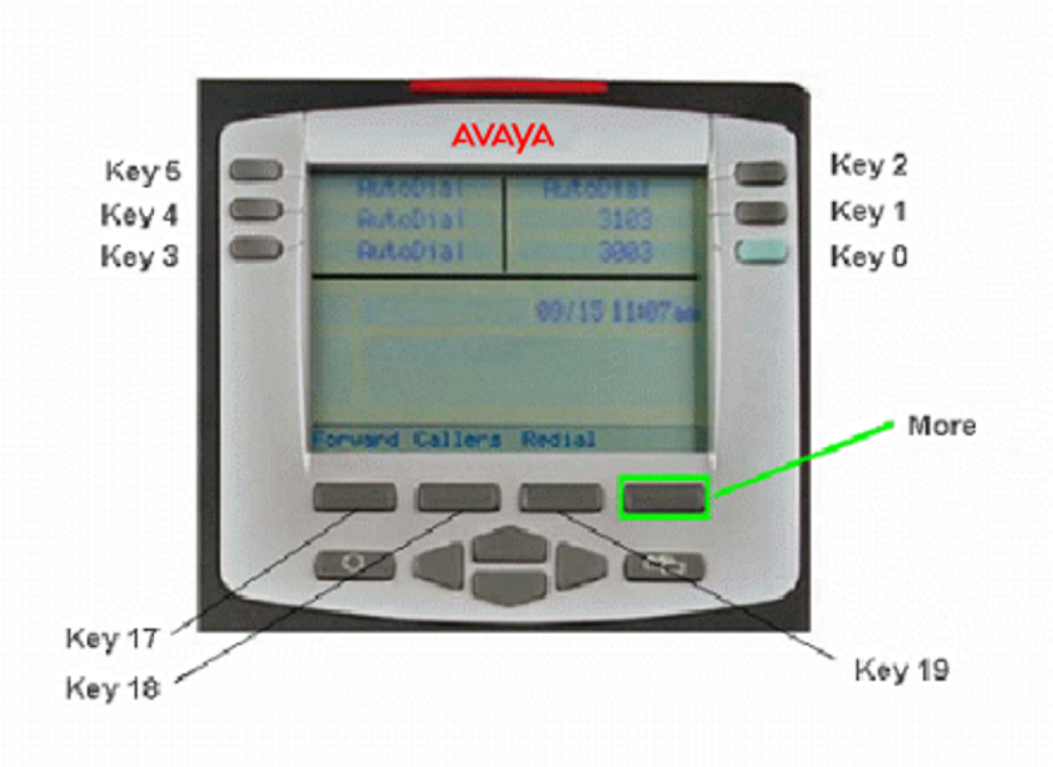


Figure 342: IP Phone 2004 with Feature Keys 0-5 and Soft Keys 17-19

Press the Shift/Outbox key to access Feature Keys 6-11.

Press the More key to access Soft Keys 20-22.

IP Phone 2004 with Feature Keys 6-11

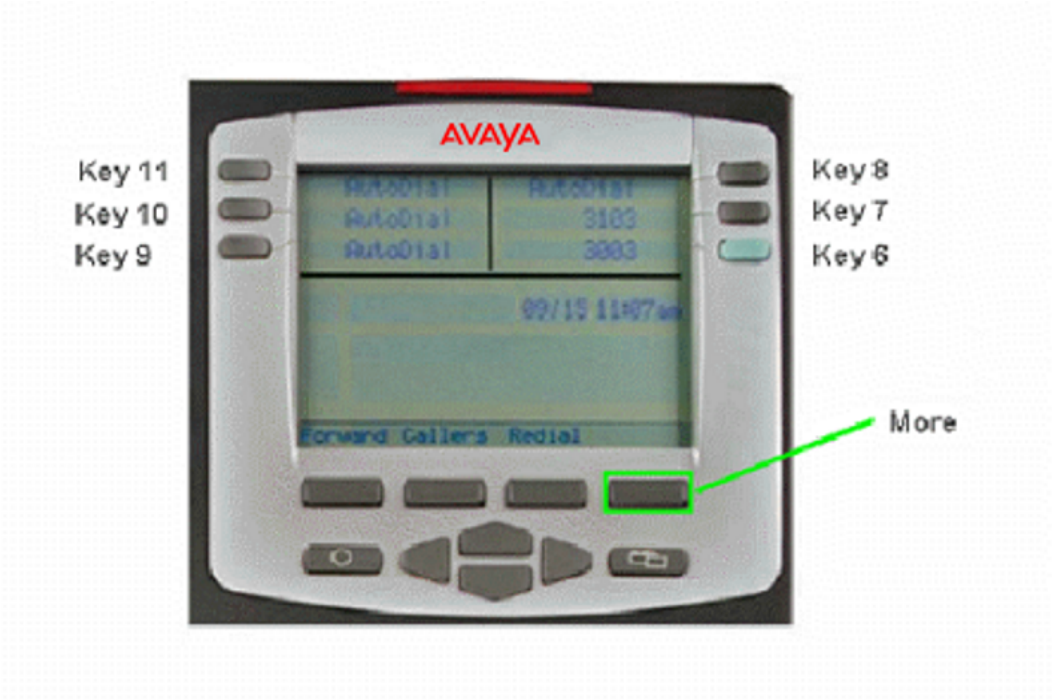


Figure 343: IP Phone 2004 with Feature Keys 6-11

Press the Shift/Outbox key to return to Feature Keys 0-5

Press the More key to access Soft Keys 20-22.

IP Phone 2004 with Soft Keys 20-22

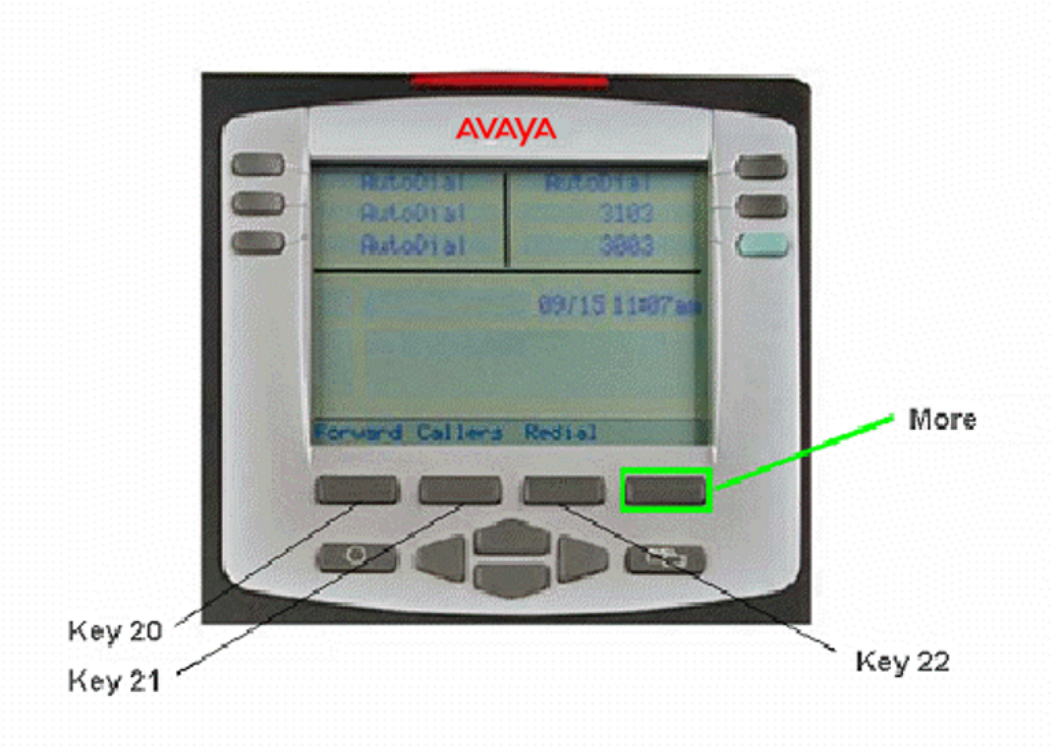


Figure 344: IP Phone 2004 with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

IP Phone 2004 Key Expansion Module 1 with Keys 32-55

The IP Phone 2004 can support up to 54 additional line/feature keys with 3 Key Expansion Module (KEM) or with one KEM using the Shift key functionality Key. With two IP Phone KEMs connected, the Shift key functionality does not affect the IP Phone KEMs since the maximum number of line/feature keys is already available.

KEM 2 contains keys 56-79.

Figure 345: IP Phone 2004 Key Expansion Module 1 with Keys 32-55

IP Phone 2004 Default Keys Value

Table 14: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)

Key No	Value
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 2007 IP Deskphone

The following figure shows the Avaya 2007 IP Deskphone layout.

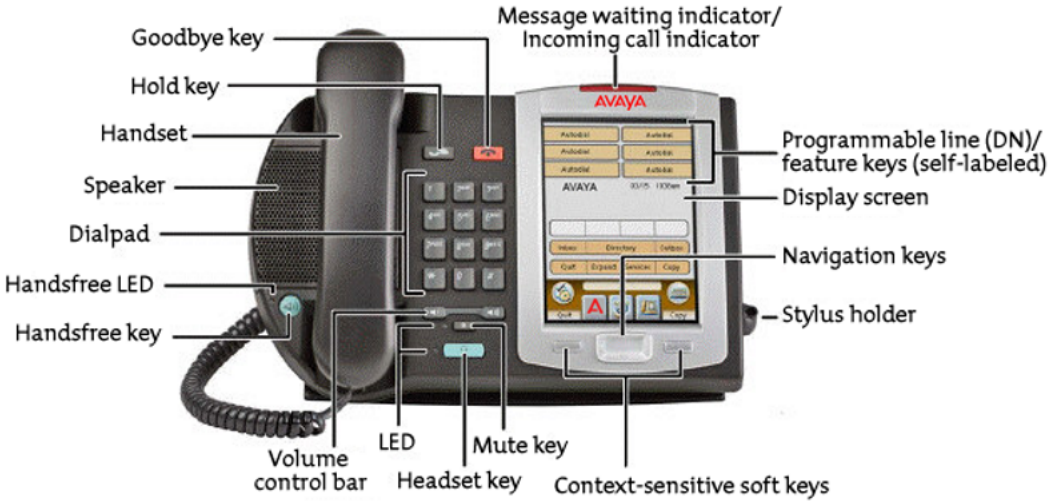


Figure 346: Avaya 2007 IP Deskphone Layout

Avaya 2007 IP Deskphone Application Areas

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

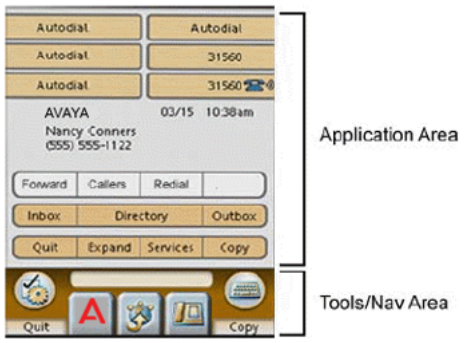


Figure 347: Avaya 2007 IP Deskphone Application Areas

Avaya 2007 IP Deskphone with Feature Keys 0-5 and Soft Keys 17-19

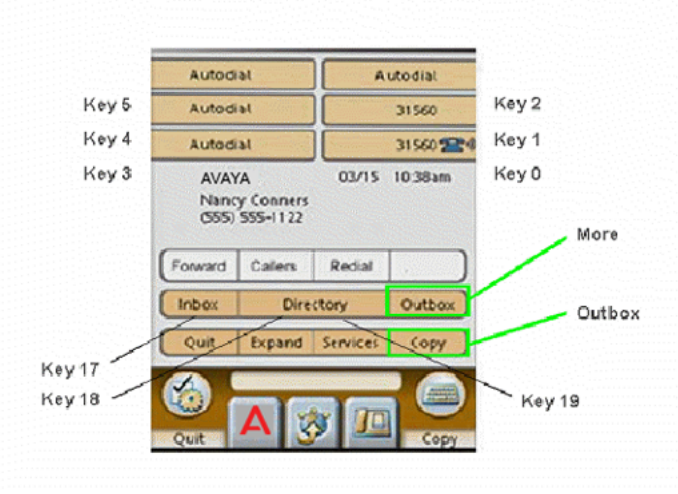


Figure 348: Avaya 2007 IP Deskphone with Feature Keys 0-5 and Soft Keys 17-19

Press the More key to access Soft Keys 20-22.

Press the Outbox key to access Feature Keys 6-11.

Avaya 2007 IP Deskphone with Feature Keys 6-11

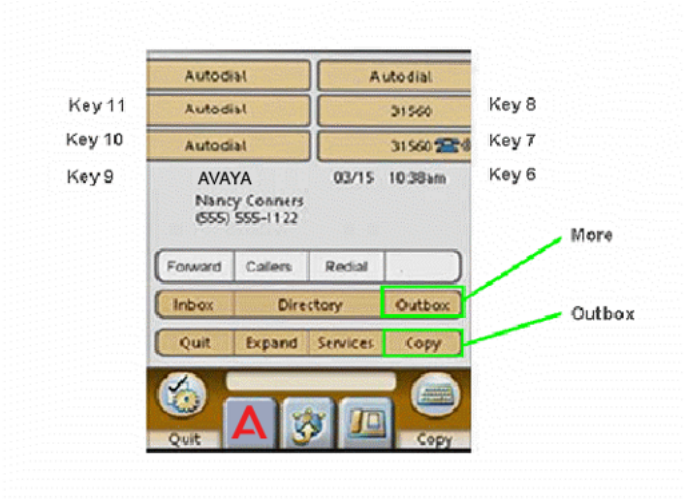


Figure 349: Avaya 2007 IP Deskphone with Feature Keys 6-11

Press the More key to access Soft Keys 20-22.

Press the Outbox key to return to Feature Keys 0-5.

Avaya 2007 IP Deskphone with Soft Keys 20-22

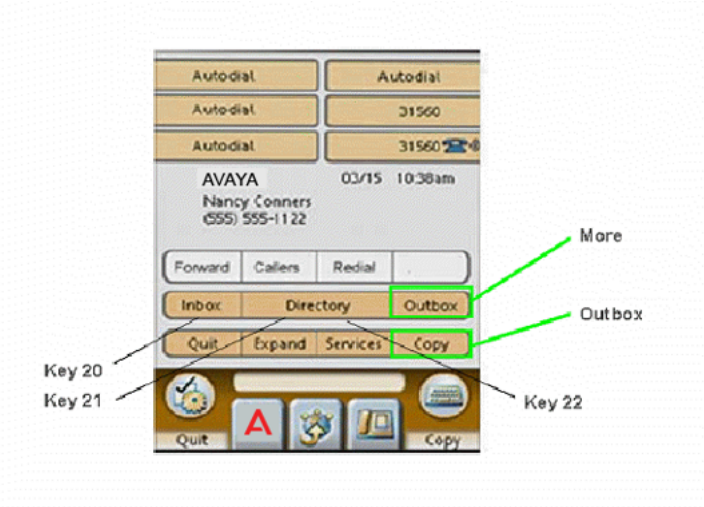


Figure 350: Avaya 2007 IP Deskphone with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

Avaya 2007 IP Deskphone Default Keys Value

Table 15: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 2033 IP Conference Phone

The following figure shows the Avaya 2033 IP Conference Phone.

Figure 351: Avaya 2033 IP Conference Phone Layout

Avaya 2033 IP Conference Phone Display Areas

The Message Indication key is assigned to key 16. Keys numbered 17 to 31 are the soft keys below the display area. Keys 27-31 are reserved for future feature implementation.

Figure 352: Avaya 2033 IP Conference Phone Display Areas

Avaya 2033 IP Conference Phone with Soft Keys 17-19

Figure 353: Avaya 2033 IP Conference Phone with Soft Keys 17-19

Use the Shift (>>) key to navigate through the layers of functions. If there are only three functions assigned to the soft keys, the Shift (>>) key does not appear and all three functions are displayed.

Avaya 2033 IP Conference Phone Default Keys Value

Table 16: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)

Key No	Value
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Avaya 2050 IP Softphone

The following figure shows the Avaya 2050 IP Softphone layout.

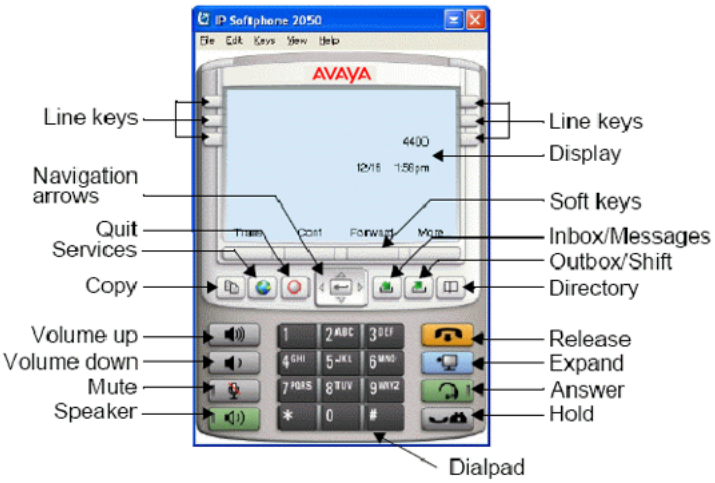


Figure 354: Avaya 2050 IP Softphone layout.

Avaya 2050 IP Softphone - Compact Skin Call Control Window

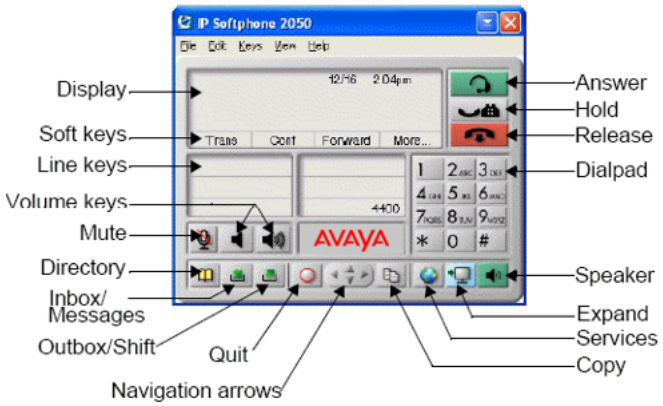


Figure 355: Avaya 2050 IP Softphone - Compact Skin Call Control Window

Avaya 2050 IP Softphone - 1140 Skin Display

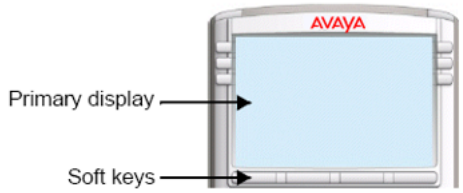


Figure 356: Avaya 2050 IP Softphone - 1140 Skin Display

Avaya 2050 IP Softphone - Compact Skin Display

Figure 357: Avaya 2050 IP Softphone - Compact Skin Display

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will only be 1 layer of soft keys containing keys 17-20 and there will be no More key.

The Message key is numbered 16. Key numbers 17 to 31 are the four soft key labels below the display area. Keys 27-31 are reserved for future feature implementation.

Avaya 2050 IP Softphone with Feature Keys 0-5 and Soft Keys 17-19

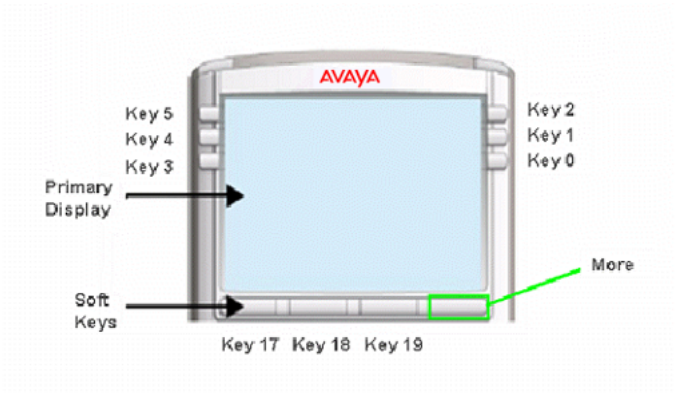


Figure 358: Avaya 2050 IP Softphone with Feature Keys 0-5 and Soft Keys 17-19

Press the Outbox/Shift key to access Feature Keys 6-11.

Press the More key to access Soft Keys 20-22.

Avaya 2050 IP Softphone with Feature Keys 6-11

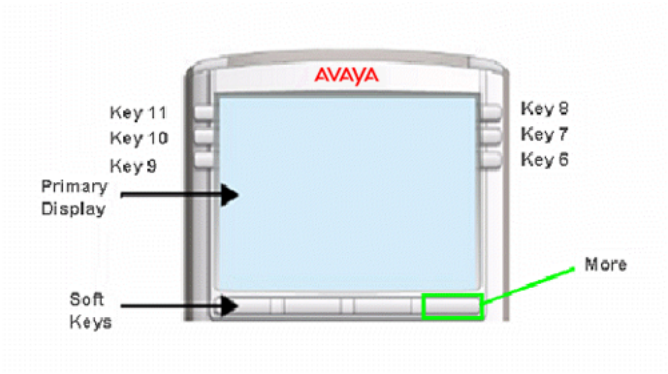


Figure 359: Avaya 2050 IP Softphone with Feature Keys 6-11

Press the Outbox/Shift key to return to Feature Keys 0-5.

Press the More key to access Soft Keys 20-22.

Avaya 2050 IP Softphone with Soft Keys 20-22

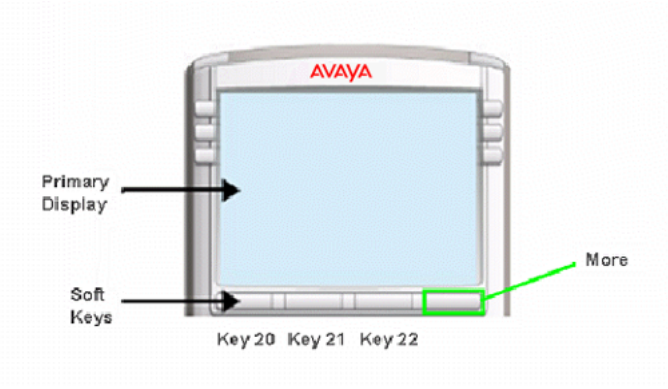


Figure 360: Avaya 2050 IP Softphone with Soft Keys 20-22

Press the More key to access Soft Keys 23-25, 26-28 and 29-31. Note that Soft Keys are numbered from left to right on each page. Pressing the More key on the last page with Soft Keys 29-31 will return you to Soft Keys 17-19.

Avaya 2050 IP Softphone Default Key Values

Table 17: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Meridian M2006 Digital Telephone

The following figure shows the Meridian M2006 Digital Telephone Layout.

Figure 361: Meridian M2006 Digital Telephone Layout

The M2006 is a single-line telephone with six programmable function keys, and accepts only one DN. The fixed keys are hold, release, and volume control. The remaining five keys can be assigned any feature that is not a DN.

M2006 with Feature Keys 0 to 5

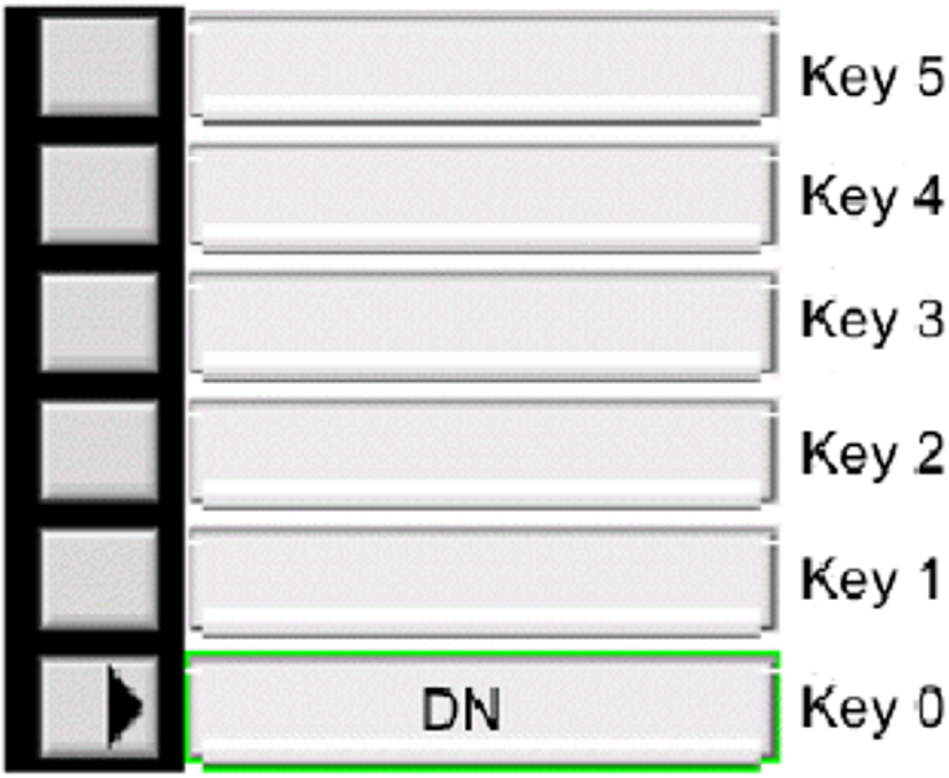


Figure 362: M2006 with Feature Keys 0 to 5

M2006 Default Key Values

No default key values.

Meridian M2008 Digital Telephone

The following figure shows the Meridian M2008 Digital Telephone Layout.

Figure 363: Meridian M2008 Digital Telephone Layout

The M2008 is a multi-line telephone with eight programmable function keys. The fixed keys are hold, release, and volume control. The remaining seven keys can be assigned any feature.

M2008 with Feature Keys 0 to 7

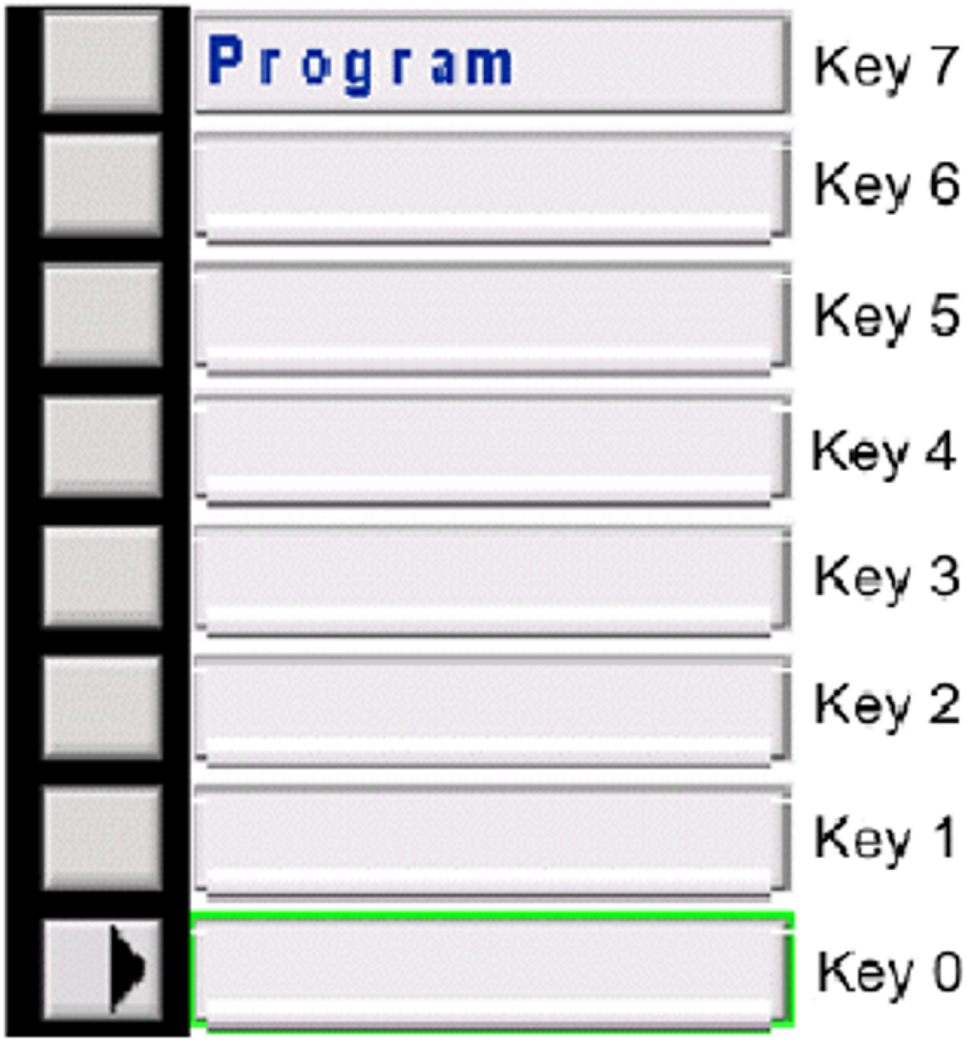


Figure 364: M2008 with Feature Keys 0 to 7

M2008 Default Key Values

No default key values.

Meridian M2616 Digital Telephone

The following figure shows the Meridian M2616 Digital telephone layout.

Figure 365: Meridian M2616 Digital telephone layout

M2616 with Feature Keys 0 to 15

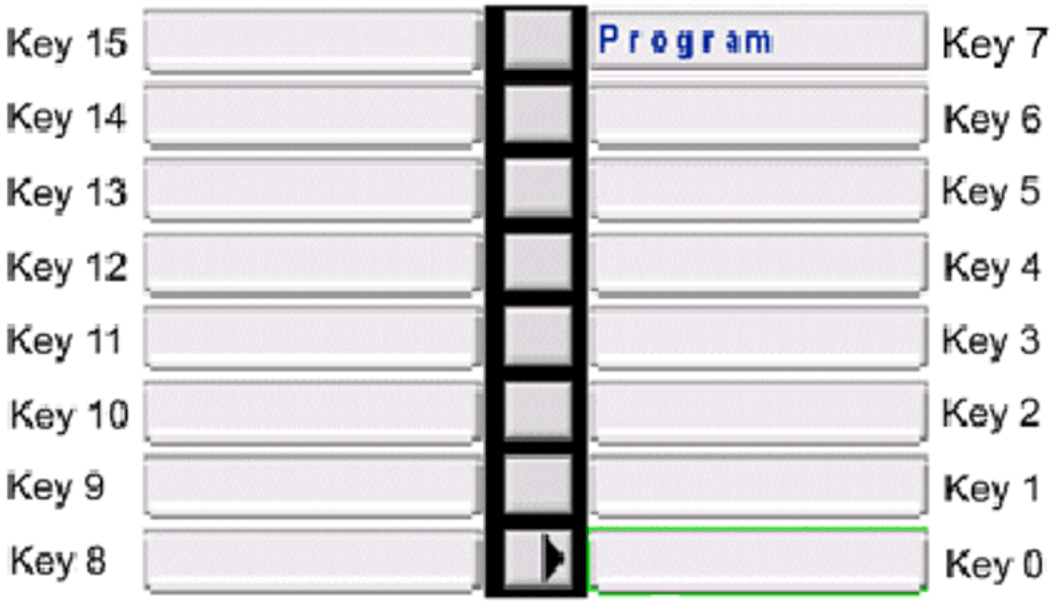


Figure 366: M2616 with Feature Keys 0 to 15

M2616 with Feature Keys 16 to 37

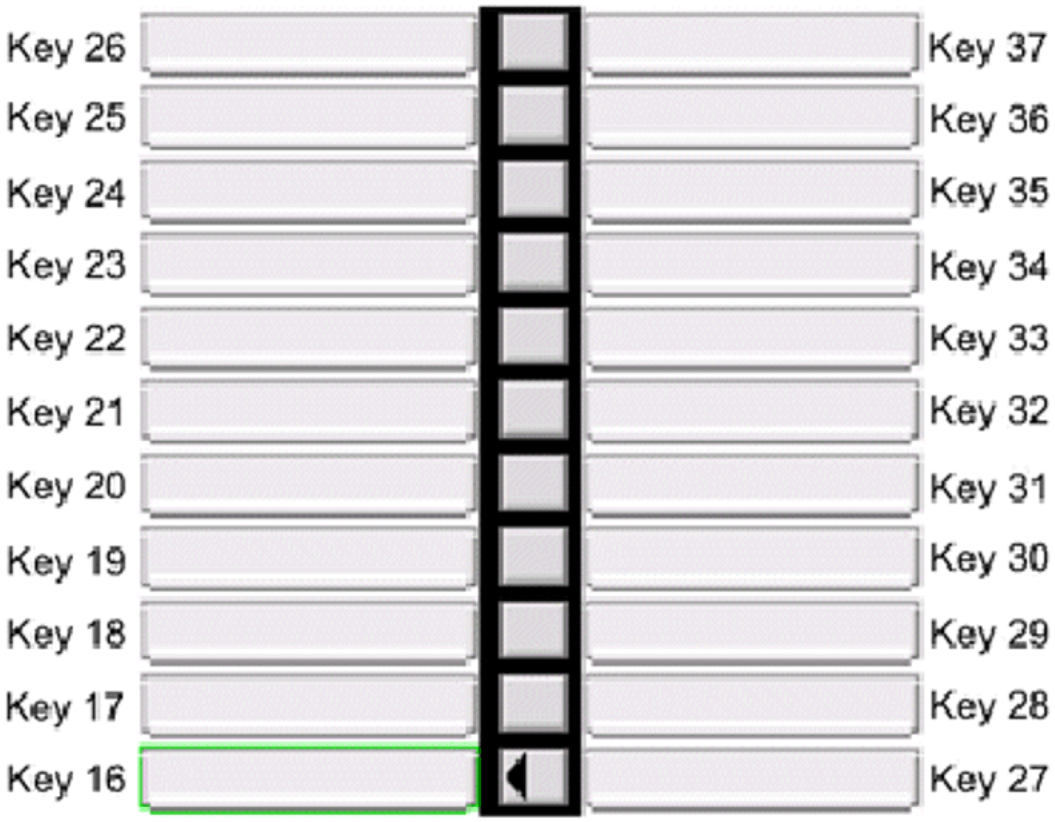


Figure 367: M2616 with Feature Keys 16 to 37

M2616 with Feature Keys 38 to 59

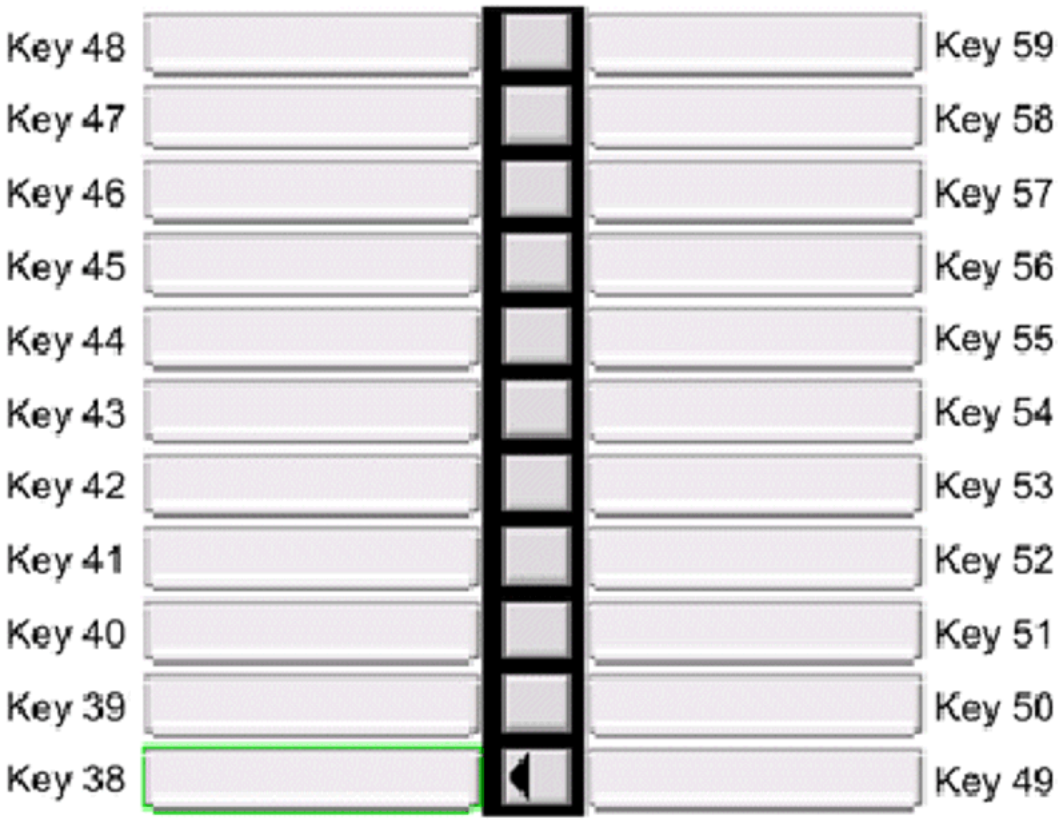


Figure 368: M2616 with Feature Keys 38 to 59

Meridian M2616 Default Key Values

No default key values.

Avaya 3902 Digital Deskphone

The following figure shows the Avaya 3902 Digital Deskphone layout.

Figure 369: Avaya 3902 Digital Deskphone layout

The Avaya 3902 Digital Deskphone has one-line (DN) capability, and three programmable soft keys (Programmable feature keys) and fixed feature keys (options, message, transfer, goodbye, hold, mute, and volume control).

As there are only three functions assigned to the soft keys, the Shift key does not appear, and all functions are displayed.

Avaya 3902 Digital Deskphone with feature keys 0 - 3

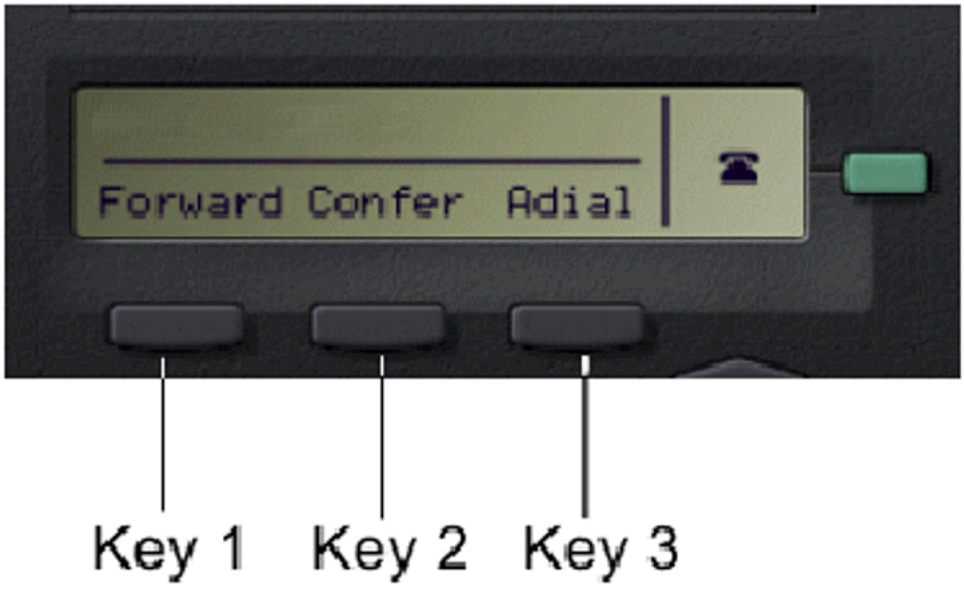


Figure 370: Avaya 3902 Digital Deskphone with feature keys 0 - 3

Avaya 3902 Digital Deskphonewith feature keys 4 - 5

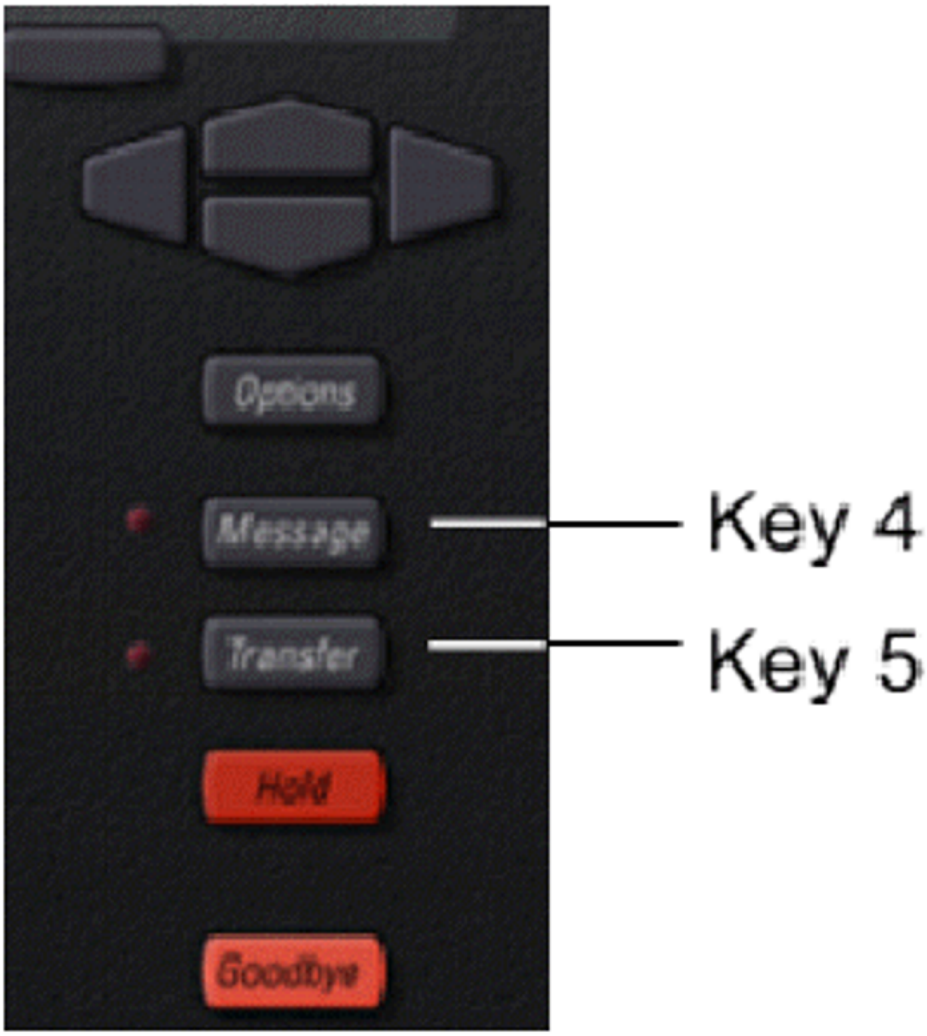


Figure 371: Avaya 3902 Digital Deskphone with feature keys 4 - 5

Avaya 3902 Digital Deskphone Default Key Values

No default key values.

Table 18: Default Keys Value

Key No	Value
4	Transfer (TRN)

Avaya 3903 Digital Deskphone

The following figure shows the Avaya 3903 Digital Deskphone layout.

Figure 372: Avaya 3903 Digital Deskphone Layout.

The Avaya 3903 Digital Deskphone has two programmable line/feature keys (self-labeled) which have two layers each, permitting access to four line/feature keys.

There are four interactive soft keys (self-labeled) that change functionality depending on the features available or the application in use.

Use the More soft key to navigate through the layers of functions.

Avaya 3903 Digital Deskphone with feature keys 0 - 1 and soft keys 17 - 19

Figure 373: Avaya 3903 Digital Deskphone with feature keys 0 - 1 and soft keys 17 - 19

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will be only 1 layer of soft keys containing keys 17 — 20 and there will be no More key.

The message key is numbered 16. Key numbers 17 — 31 are the four soft key labels below the display area. Keys 27 — 31 are reserved for future feature implementation.

Avaya 3903 Digital Deskphone with feature keys 2 - 3

Figure 374: Avaya 3903 Digital Deskphone with feature keys 2 - 3

Use the More key to access soft keys 20 — 22.

Avaya 3903 Digital Deskphone with soft keys 20 - 22

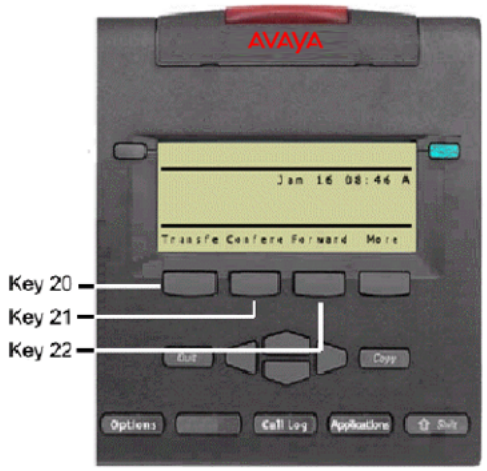


Figure 375: Avaya 3903 Digital Deskphone with soft keys 20 - 22

Press the More key to access soft keys 23 — 25, 26 — 28, and 29 — 31.

Avaya 3903 Digital Deskphone with soft keys 23 - 25

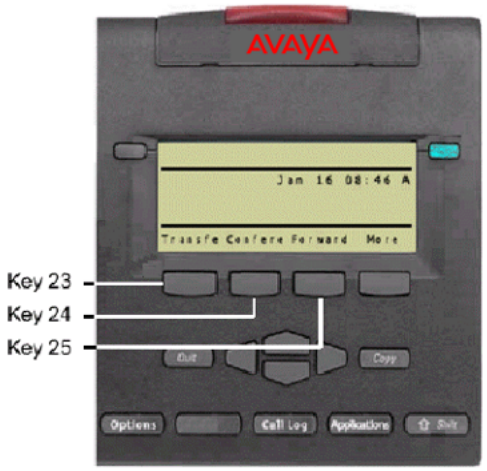


Figure 376: Avaya 3903 Digital Deskphone with soft keys 23 - 25

Avaya 3903 Digital Deskphone with soft keys 26 - 28

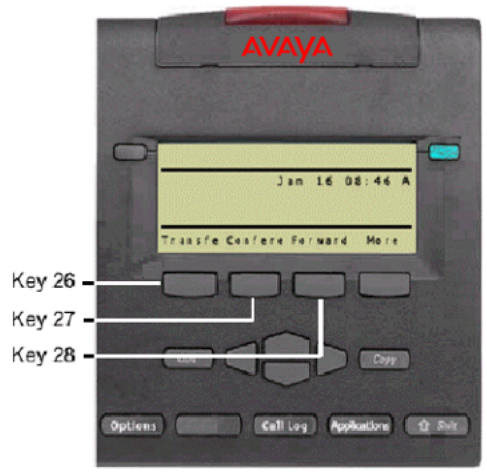


Figure 377: Avaya 3903 Digital Deskphone with soft keys 26 - 28

Avaya 3903 Digital Deskphone with soft keys 29 - 31

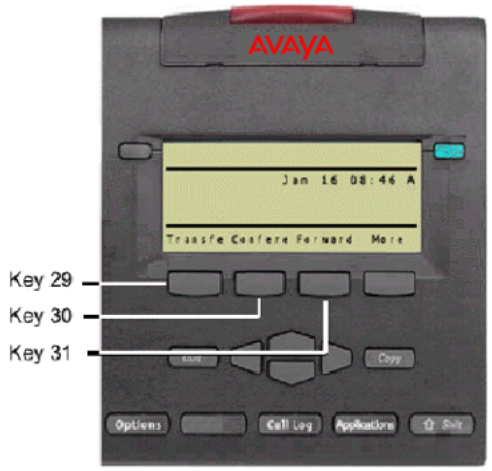


Figure 378: Avaya 3903 Digital Deskphone with soft keys 29 - 31

Avaya 3903 Digital Deskphone Key Values

Table 19: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)

Key No	Value
27	Callers List (CLT)
28	Redial List (RLT)

Avaya 3904 Digital Deskphone

The following figure shows the Avaya 3904 Digital Deskphone layout.

Figure 379: Avaya 3904 Digital Deskphone Layout.

The three keys on both sides of the LCD indicator panel represent two layers of programmable keys. Use the shift key to view and use the second layer of keys.

Use the More soft key to navigate through the layers of functions.

Avaya 3904 Digital Deskphone with feature keys 0 - 5, 16, and soft keys 17 - 19

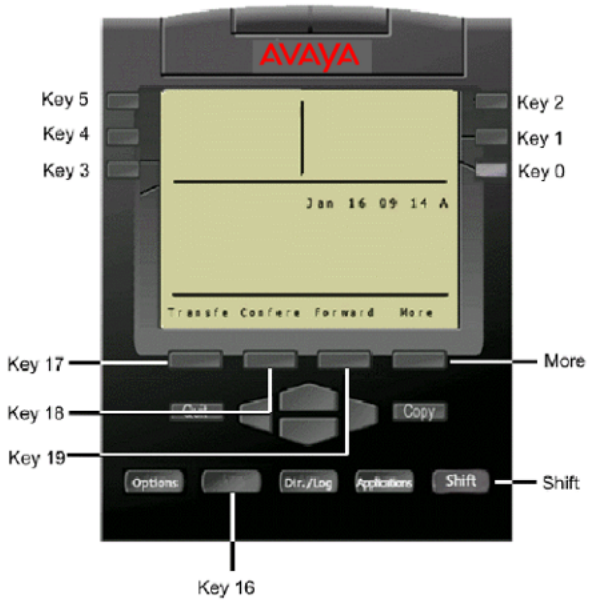


Figure 380: Avaya 3904 Digital Deskphone with feature keys 0 - 5, 16, and soft keys 17 - 19

Use the More soft key to navigate through the layers of functions. If there are only four functions assigned to the soft keys, the More key does not appear and all four functions are displayed. That is, if the soft keys are only defined up to key 20, there will be only 1 layer of soft keys containing keys 17 — 20 and there will be no More key.

Message waiting is not a default feature for key 16. Key numbers 17 — 31 are the four soft key labels below the display area. Keys 27 — 31 are reserved for future feature implementation.

Avaya 3904 Digital Deskphone with feature keys 6 - 11

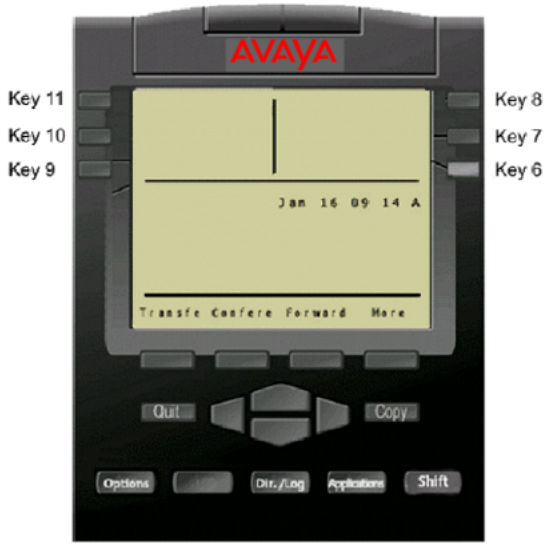


Figure 381: Avaya 3904 Digital Deskphone with feature keys 6 - 11

The Avaya 3904 Digital Deskphone phone can have additional expansion modules, providing up to 55 additional line/feature keys.

DBA 1 contains keys 32 — 55, KBA 1 contains keys 32 — 53, and KBA 2 contains keys 54 - 75.

Avaya 3904 Digital Deskphone DBA 1 with Keys 32 to 39

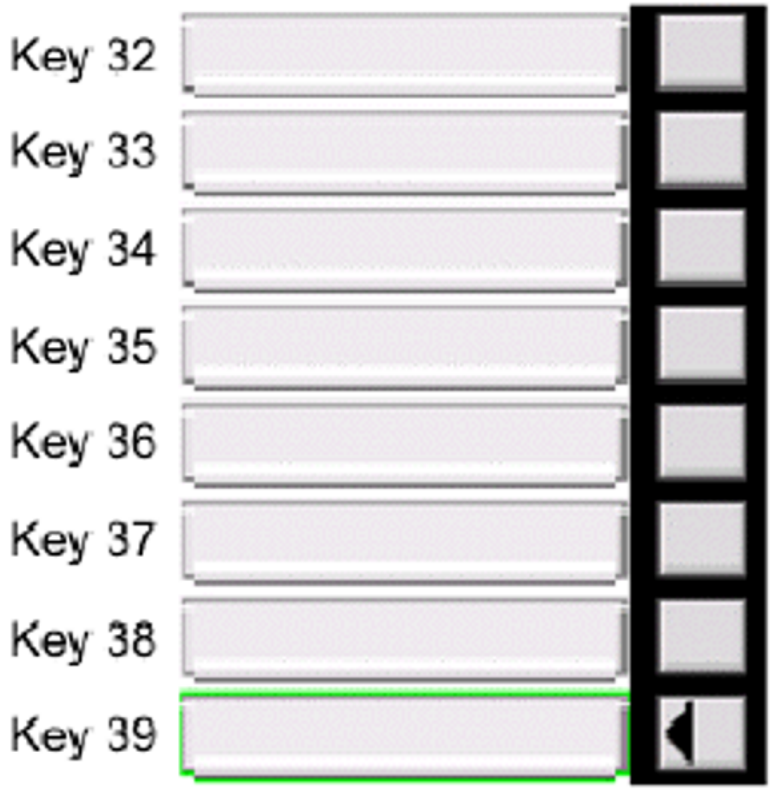


Figure 382: Avaya 3904 Digital Deskphone DBA 1 with Keys 32 to 39

Avaya 3904 Digital Deskphone DBA 1 with Keys 40 - 47

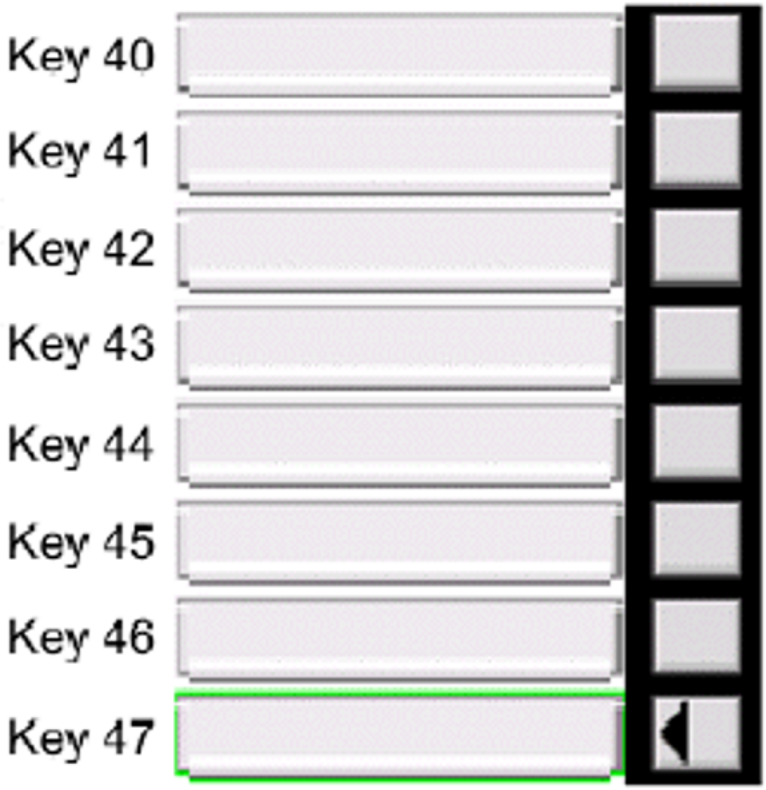


Figure 383: Avaya 3904 Digital Deskphone DBA 1 with Keys 40 - 47

Avaya 3904 Digital Deskphone DBA 1 with Keys 48 - 55

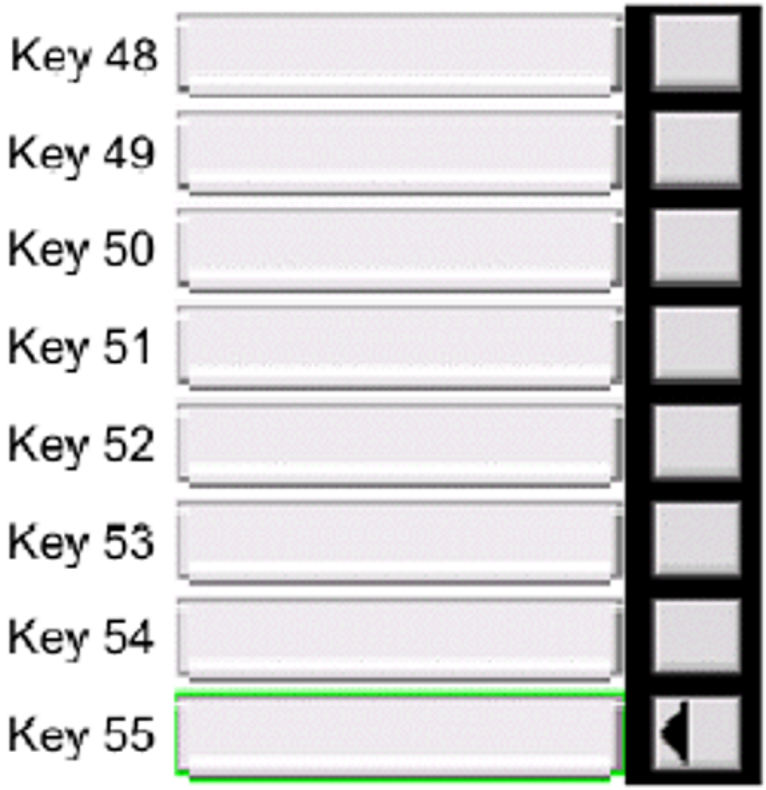


Figure 384: Avaya 3904 Digital Deskphone DBA 1 with Keys 48 - 55

Avaya 3904 Digital Deskphone KBA 1 with Keys 32 to 53

Figure 385: Avaya 3904 Digital Deskphone KBA 1 with Keys 32 to 53

Avaya 3904 Digital Deskphone KBA 2 with Keys 54 - 75

Figure 386: Avaya 3904 Digital Deskphone KBA 2 with Keys 54 - 75

Avaya 3904 Digital Deskphone Default Key Values

Table 20: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)

Key No	Value
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)
27	Callers List (CLT)
28	Redial List (RLT)

Avaya 3905 Digital Deskphone

The following figure shows the Avaya 3905 Digital Deskphone layout.

Figure 387: Avaya 3905 Digital Deskphone Layout.

The Avaya 3905 Digital Deskphone has eight programmable line/feature keys (self-labeled) giving the user access to eight line/feature keys.

There are four interactive soft keys (self-labeled) that change functionality depending on the features available or the application in use.

Use the More soft key to navigate through the layers of functions.

Avaya 3905 Digital Deskphone with Feature Keys 0 - 11 and Soft Keys 16 - 18

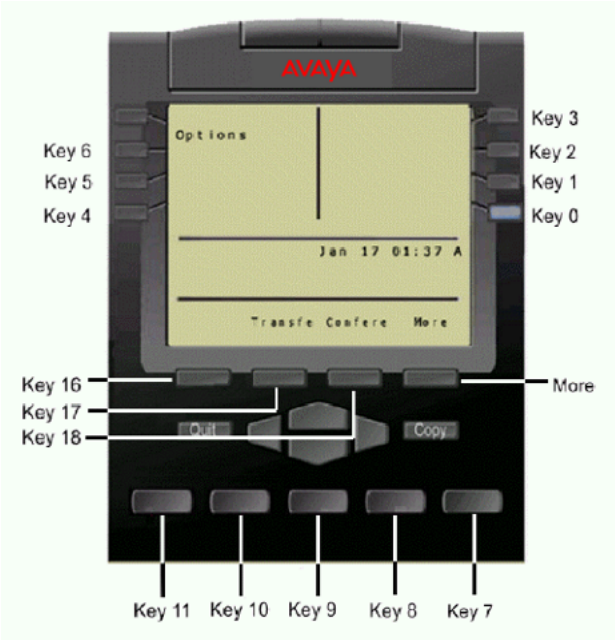


Figure 388: Avaya 3905 Digital Deskphone with Feature Keys 0 - 11 and Soft Keys 16 - 18

Press the More key to access soft keys 19 — 21.

Avaya 3905 Digital Deskphone with Soft Keys 19 - 21

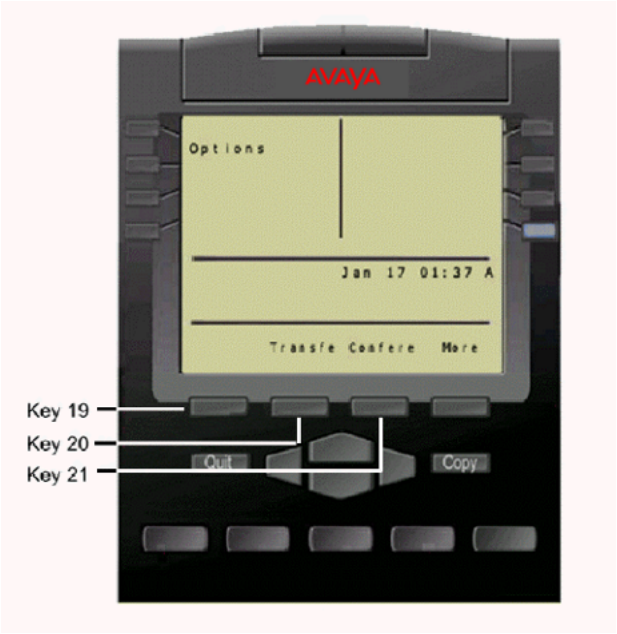


Figure 389: Avaya 3905 Digital Deskphone with Soft Keys 19 - 21

Press the More key to access soft keys 22 — 24, 25 — 27, 28 — 30, and key 31.

Avaya 3905 Digital Deskphone with Soft Keys 22 - 24

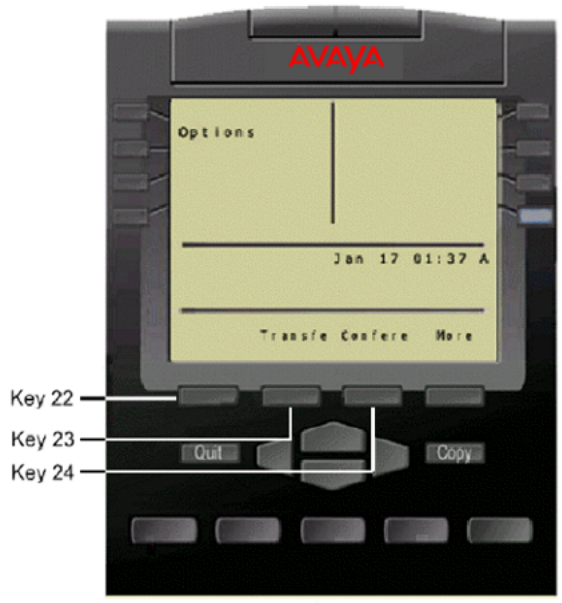


Figure 390: Avaya 3905 Digital Deskphone with Soft Keys 22 - 24

Avaya 3905 Digital Deskphone with Soft Keys 25 - 27

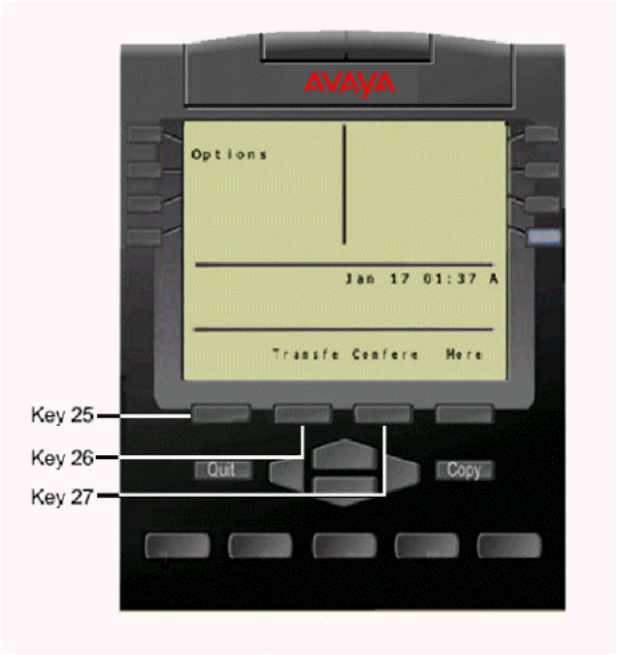


Figure 391: Avaya 3905 Digital Deskphone with Soft Keys 25 - 27

Avaya 3905 Digital Deskphone with Soft Keys 28 - 30

Figure 392: Avaya 3905 Digital Deskphone with Soft Keys 28 - 30

Avaya 3905 Digital Deskphone with Soft Key 31

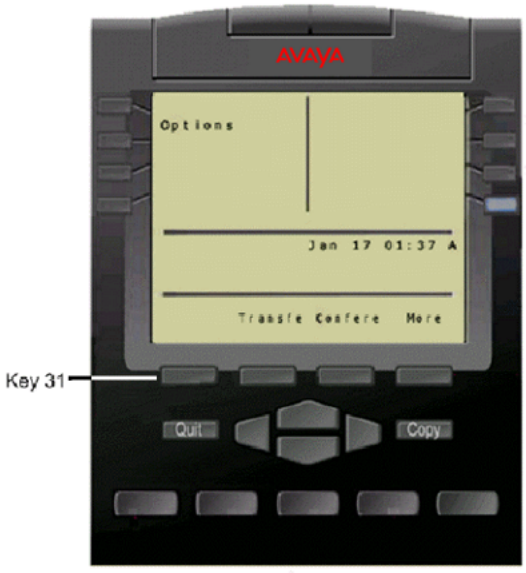


Figure 393: Avaya 3905 Digital Deskphone with Soft Key 31

DBA 1 contains keys 32 — 55, KBA 1 contains keys 32 — 53, and KBA 2 contains keys 54 - 75.

Avaya 3905 Digital Deskphone DBA 1 with Keys 32 - 39

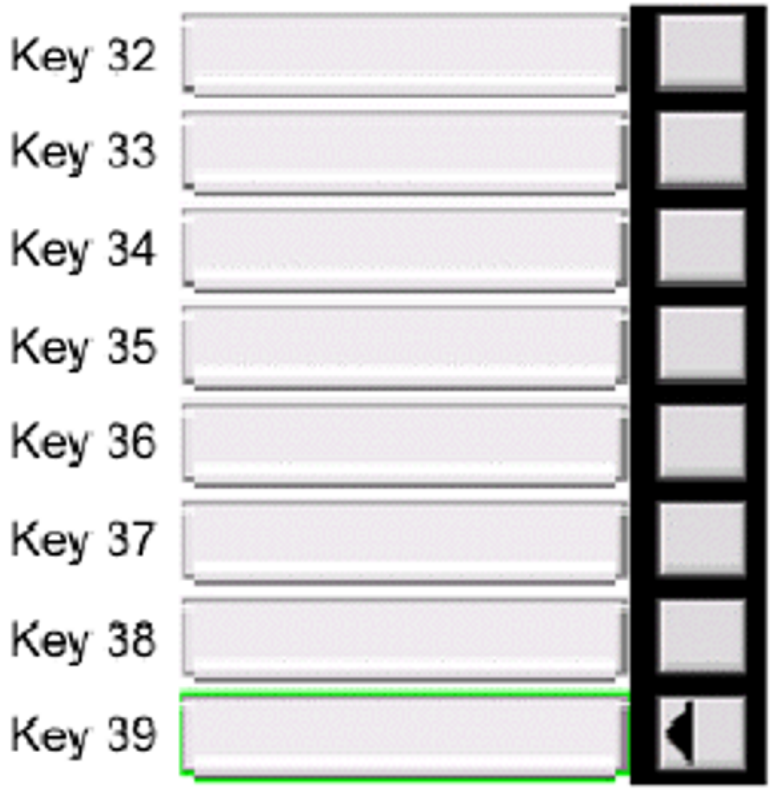


Figure 394: Avaya 3905 Digital Deskphone DBA 1 with Keys 32 - 39

Avaya 3905 Digital Deskphone DBA 1 with Keys 40 - 47

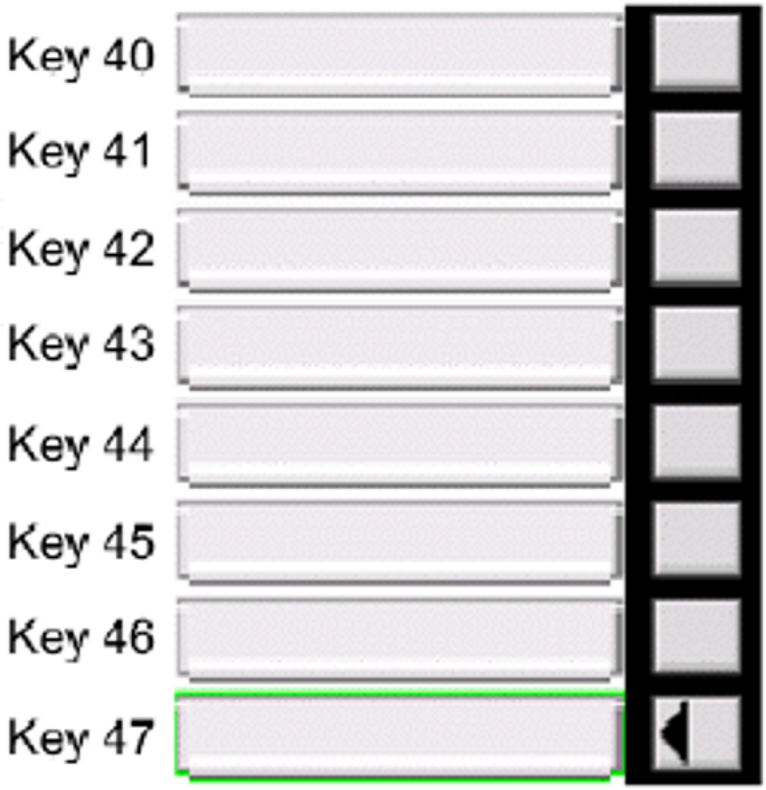


Figure 395: Avaya 3905 Digital Deskphone DBA 1 with Keys 40 - 47

Avaya 3905 Digital Deskphone DBA 1 with Keys 48 - 55

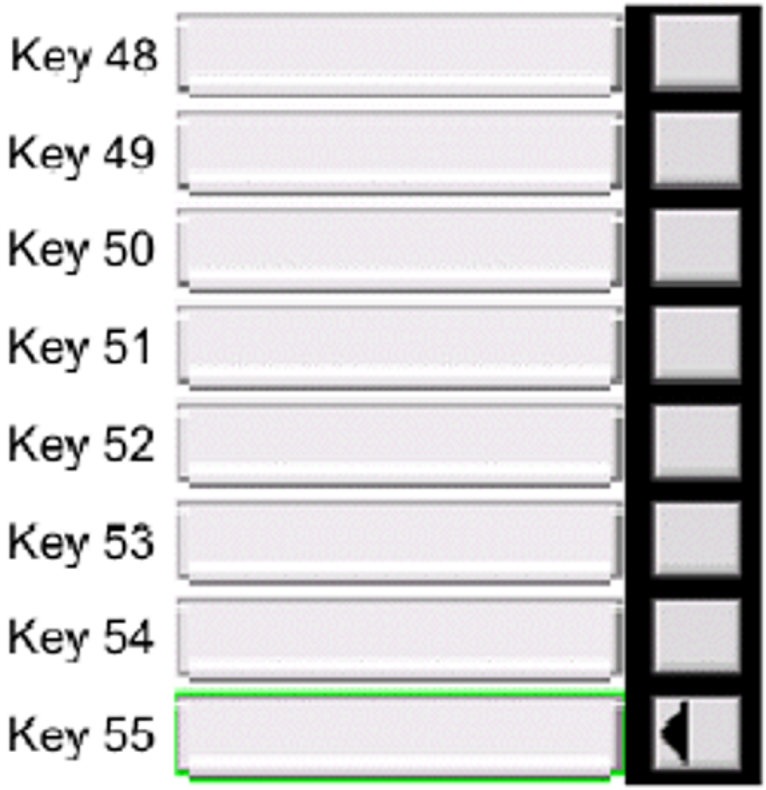


Figure 396: Avaya 3905 Digital Deskphone DBA 1 with Keys 48 - 55

Avaya 3905 Digital Deskphone KBA 1 with Keys 32 - 53

Figure 397: Avaya 3905 Digital Deskphone KBA 1 with Keys 32 - 53

Avaya 3905 Digital Deskphone KBA 2 with Keys 54 - 75

Figure 398: Avaya 3905 Digital Deskphone KBA 2 with Keys 54 - 75

Avaya 3905 Digital Deskphone Default Key Values

Table 21: Default Keys Value

Key No	Value
16	Message Waiting (MWK)
17	Call Transfer (TRN)
18	Party Conference (A06)
19	Forward All Calls (CFW)
20	Ring Again (RGA)

Key No	Value
21	Call Park (PRK)
22	Ringing Number Pick-up (RNP)
24	Privacy Release (PRS)
25	Charge Account (CHG)
26	Calling Party Number (CPN)
27	Callers List (CLT)
28	Redial List (RLT)

Index

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

X

Z