ShoreTel®
UNIVERSITY

RELEASE NOTES

ShoreTel 9
ShoreWare Server
Release Notes

RELEASE 9

Document and Software Copyrights

Trademarks

Patents

Version Information

Company Information

Table of Contents

System Parameters

System Specifications

Hardware and Software Requirements

Server Device Requirements

Operating Systems

ShoreWare Version 9 server software is supported on the following operating systems:

- Windows Server 2003 SP2 (Standard or Enterprise)

    ShoreWare Version 9 is not supported on Windows 2003 SP1

- Windows Server 2003 R2 Enterprise Edition, 32-bit (Standard or Enterprise)

ShoreWare is supported only on 32-bit operating systems. There is no 64-bit support.

Server Hardware Requirements

Table 1 displays the minimum recommended configuration for servers running ShoreWare Main Server software. Sound card, speakers, and microphone are recommended for all configurations.

Users	Calls/Hour	Pentium Processor	RAM	Network
100	1,000	E2160 / Single DualCore 1.8 GHz	1 GB	100 Base-T
500	5,000	Xeon 3050 / Single DualCore 2.13 GHz	2 GB	100 Base-T
1,000	10,000	Xeon 3070, 5150 / Single DualCore 2.66 GHz	3 GB	100 Base-T or Gigabit Ethernet
2,500	25,000	Xeon 3220 / Single QuadCore 2.4 GHz	4 GB	100 Base-T or Gigabit Ethernet
5,000	50,000	Xeon 3230 / Single QuadCore 2.66 GHz	4 GB	100 Base-T or Gigabit Ethernet
10,000	50,000	Xeon 5365 / Single QuadCore 3.0 GHz	4 GB	100 Base-T or Gigabit Ethernet

Table 1   Main Server Hardware Requirements

Table 2 displays the minimum recommended configuration for servers running ShoreWare Distributed Server software.

Users	Calls/Hour	Pentium Processor	RAM	Network
100	1,000	E2160 / Single Dual-Core 1.8 GHz	1 GB	100 Base-T
500	5,000	Xeon 3050 / Single Dual-Core 2.13 GHz	2 GB	100 Base-T
1,000	10,000	Xeon 3070, 5150 / Single Dual-Core 2.66 GHz	3 GB	100 Base-T or Gigabit Ethernet
Contact Center and Enterprise Contact Center Support Requirements – Refer to Contact Center Documentation				

Table 2   Distributed Server Hardware Requirements

To maintain high server performance and reliability, ShoreTel recommends Gigabit Ethernet Interface for all configurations regardless of the number of users or network load. Although the 100 Base-T interface can provide acceptable performance and reliability for the specified configurations, administrator intervention is more frequently required to properly configure the IP network and prioritize real-time information during the peak network traffic conditions.

SBE Hardware Requirements

Table 3 displays the recommended configuration for servers running SBE software.

Users	Calls/Hour	Processor	RAM	Network
50	500	Celeron D – 3.0 GHz	1 GB	100 Base-T

Table 3   SBE Hardware Requirements

Client Device Requirements

Operating Systems

The Version 9 client software is supported on the following operating systems:

- Windows Client Operating System

    — Windows XP Professional SP3 – 32-bit
    — Windows Vista, Business Edition, SP1 – 32-bit

- Windows Terminal Server

    — Windows 2003 SP2 Terminal Server – 32- or 64-bit
    — Windows 2003 R2 Terminal Server – 32- or 64-bit

- Citrix

    For current information about support for specific Citrix versions and Call Manager features supported on the Citrix platform, refer to the Citrix product bulletin, available at

    https://login.shoretel.com/?src=s&ReturnUrl=%2falerts%2fdownloads%2f2008-06-04.pdf

Client Hardware Requirements

Computer Hardware requirements for running Call Manager depend on the Call Manager version and the video call resolution. Table 4 displays the minimum recommended configuration for computers running ShoreWare Call Manager.

Call Manager Version	Processor	RAM[a]		Disk[b]	
		XP	Vista	XP	Vista
Personal	Pentium 3 – 800 MHz	100 MB	100 MB	1 GB	1 GB
Professional	Pentium 4 – 2.0 GHz	150 MB	150 MB	1 GB	1 GB
Agent, Supervisor, Operator (<40 extension presences)	Pentium 4 – 2.0 GHz	150 MB	150 MB	1 GB	1 GB
Agent, Supervisor, Operator (<500 extension presences)	Pentium 4 – 3.0 GHz	150 MB	150 MB	1 GB	1 GB
All Versions, VGA Video	Dual-Core 1.6 GHz	150 MB	150 MB	1 GB	1 GB
All Versions, XGA Video	Core 2 Quad 2.4 GHz	150 MB	150 MB	1 GB	1 GB

Table 4   Client Device Hardware Requirements

a. Lists Call Manager memory requirements during normal operation. When running other office applications on the PC in addition to Call Manager, memory recommendations are 512 MB (XP) or 1 GB (Vista).

b. Disk space requirement is for installation on a system without .NET Framework installed previously. Once installed, Call Manager requires less than 100MB of disk space.

Video Bandwidth Requirements

Video calls require the following bandwidth:

- **VGA**: 600 kbps
- **XGA**: 1.2 Mbps

Video Hardware Requirements

Computers configured for video calls require the following:

- **VGA Video**: Graphic Card with 64 MB of VRAM, DirectX 9.0c-compatible
- **XGA Video**: Graphic Card with 256 MB of VRAM, DirectX 9.0c-compatible

Director and ShoreWare Web Access Requirements

Director and ShoreWare Web Access require one of the following internet browsers:

- MS Internet Explorer 6.0, SP2
- MS Internet Explorer 7.0

Supported Devices

ShoreGear Switches

Version 9 supports the following ShoreGear Voice Switches:

- ShoreGear 50
- ShoreGear 50V
- ShoreGear 90
- ShoreGear 90V
- ShoreGear 90BRI
- ShoreGear 90BRIV
- ShoreGear 220T1
- ShoreGear 220E1
- ShoreGear 220T1A
- ShoreGear 30
- ShoreGear 30BRI
- ShoreGear 24A
- ShoreGear T1k
- ShoreGear E1k
- ShoreGear 120
- ShoreGear 60
- ShoreGear 40
- ShoreGear T1
- ShoreGear E1

ShorePhone Telephones

Version 9 supports the following ShorePhone Telephones

- IP565

- IP560g
- IP560
- IP530
- IP265
- IP230g
- IP230
- IP212k
- IP115
- IP110
- IP8000
- AP110
- AP100

Upgrade Paths and Application Support

Upgrade Path

ShoreTel supports single step upgrades to Version 9 from Version 8.1 and Version 7.5

ShoreTel supports upgrade paths from other versions through an intermediate upgrade to either Version 7.5 or Version 8.1.

Email Integration

The Version 9 Client application supports email integration with the following products:

- Outlook 2003, SP2
- Outlook 2007

When running on Citrix, Call Manager does not import Outlook contacts if Outlook is in seamless mode. To import contacts, user must close Outlook seamless window and either start Call Manager or click the **Import Contact** button.

Version 9 discontinues support for integrating email with Outlook 2002.

Converged Conferencing

Version 9 supports interoperability for Converged Conferencing 7.1 and above.

Contact Center

Version 9 supports interoperability for Contact Center 4.66.05 and above.

SIP-BRI 8

Version 9 supports interoperability for SIP-BRI 8 Build R3.T_2006-10-04 and above.

SIP Devices

Version 9 supports the following SIP devices as SIP extensions:

- IP8000

Character Sets

This version of ShoreWare supports only ISO 8859-1, also known as Latin -1 or Microsoft Windows CP1252 character set (see http://www.microsoft.com/globaldev/reference/sbcs/1252.mspx/ for supported character set). This set consists of characters from the Latin script. This character encoding is used throughout the Americas, Western Europe, Oceania, and much of Africa.

It is also commonly used in most standard Romanizations of East-Asian languages. Certain characters in Central\Eastern Europe, Baltic languages, Cyrillic, Arabic, Greek are displayed as "?" if the character encoding is not found. Double-byte characters, such as those found in Chinese, Japanese and Korean languages, are also not supported and displayed as"?". System directory entries, imported Outlook Contacts or other user-generated entries (i.e., IM contacts) should use Latin-1 encoding to ensure all characters are displayed properly.

Codecs

Version 9 supports the following codecs:

- L16/16000
- L16/8000
- AAC_LC/32000
- PCMU/8000
- PCMA/8000 (G.711)
- G722/8000
- DVI4/8000
- BV32/16000
- BV16/8000
- G729/8000

System Capacity

Version 9 supports the following:

- **Users**

  — 10,000 users if DRS is enabled.
  — 1,000 users if DRS is not enabled.

- **ShoreGear Switches**

  — 60 switches per site if DRS is not enabled.
  — 500 switches per site if DRS is enabled.

- **ShoreGear Voicemail Model Switches**

  — 50 Voicemail Model switches per site
  — 100 Voicemail Model switches per system.

- **Servers**

- — One main server.
- — 20 distributed servers.

- **IP Phones**

  - — 5 ShorePhones per ShoreGear port.
  - — 100 SIP Proxies per ShoreGear port.

- **Desktop Clients**

  - — 10,000 Call Manager instances per system.
  - — 1,000 Call Manager instances per server.
  - — 100 Call Manager instances per WTS (64-bit) server[1]
  - — 200 operator clients per system.
  - — 500 monitored extensions per client.
  - — 5000 monitored extensions per system.

- **Make-me Conferencing**

  - — One conferenced party per ShoreGear port.

- **Voice Mail**

  - — 10,000 mailboxes per system.
  - — 3,000 mailboxes per server.
  - — 254 simultaneous calls per server.

- **Workgroups**

  - — 256 workgroups.
  - — 300 agents per workgroup.
  - — 16 agents per workgroup when simultaneous hunt is enabled.
  - — 500 agents per system.
  - — 128 supervisors per system.

- **Call Volume**

  - — 5,000 BHCA.

- **CDR Size**

  - — Not restricted by ShoreWare.

---

1. Assumes WTS server running on Core 2 Quad 2.4 GHz with 16 GB RAM.

ShoreTel®

System Features

Active Directory

Introduction

ShoreTel 9 integrates Active Directory with the ShoreTel directory to provide the following functions:

- Bulk Import of user accounts
- Synchronize ShoreTel user accounts with Active Directory user records
- Authentication of Active Directory users

Active Directory compliant directories centrally stores information for all users, computers, and other entities. This feature adds the capacity to provision and authenticate user accounts that are generated and maintained by other applications.

Refer to the Glossary for a definition of the following terms used in this release note:

- Active Directory (AD)
- DBImport
- Explicit Authentication
- Lightweight Directory Access Protocol (LDAP)
- LDAPExport
- Single Sign On (SSO)

Description

Directory services store organization information and settings in a central, organized, accessible database. LDAP is the protocol used for exchanging information between client applications and the serving directory. An LDAP directory allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization.

Active Directory (AD) is the Microsoft application that implements LDAP on Windows based systems. AD is widely deployed among large enterprises.

The ShoreTel AD implementation supports the synchronization of user records between the ShoreTel database and other applications using AD on Windows based networks.

ShoreTel AD includes the following features:

- Authentication of AD Users, as described in Authenticating AD Users on page 22.

- Synchronizing AD Directory and ShoreTel Director user records, as described in Synchronizing AD and Director User Records on page 25.

- Bulk Provisioning of User Accounts, as described in Bulk Provisioning of User Accounts on page 26.

Active Directory Implementation

Active Directory Integration is an optional ShoreTel feature that is disabled by default. Systems that disable AD Integration do not recognize links to the Active Directory for AD properties attached to system users and do not provide AD authentication, synchronization, or provisioning services.

When AD Integration is enabled, only users that have Administrative Permissions can log into Director. This requires the explicit definition of at least one administrator role and the assignment of users requiring Director access to an administrative role.

Enabling AD Integration on a ShoreTel System

AD is enabled from the *Edit Other System Parameters* panel, as shown in Figure 1, is accessed through ShoreWare Director by selecting *Administration -> System Parameters -> Other*.

To enable AD, select *Enable AD Integration* located at the bottom of the panel, then enter the Active Directory path in the data entry field.

Figure 1   Enabling Active Directory

IMPORTANT   Since AD prevents anonymous users from logging in through the default administrator account, the *default Director access method (admin/changeme) is not available when AD is enabled*. At least one user must be assigned Administrative rights before enabling AD.

Configuring AD on a New System provides a procedure that includes required user and administrative assignment steps for enabling Active Directory on a newly installed ShoreTel system.

Configuring AD on a New System

The following procedure enables AD Integration on a new system including the initial user configuration and assignment of administrative permissions:

Step 1 Login to an Active Directory account through which ShoreWare Director will be accessed.

Step 2 Access ShoreWare Director by entering the following parameters:

username – admin
password – changeme

Step 3 Add a user to the ShoreTel system with a *Client User ID* name that matches the Active Directory login name.

To add a system user, select *Administration -> Users -> Individual Users* from the Main Menu. Refer to the ShoreTel Administration Guide for more information.

Step 4 Assign Administrative Rights to the new user account.

To assign rights, press the New button in the Administrators List panel that is accessed by selecting *Administration -> System Parameters -> Administrative Permissions -> Administrators* panel. Refer to the ShoreTel Administration Guide for more information.

Step 5 Open the *System Parameters: Edit Other Parameters* panel by selecting *Administration -> System Parameters -> Other* from the Director Main Menu Login, as shown in Figure 1.

Step 6 Select *Enable AD Integration* located at the bottom of the panel, then enter a valid AD path in the **AD Path** data entry field.

Step 7 When prompted to save your changes and close the window, press the **OK** button and *Yes* option.

This step logs you out of Director

Step 8 Log into Director again, using the username created in Step 3.

The default password is changeme.

Step 9 Open the Edit User panel for the new user and enable Active Directory for that user, including the domain and user ID for the user.

Step 10 Log out of ShoreWare Director and close the window.

Subsequent ShoreWare Director launches when logged on to the domain through this username will automatically log into Director.

Mapping Active Directory Attributes to ShoreTel Fields

ShoreTel user records contain eleven data fields that map directly to Active Directory records. The following is a list of these data fields, categorized by the Director panel that sets their ShoreTel value.

Edit User panel

- *First Name*: Active Directory field capacity is 64 characters; ShoreTel capacity is 50.
- *Last Name*: Active Directory field capacity is 64 characters; ShoreTel capacity is 50.
- *Number*: ShoreTel extracts the number of digits specified by the extension length, starting from the right side of the AD phone number.
- *DID*
- *Email Address*
- *Client User ID*: Active Directory length is limited to 20 characters.

System Directory

- *Home Phone*
- *Pager*
- *Cell Phone*
- *Fax Phone*

ShoreTel Database (does not appear in Director)

- *LDAP-GUID*: Used internally by the ShoreTel system when performing subsequent user updates from the AD database.

Authenticating AD Users

ShoreTel supports AD authentication for users logging into Call Manager, Web Client, and Director, permitting access to these programs without providing the ShoreWare username or password.

- AD Users logging into Director and Call Manager are authenticated through Single Sign On (SSO) with their current network credentials. Users are not required to re-enter their credentials to access these applications.

- AD users logging into Web Client are authenticated through Explicit Authentication, which requires re-entry of their credentials each time they access the application.

Director

When AD Integration is enabled, user access to ShoreWare Director is restricted as follows:

- only users with a domain account can log into Director
- only users with administrative permissions can log into Director
- users do not need to be logged into their domain account to access Director
- users do not need their ShoreTel account configured for Active Directory (AD Users) to access Director

The following sections describe Director access scenarios.

AD User Logged into the Domain

Users configured for AD within ShoreWare that are logged into the domain network are directed to the Director Quick Look panel when they attempt to access Director without entering their network credentials.

Upon logging off from Director, the browser displays a ShoreWare entry panel that allows Director access by pressing a button, as shown in Figure 2.
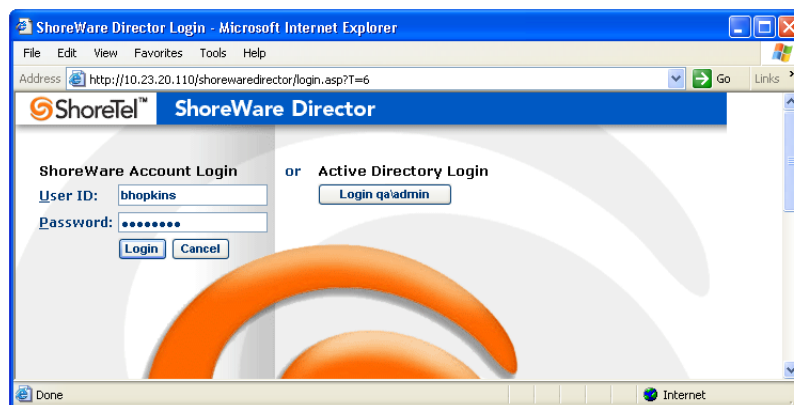
Figure 2 **Director Login panel – AD user**

Non-AD User Logged into the domain

Users that are not configured for AD within ShoreWare that are logged into the domain network are directed to a Director Login panel, as shown in Figure 3. Users access Director from this panel by entering their ShoreTel username and password in the respective data fields.
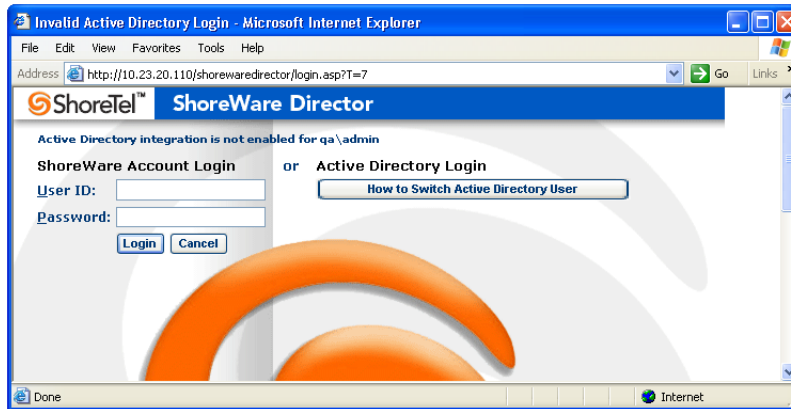
Figure 3   Director Logon panel – Non-AD user

Users not logged into the domain

Users attempting to access Director without first logging into the domain network are initially routed to a domain login panel, as shown in Figure 4. After entering their network credentials, users are routed to the appropriate panel – AD users are routed to the Quick Look panel and Non-AD users are directed to a login panel.

Figure 4   Domain Login Panel

Call Manager

When AD Integration is enabled, access to Call Manager is available to all system users, including users without domain accounts or not configured as ShoreTel AD users.

Initial Configuration

When installing Call Manager, users authenticated through AD are not queried for their credentials; they are immediately prompted for the server name after which wizard panels guide them through the setup process.

Users that are not authenticated through AD are required to enter their name, password and server name. After verifying the user's credentials, Call Manager guides the user through the setup process.

Logging into Call Manager

Attempts to log into Call Manager after the initial setup are handled on the basis of the user's AD configuration. Active Directory users are authenticated by SSO through the verification of their AD credentials. Users not configured for Active Directory are authenticated through the verification of their ShoreTel username and password, as previously loaded through their Call Manager account. In either case, users are typically not required to re-enter their username or password each time they open Call Manager from their computer.

Call Manager behavior when authentication fails is not changed by this feature.

User Name – Telephony Options panel

The User Name data field at the top of the Options and Preferences: Telephony panel displays the user name of the Call Manager account. This field is *read only* for users authenticated through AD credentials, as shown in Figure 5.
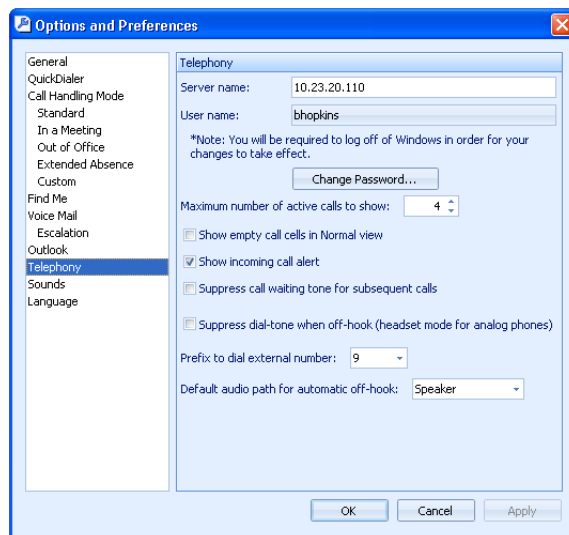
Figure 5   Options and Preferences: Telephony panel

Web Client

When AD Integration is enabled, access to the Web Client is available to all users, including users without domain accounts or not configured as ShoreTel AD users.

Attempts to log into Web Client always require the user to enter credential information. Domain members configured as ShoreTel Active Directory members enter their Active Directory user name and password and are authorized through Explicit Authentication. All other users enter their ShoreTel username and password.

Synchronizing AD and Director User Records

Director provides an interface for adding, updating, and deleting AD users from the ShoreTel database. Synchronization is performed on individual users and does not affect the AD directory.[1]

Enabling AD for a ShoreTel User

When AD Integration is enabled, the first parameter on the **Edit User: General** panel enables Active Directory for the user, as shown in Figure 6.

To enable Active Directory for a user, enable the Active Directory User option at the top of the panel, then enter the domain\user name for the user, as shown in Figure 6.

Figure 6   **Enabling Active Directory for a User**

Updating AD Fields

Active Directory users can synchronize user account records with contents from the Active Directory database by pressing the *Sync from AD* button located left of the user's Active Directory user ID. Pressing the *Show From AD* button displays parameter settings for the user's Active Directory account.

The *Show From AD* and *Sync From AD* buttons are inactive for users accessing this panel that are not configured as AD users.

Removing AD Users

When an administrator attempts to delete a user with an AD account, ShoreWare displays a warning message and requires confirmation before removing the record from the ShoreTel database.

---

1. The authentication process is defined between the computer running the HQ server and the computer hosting Active Directory. Authenticating AD records from a different computer involves *Delegation*, which is defined by Microsoft as a process where a trusted account impersonates the account that has AD access permission – in this case, from the computer hosting the HQ server.

   Authentication Delegation is available in most ShoreTel configurations, allowing AD queries through the Edit User panel from any computer running Director. If a problem arises when attempting to access AD information through the Edit User panel from a remote device, access Director through an intranet URL from the computer hosting the Headquarters Server software.

   For more information about Authentication Delegation, refer to Microsoft technical software.

Bulk Provisioning of User Accounts

ShoreTel supports the bulk provisioning of user accounts from AD records through a two step process:

Step 1 Export AD records to a CSV file.

Exporting AD Records describes this step.

Step 2 Import CSV records to the ShoreTel user database.

Importing the CSV File on page 27 describes this step.

Exporting AD Records

ShoreTel provides a VBScript file to export data records from an Active Directory database to a CSV file. The VBScript file can be used as a template for specific ShoreTel system requirements.

The parameter section of the file is shown in Figure 7. This section consist of two subsections:

Figure 7   **Sample ldaptocsv.vbs file – parameter sections**

- The top section receives values from the AD database for each imported file. As indicated in the comments section, one value can be assigned to individual fields for all users by entering the value in place of the quotes.

- The bottom section is a data template containing non-AD fields that are saved to the CSV file. The values entered in these fields are assigned to all records retrieved from the AD database.

The following command line executes the AD to CSV file import:

cscript ldaptocsv.vbs *outputCSVfile LDAPpath [modifiedInLastN#OfDays]*

where

outputCSVfile specifies the name of the output file
LDAPpath specifies the path to the AD database
[modifiedInLastN#OfDays]

The resulting CSV file can be modified though a spreadsheet program to customize user settings for import to the ShoreTel database.

Importing the CSV File

DBImport.exe is a executable file that imports CSV contents to the ShoreTel database that was introduced in a previous ShoreWare release and described in the ShoreTel Administrator Guide.

To support AD record imports, the following fields are supported by DBImport.exe:

- **LDAP-User flag**: indicates that the user settings were imported from an AD database.

- **LDAP-GUID**: a data field that creates an association between an LDAP record and the corresponding ShoreTel record.

- **LDAP-DomainName**: specifies the name of the user's domain network.

The following command line imports CSV file records to the ShoreTel database.

Dbimport -log DbLog.log -err DbErr.err <inputCSVfile>

LLDP / 802.1x

Introduction

Version 9 enhances ShorePhones to support LLDP-MED and 802.1x.

The *Link Layer Discovery Protocol-Media Endpoint Discovery* (LLDP-MED) is an enhancement to the Link Layer Discovery Protocol (LLDP) that addresses the following:

- Device location discovery to support location databases and VoIP E911 services.
- Auto-discovery of LAN policies to support "plug and play" networking.
- Extended and automated power management of PoE endpoints.
- Inventory management.

A component of IEEE 802.1 group of networking protocols, 802.1x addresses port-based Network Access Control. It provides an authentication mechanism for devices attaching to a LAN port to either establish a point-to-point connection or prevent the device from accessing the port if authentication fails. 802.1x is based on the Extensible Authentication Protocol (EAP).

Refer to the Glossary for a definition of the following terms used in this release note:

- 802.1x
- LLDP-MED

LLDP-MED

LLDP-MED, an enhancement to the basic LLDP protocol, addresses the discovery of endpoints by networks supporting LLDP.

Implementing LLDP-MED requires LLDP-MED capable network switches. ShorePhones IP110 and IP210 do not support LLDP-MED.

Feature Description

ShorePhones that are updated to ShoreTel 9 comply with all mandatory TIA-1057 LLDP-Med functionality for Class III Communications Device Endpoints and selected optional capabilities or limitations.

Implementation

ShoreTel changes that support LLDP-MED implementation include the following:

- Definition of a new telephone parameter – LldpEnable

  LldpEnable is a one character ASCII parameter. Valid settings for LldpEnable are 0 and 1:

  — LldpEnable = 1 (LLDP is enabled)
  — LldpEnable = 0 (LLDP is disabled)

  Default value is 1 (enabled)

- Modify Setup Source Preferences

  When setting up ShorePhones, parameter settings are obtained from the following sources, listed in order of highest to lowest precedence:

— Config File
— DHCP (if active)
— LLDP (if active)
— Setup Command
— Default values

802.1x

A component of IEEE 802.1 group of networking protocols, 802.1x addresses port-based Network Access Control. It provides an authentication mechanism for devices attaching to a LAN port to either establish a point-to-point connection or prevent the device from accessing the port if authentication fails. 802.1x is based on the Extensible Authentication Protocol (EAP).

ShorePhones IP110 and IP210 do not support 802.1x.

Feature Description

ShorePhones that are updated to ShoreTel 9 comply with all mandatory 802.1x functionality for Class III Communications Device Endpoints and selected optional capabilities or limitations.

If 802.1x is enabled on the ShorePhone and disabled on the Network switch, the ShorePhone never comes up.

Implementation

ShoreTel changes that support IEEE 802.1x implementation include:

• Definition of a new telephone parameter – 802.1xEnable

  802.1xEnable is a one character ASCII parameter. Valid settings for 802.1xEnable are 0 and 1:

  — 802.1xEnable = 1 (802.1 authentication is enabled)
  — 802.1xEnable = 0 (802.1 authentication is disabled)

    Default value is 0 (disabled)

Unicode Character Set Support

Introduction

Feature Description

ShoreTel 9 supports Unicode Character sets by incorporating the v5.1 MySQL ODBC connector, resulting in databases that support Unicode Character sets. ShoreTel 9 does not localize any ShoreTel application, including Director, not localized in a previous version.

Support of Unicode Character sets extends to the ShoreTel system and CDR databases.

Refer to the Glossary for a definition of the following terms used in this release note:

- Call Detail Record (CDR)
- CDR Database
- MySQL
- ODBC
- ODBC Connectors
- System Database

Implementation

ShoreTel 9 implements this feature through the following:

- Changing MySQL ODBC connector version to v5.1.

  V5.1 supports Unicode for Windows Server and Linux Server.

- Changing CDR reports to use *ArialUnicode For ST* font.

  Font changes require the appropriate authorization on the computer where they are installed or removed.

Usage Information

Ascender Corporation provides four font files (Arial Unicode for ShoreTel, Arial Unicode for ShoreTel Bold, Arial Unicode for ShoreTel Italics, and Arial Unicode for ShoreTel Bold Italics) for three languages: Japanese, Simplified Chinese, and Traditional Chinese. Only one set of files – supporting one language – can be installed on a computer at any time.

To install a font on a machine where web reports are required, **perform the following:**

Step 1 Open the Edit Reporting Options panel by selecting *Reporting -> Options* from the Directory Main Menu.

Figure 8 displays the Edit Reporting Options panel.

Step 2 Select the desired language from the Select Language Variant drop-down menu.

Step 3 Press the Install Fonts button.

ShoreTel installs the requested font set on the computer.

Figure 8   **Reporting Options panel**

Chinese Traditional font is installed on the Headquarters server by default. Access reports from a client machine or using a different Asian font requires a font installation through the Reporting Options panel.

SRTP-AES

Introduction

Definition

ShoreTel 9 supports SRTP for encrypting, authenticating, and replaying media streams for ShoreGear switches and ShorePhones that support encryption. Implementation details include the following:

- Media streams support of the AES algorithm

- ShorePhone and ShoreGear support of government certified AES

- All SRTP mandatory features:

  — Support AES in Counter Mode at 128-bit
  — Support key derivation rate (KDR) at 0
  — Do not support AES in F8 Mode
  — Do not support Master Key Identification (MKI)

Refer to the Glossary for a definition of the following terms used in this release note:

- Advanced Encryption Standard (AES)
- Real-time Transport Control Protocol (RTCP)
- Real-time Transport Protocol (RTP)
- Secure Real-Time Transport Protocol (SRTP)
- Session Description Protocol (SDP)

History

ShoreWare 6 introduced a proprietary 64-bit encryption algorithm for protecting media streams between ShoreTel devices, including ShoreGear switches and ShorePhones. ShoreWare encrypts RTP (payload) packets within the ShoreWare network. Call control packets are not encrypted.

ShoreWare 8 introduced a 128-bit proprietary algorithm that replaced the 64-bit version.

Background

AES is a United States Encryption standard defined in Federal Information Processing Standard (FIPS) 192, published in Nov. 2001. AES is a symmetric block cipher which can process 128-bit blocks, using key sizes of 128, 192, or 256-bit.

 In June 2003, the US Government announced that any key length of AES is sufficient to protect classified information up to secret level. Top secret information requires key length of 192 or 256-bit.

SRTP, a profile of the Realtime Transport Protocol (RTP), provides confidentiality, message authentication, and replay protection to the RTP traffic and to the control traffic (RTCP). AES is the default and only standardized cipher for SRTP.

ShoreTel 9 support AES and SRTP through adopting RFC 4568.

SRTP-AES Description

System Support

ShoreTel 9 supports SRTP for encrypting, authenticating, and replaying media streams for ShoreGear switches and ShorePhones that support encryption. ShoreWare encrypts RTP (payload) packets sent within the ShoreTel network. Call control packets are not encrypted. ShoreTel 9 retains the proprietary 128-bit encryption algorithm that is available in previous version as an alternative to SRTP encryption.

Encryption is enabled or disabled on a system basis, encompassing all sites, and cannot be specified for individual devices or selected calls. Encryption is transparent to end users and cannot be selected for individual devices or calls. Calls in progress when the encryption setting is changed remain the same encryption method through the duration of the call.

System administrators enable and select an encryption algorithm through ShoreWare Director. The following encryption options are available:

- None
- 128 bit ShoreTel Proprietary
- SRTP - 128 bit AES

SRTP with AES and authentication has a significant impact on the system load when a large number of media channels are encrypted.

SRTP-AES encryption is provided on all ShoreTel 9 systems and does not require an additional license.

Devices

Switches and Codecs

SRTP encryption is supported by the following ShoreGear Voice Switches:

- All Voicemail Model switches
- All 1-U Half Width switches
- All 1-U Full Width switches

Switches do not support SRTP with linear (LRNB/8000) or wide-band (LRWB/16000) codecs. When SRTP is enabled, codec negotiation excludes these codecs.

ShoreGear switches support a maximum of 36 encrypted media streams. This limitation potentially impacts switches that provide T1 or E1 channels with high 3-way conference call traffic.

Each channel in a 3-way conference requires two media stream encryption resources, limiting switches to 18 encrypted channels for 3-way conferences. In this scenario, all remaining trunks provided by the switch are blocked while 18 channels are engaged in 3-way conference calls. Switches can service any combination of two-way (one encrypted media stream) and three-way (two encrypted media streams) calls that do not exceed 36 media streams. Analog ports on the SG-220T1A are included in this limitation.

Phones and Applications

All ShorePhones that run the ShoreTel 9 firmware support SRTP-AES. SoftPhone, which is available through Call Manager, also supports SRTP-AES.

Call Manager and ShorePhones display a padlock icon for each call utilizing SRTP encryption. The Call History list also uses the padlock icon to denote encrypted calls. ShorePhones IP210, IP110, and IP115 do not display the encrypted call padlock icon. The padlock icon indicates that the call media is secure on the ShoreTel network. ShoreTel cannot guarantee call security outside of the network, such as calls that terminate across an analog or digital trunk. The padlock icon is not displayed when Proprietary Encryption is active.

The ShoreTel Conference Bridge, the IP 8000 Conference Phone, voicemail, and auto attendant do not support SRTP-AES encryption.

Phones that do not support SRTP cannot perform barge in, whisper, or silent monitor functions on existing calls that are SRTP encrypted. When added to a call using SRTP, new parties using devices that do not support SRTP exchange unencrypted media streams. SRTP does not address user registration, call setup, or signaling related security.

Installation and Upgrades

SRTP-AES support requires the upgrade of switch software and phone firmware to ShoreTel 9. Upgrades of AES/SRTP in switches and IP phones may be decoupled. Phone calls are encrypted with the proprietary method on phones that do not support AES/SRTP.

Media Encryption is disabled on new installations. Media Encryption settings remain in place after a system is upgraded to ShoreTel 9.

Provisioning

Encryption is configured in the **Call Control: Options** panel, shown in Figure 9. The *Media Encryption* parameter determines the encryption setting for the entire system.

Figure 9   Configuring Media Encryption

To configure encryption:

Step 1 Open the **Call Control: Options** panel by selecting *Administration -> Call Control -> Options* from the main menu.

Step 2 Select the desired option from the Media Encryption drop down menu, as shown in Figure 9.

Step 3 Press the Save button at the top of the panel.

Disaster Recovery Enhancements

Introduction

ShoreTel 9 introduces Disaster Recovery Enhancements to improve system compatibility with supported failover solutions. Disaster Recovery Enhancements implements primary and secondary IP addresses to distinguish the Headquarters server from its backup server.

Refer to the Glossary for a definition of the following terms used in this release note:

- Distributed Routing Service (DRS)
- Failback
- Failover

Description

ShoreTel 9 Disaster Recovery Enhancements consist of the following:

- The Headquarters server specifies a primary and a secondary IP address.

  — The server located at the primary IP address performs as the Headquarters server during normal operation.

  — The server located at the secondary IP address performs as the Headquarters server during a failover.

  Implementing the secondary server requires an additional Headquarters server license.

- ShoreTel system components access the server at the primary IP address during normal conditions and the secondary server under failover conditions when requesting services from the Headquarters server.

- The primary and secondary Headquarters server cannot be running and connected to the network at the same time.

- Single Headquarters Server mode is supported when a secondary IP address is not specified.

  To convert a system to single Headquarters Server mode, remove the address from the secondary IP address field, then reboot the Headquarters server.

- When the secondary IP address is specified, Citrix Servers and Window Terminal Server must reference the Headquarters server by the DNS name.

Conditions during the Failover and Failback Operations

ShoreWare performs a failover operation when the primary server fails to transfer Headquarters server functions to the secondary server. After the failover operation is complete, the secondary server performs all Headquarters server functions.

The system administrator manually initiates the failback operation to restore Headquarters server function to the primary server. After the failback is complete, the system structure that existed before the failback operation is restored. Refer to the documentation accompanying the failover solutions for instructions on initiating a failback operation.

Failover and failback operations typically require between five to 20 minutes, depending on the system configuration. During these periods, no Headquarter server services are available. Failover and failback operation effects are resolved after the operations are complete and the secondary (for failover) or primary (failback) server is functioning as the Headquarters server.

Failover and failback operation effects on Call Manager include:

- Users configured on the Headquarters server lose most connectivity capabilities, including telephony and video. IM connectivity is not affected.

- Users configured on distributed servers maintain all connectivity capabilities.

- Configuration changes are unavailable.

- Users logging into Call Manager while the secondary server controls the system must specify the IP Address of the secondary server.

  Refer to the Call Manager User's Manual for instructions on specifying the server IP address.

Failover and failback operation effects on voicemail include:

- Sites that receive voicemail through the Headquarters server lose voicemail access.

- Mailboxes lose access to any voicemail that is routed through the Headquarters server.

- Sites that receive voicemail from distributed servers retain voicemail access.

Failover and failback operation effects on other system components include:

- Account Code and Workgroup services are not available.

- Director, Web Client, and Call Manager configuration changes are not available.

- If DRS is enabled, intersite calls are unavailable to users residing on sites whose only access to a DRS server is through the Headquarters server.

System Failover Conditions

After the failover operation is complete, the secondary server performs all distributed server and application connectivity activities managed by the Headquarters server.

System Failback Conditions

After the failback operation is complete, the primary server resumes all distributed server and application connectivity activities managed by the Headquarters server.

Implementation

Server Address Configuration

The primary and secondary IP addresses are configured on the Edit Server panel for the Headquarters server, as shown in Figure 10. To access the Edit Server panel, open the Application Servers List by selecting *Administration -> Application Servers* from the Main Menu, then select the Headquarters Server on the list. On the Edit Server panel, the **Host IP Address** parameter configures the Primary IP address.

Figure 10   Designating Primary and Secondary IP Addresses

When the primary and secondary servers are in different subnets, their IP addresses must be static.

The DNS server accessed by a ShoreTel system must associate the same server name to the primary and secondary servers if

- The primary and secondary servers are configured with static IP addresses.

    and

- The HQ server supports MCM clients or clients on Citrix or Windows Terminal Servers.

The primary and secondary servers cannot be running and connected to the network at the same time.

System Failover Requirements

The following sections describe required administrator tasks after the failover operation.

License Compliance

After a failover operation transfers Headquarters server control to the secondary server, license status on the secondary server is non compliant. To restore the system to compliance, reinstall all licenses that were originally purchased for the secondary server.

MCM Failover Requirements

To assure proper MCM client operation and performance after a Failover or a Failback, the browser cache must be cleared. The system administrator should send messages to all MCM clients after a failover operation advising them to clear the browser cache on their devices.

System Failback Requirements

The following sections describe required administrator tasks after the failback operation.

License Compliance

After a failback operation transfers Headquarters server control to the secondary server, license status on the secondary server is non compliant. To restore the system to compliance, reinstall all licenses that were originally purchased for the secondary server.

MCM Failback Requirements

To assure proper MCM client operation and performance after a Failback, the browser cache must be cleared. The system administrator should send messages to all MCM clients after failback procedures advising them to clear the browser cache on their devices.

CDR Reports – Codecs

Introduction

Definition

ShoreTel 9 enhances the CDR database and CDR reports to support the following:

- codecs added in ShoreTel 8
- references to codec strings added by the administrator

Refer to the Glossary for a definition of the following terms used in this release note:

- Call Detail Record (CDR)
- CDR Database
- Codec

Background

ShoreTel 8 supports the following codecs:

- G711µ
- G711a
- L16/16000
- DVI4/8000
- G729A/8000
- G729B/8000
- L16/16000
- G722/8000
- BV32/16000
- BV16/8000
- AAC_LC/32000

ShoreTel 8 also permits administrators to add other codecs.

Implementation

The TMS-CDR Media Stream Statistics Report and the Media Stream Detail Report indicates the encoding method that the call employed. The list of valid parameter settings is expanded to include all codecs supported by ShoreTel.

The following is a list of ShoreTel field values used by the CDR database and the codec that they represent:

- 1 ALAW   PCMA/8000 (or G711A)
- 2 MULAW   PCMU/8000 (or G711µ)
- 3 LINEAR   L16/16000
- 4 ADPCM   DVI4/8000
- 5 G729A   G729A/8000
- 6 G729B   G729B/8000
- 7 LINEARWIDEBAND   L16/16000
- 8 G722   G722/8000

- 9 BV32   BV32/16000
- 10 BV16   BV16/8000
- 11 AAC_LC32000   AAC_LC/32000
- 12 Custom   Codec added by administrator

Failover

Introduction

Definition

ShoreTel 9 implements the following Failover enhancements:

- **IP Phone Calls Continue Through Failover** feature enhances IP Phone Failover to continue a voice call, even after the managing switch becomes unavailable, until the normal completion of the call

- **Spare Switch Failover** introduces spare switches for handling IP Phones that failover.

Refer to the Glossary for a definition of the following terms used in this release note:

- Call Manager (switch)
- Failback
- Failover
- IP Phone Configuration Switch
- IP Phone Failover
- IP Phone Keep Alive

This release note uses the following endpoint and switch designations to describe the component functions during the failover process.

- **Local endpoint:** The endpoint controlled by the failed switch during a failover.
- **Remote endpoint:** The endpoint controlled by the functioning switch during a failover.
- **Failed switch:** The switch that triggered the failover when it became unavailable.
- **New switch:** The switch that replaces an unavailable switch in response to a failover.
- **Surviving Switch:** The switch that remains available when a failover is triggered.

IP Phone Operation

IP phones in a ShoreTel system interact with two ShoreGear switches: the configuration switch and the call manager switch. The configuration switches help the IP phones obtain their configuration from the ShoreWare server, which functions as a FTP server for the IP phones. Each system has one configuration switch and can designate a second switch as a backup.

During the configuration process, each IP phone is assigned a ShoreGear switch that acts as its call manager for setting up and tearing down calls. IP phones communicate with ShoreGear switches via MGCP, a device control protocol. The relationship between the switch (call manager) and the phone (gateway) follows a master–slave model.

Media travels through the ShoreTel system using Real-Time Protocol (RTP). After call setup, media flows directly between IP phones via RTP. The ShoreGear switch is involved only when setting up or tearing down a call.

IP Phone Calls Continue Through Failover

Feature Description
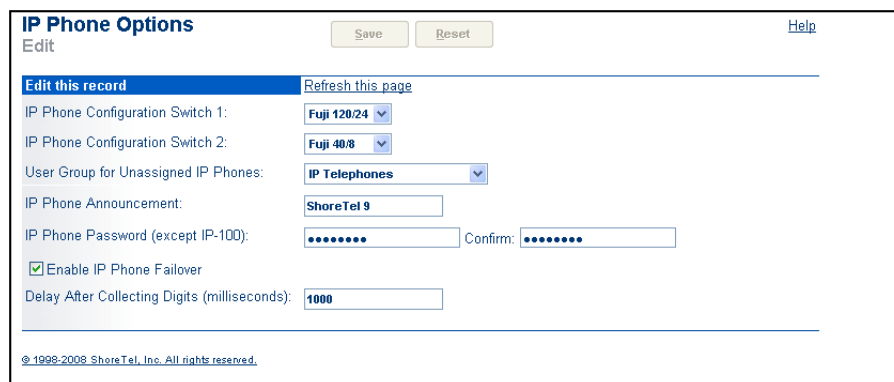
The **IP Phone Calls Continue Through Failover** feature maintains active calls through the normal completion of the call even when the call manager switch handling the call becomes unavailable.

Background

When a phone's call manager switch becomes unavailable during a call while IP Phone Failover is enabled, the phone goes through two failover stages:

- **Pending Failover** is the period between when the phone does not receive the expected acknowledgement signal from its call manager switch until the time that an alternate switch is assigned to perform call manager tasks for the phone. This period typically lasts between two to four minutes after the switch becomes unavailable.

- **Failover** is the period after the alternate switch is assigned to perform call manager tasks for the phone.

IP Phone Failover is enabled from the IP Phones Options edit panel, as shown in Figure 11.

Figure 11   Enabling IP Phone Failover

Legacy Behavior

When a phone enters the *Pending Failover* stage, calls in progress remain active. Call control options, including softkey operation, are unavailable during this time. Users cannot initiate new calls and the phone display remains frozen during Pending Failover.

In previous ShoreTel versions, all active calls are dropped when the phone enters the *Failover* stage. The phone then resumes normal operation, allowing the user to initiate or receive calls and perform call control actions on new calls.

Feature Definition

IP Phone Calls Continue Through Failover feature maintains active calls through the beginning of the *Failover* stage until the normal completion of the call. All *Pending Failover* restrictions remain in place after the phone enters the *Failover* stage until calls maintained through Failover initiation are completed.

This feature is applicable to ShorePhones, SIP extensions, and Conference Bridges. SoftPhone does not support continuation of calls through failover.

IP Phone Behavior during Failover

ShorePhone – Local Endpoint

During the Pending Failover stage, the telephone user interface (TUI) displays a *No Service* message until the phone is assigned to a new switch. Call control operations are not available on surviving calls. All inbound calls to the local endpoint are routed to the destination specified by the current Call Handling Mode.

During the Failover stage, the TUI displays *Failover Mode* while surviving calls remain active. Pressing phone keys generates a *No Service* message on the TUI. Call control operations on surviving calls remain unavailable. All inbound calls to the local endpoint are routed to the destination specified by the current Call Handling Mode. After all surviving calls are concluded, the ShorePhone returns to normal operation.

ShorePhone – Remote Endpoint

ShorePhones on remote endpoints during failover calls can hang up the call, place the call on hold, or retrieve the call from hold. All other softkey operations are unavailable for the duration of the call. The ShorePhone continues displaying call information until the end of the call. Call control operations on other calls remain available.

SIP Phones

This feature causes no changes to messages displayed by SIP devices. Failover procedures and restrictions are applicable to SIP phones. Call control operations initiated from SIP phones on failover calls are not available.

Trunk Behavior

ShoreTel only releases the trunk after the remote side goes on-hook. System cleanup procedures, executed every two hours, release trunks that were left hanging.

Restrictions

Bandwidth cannot be reallocated on the *failover switch*.

Spare Switch Failover

Background

Prior to version 9, ShoreTel does not reserve switches exclusively for servicing phones losing access to their call manager switch. Phones fail over to switches with available resources that are assigned to the same site as the phone.

Effective use of IP Phone Failover requires sufficient excess switch capacity at each site for reassigning call manager resources to phones having lost switch access.

Feature Description

Spare Switch Failover introduces spare switches for handling IP Phones that failover. Spare switches are reserved for servicing IP Phones unable to access their call manager switch. A spare switch is available at the site where it is configured and all descendants of that site.

A spare switch remains dormant until activated by a site. IP Phone failover processes within a site are unaltered by this feature until a site has no remaining call manager resources for assignment to failover devices. When an IP Phone initiates a failover when no switch

resources are available, ShoreWare searches the site and its ascendant sites until a dormant spare switch is identified. The spare switch is assigned to the site requiring the resource, after which a call manager resource is assigned to the IP Phone performing the failover.

Active spare switches only service IP Phones that failover from losing call manager resources. Other switch resources are unavailable including analog extensions, trunks, media proxy, make-me conference ports, and music on hold. Office Anywhere extensions may be created on the switch.

Implementation

Spare Switches

Spare switches provide replacement IP phone capacity for failed switches in the site and descendant sites. When activated, the spare switch is moved to the site of the failed switch.

Users configure switches as a spare through Director. Spare switch resources are not allocated during configuration. Each spare is assigned to a home site and can be used from any descendants of the home site. The entire capacity of the switch is available for MGCP and SIP extension at the site to which it is assigned through a Failover operation.

ShoreGear switches that can be configured as spares include:

- ShoreGear 120/24
- ShoreGear 40/8
- ShoreGear 60/12
- ShoreGear 50
- ShoreGear 90
- ShoreGear 220T1
- ShoreGear 220E1
- ShoreGear 90BRI
- ShoreGear 220T1A
- ShoreGear 30
- ShoreGear 30BRI

Voicemail Model switches cannot be configured as spare switches.

Spare switches cannot change languages when they are activated. Language incompatibilities are denoted with an **Firmware upgrade available** message when a switch is configured into a site with a different language.

Established calls survive the failover process when a spare switch is required.

Spare Switch Failover

Switches are returned to spare status through Director when the user has sufficient IP phone capacity to support the devices that the spare switch is servicing. IP phones managed by the switch are moved to other switches at the site when the spare switch fails back.

If the site does not have sufficient capacity to cover IP phones after a failback operation, the spare switch performs another failover.

Failback

Failback is the operation that restores the spare switch to reserved status. Spare switch failback is manually performed through Director; automatic failback of spare switches is not supported.

ShoreTel®

IP phones managed by the switch are moved to other switches after failback operation. If the site does not have sufficient capacity to cover IP phones when a failback is initiated, the spare switch performs another failover.

Failback is performed from the Maintenance – Switch Summary panel in Director.
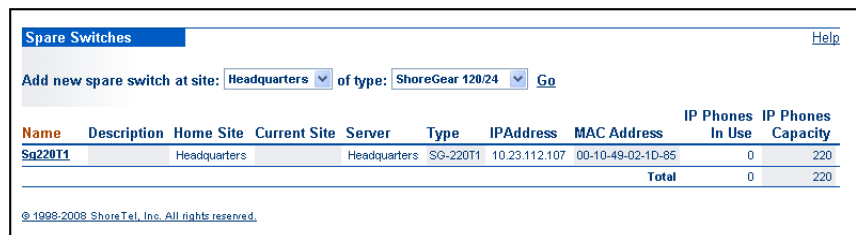
Provisioning – Director

The following Director panels are added or modified to support Spare Switch Failover

Spare Switch List

The Spare Switch List panel, shown in Figure 12, is a new Director panel that adds a switch to the specified site. You can access the configuration panel for a spare switch by clicking that switch's name.

To access the **Spare Switch List**, select *Administration -> Switches -> Spare* from the Director Main Menu.

Figure 12   Spare Switch List panel

Edit Spare Switch panel

The Edit Spare Switch, shown in Figure 13, configures parameter settings for the specified ShoreGear Switch. The Spare Switch panel differs from Primary Switch configuration panels in that port resources are not allocated to system devices.

Figure 13   Edit Spare Switch panel

To access the **Edit Spare Switch List**, select *Administration -> Switches -> Spare* from the Director Main Menu, then click the Go text at the top of the panel to add a switch or click the desired switch name to edit that switch.

Enabling IP Phone Failover

IP Phone Failover must be enabled from the Edit IP Phone Options panel.

Quick Look panel

The Quick Look panel is modified to display a **Temporary Disable IP Phone Failover Across Sites** selection box at the bottom of the panel. When this option is selected, spare switches do not failover throughout the entire system. Figure 14 displays a Quick Look panel with the **Temporary Disable IP Phone Failover Across Sites** selection box.

Figure 14 **Temporary Disable IP Phone Failover Across Sites selection box**

Maintenance – Switches Summary

The Maintenance – Switches Summary panel, shown in Figure 15, is modified to add a section listing the Spare Switches located on the specified site. This section indicates the activity level of the switch and, when active, the site upon which the switch is deployed.

Manual failbacks are performed from this panel by accessing the drop down menu for the desired switch and selecting **Fail Back**.

Figure 15 **Maintenance – Switches Summary panel**

Call Manager on 64-bit Windows Terminal Server

Introduction

ShoreTel 9 supports running Call Manager on Windows Terminal Server 64-bit operating system.

Description

ShoreTel 9 supports Call Manager on the following platforms:

- 32-bit systems: Windows 2003 (including Citrix and Windows Terminal Server), Windows XP, or Windows Vista operating systems
- 64-bit systems: *only* on Windows 2003 running Windows Terminal Server

Implementation

Initial Call Manager Installation

Installing Call Manager on 64-bit Windows running Windows Terminal Server requires the following steps:

Step 1 Install DotNet Framework for 64-bit Windows machines – Version 2.0 or higher.

DotNet Framework is not supplied with the ShoreTel installation software. This software is available from Internet sources or from your software vendor.

Step 2 Install Call Manager.

Step 3 Access *Control Panel -> Phone and Modem -> Advanced (tab)* and remove ShoreTel Remote TAPI Service P.rovider.

Step 4 Run TSPInstall.exe

TSPInstall.exe is provided with the ShoreTel installation software.

Installing 32-bit ShoreWare Clients on a 64-bit platform places files in the following folders:

- The default location is `C:\Program Files (x86)`
- The location of 32-bit client dll files is `C:\Windows\SysWow64`

Upgrading Call Manager on WTS 64-bit

To upgrade Call Manager on 64-bit WTS platform, perform the following procedure:

Step 1 Access *Control Panel -> Phone and Modem -> Advanced (tab)* and remove ShoreTel Remote TAPI Service Provider.

Step 2 Perform the procedure in the Initial Call Manager Installation section, starting with Step 1.

Director Enhancements

DiffSrv / ToS Support

Introduction

Definition

ShoreTel 9 extends DiffServ/ToS packet marking as follows:

- The existing DiffServ/ToS marking for voice IP packets is extended to voice, voicemail, workgroup, account code collection, and contact center calls.

- DiffServ/ToS marking for video IP packets is introduced.

Refer to the Glossary for a definition of the following terms used in this release note:

- Differentiated Services
- DSCP
- QoS
- Per-Hop Behavior
- ToS

Description

ShoreTel 9 extends the DiffSrv/ToS setting to all voicemail, workgroup, account code collection (ACC), or contact center calls. One setting applies to all ShoreTel servers in a ShoreTel system.

ShoreTel 9 also introduces DiffServ/ToS marking for video IP packets. The default value for the Video DiffServ/ToS Byte is 0, indicating that priority is not defined for Video packets. Changing the Video QoS setting does not affect video sessions in progress. The updated value is applied to new video sessions. Call Manager recognizes the change without being restarted.

Implementation

Voice Packet Marking

The Director Call Control panel provides an option to configure DiffSrv/ToS setting for Voice calls, as shown in Figure 16. All ShoreTel servers need to be rebooted to enable the new setting. This parameter configures DiffServ/ToS for voicemail, workgroup, account code collection (ACC), and contact center calls.

This panel is not altered by the Voice Packet Marking capability change.

Video Packet Marking

The Director Call Control panel is modified to provide a video packet DiffSrv/ToS configuration options, as shown in Figure 16. Changing this setting does not affect active video sessions. New video sessions will use the updated value. Call Manager recognizes the new value without being restarted.

The default value for the Video DiffServ/ToS Byte is 0, which defines no priority for Video.

Figure 16   DiffSrv / ToS Parameter

Support of 256 Workgroups

Introduction

Definition

ShoreTel 9 increases the number of Workgroups supported by ShoreWare to 256.

Background

ShoreTel 8.1 supports up to 128 workgroups, with up to 300 members per workgroup. A workgroup enables a group of users to appear as a single unit to calling parties. Calls can be routed in top-down, longest-idle, round-robin, and simultaneous-ring fashion. Workgroups are typically used by support and sales groups to automate call handling.

Refer to the Glossary for a definition of the following terms used in this release note:

- Automatic Call Distributor (ACD)
- Workgroup

Implementation

Director allows the creation of a maximum of 256 workgroups in the system.

To view the list of Workgroups, select *Administration -> Workgroups* from the Director Main Menu. Figure 17 displays the Workgroups List panel.

Figure 17   Workgroups List panel

SIP Trunk Profiles

Introduction

Definition

SIP Trunk Profiles is a Director enhancement that supports custom SIP Trunk parameter settings to specify third party service provider configurations.
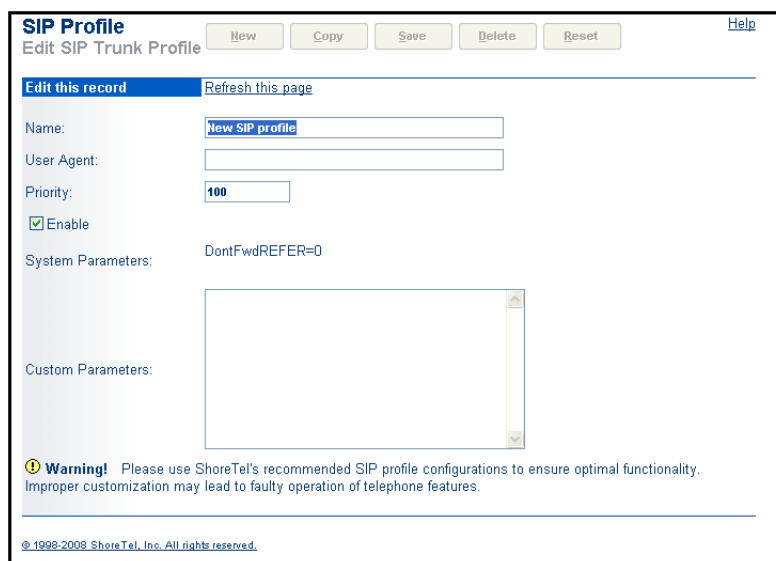
In addition to a generic profile, ShoreWare provides a profile that supports ATT BVOIP.

Refer to the Glossary for a definition of the following terms used in this release note:

- Internet Telephony Service Provider (ITSP)
- Session Initiation Protocol (SIP)
- SIP Trunk
- SIP Extensions

Panel Description

The Edit SIP Trunk Profiles panel, shown in Figure 18, is the Director panel that specifies settings for packets sent from trunks to which the profile is assigned. The Edit SIP Profile panel is accessed from the SIP Profile List by adding a new profile or editing an existing profile. All parameter fields can be edited for User Defined profiles. Enable is the only parameter that can be modified on predefined panels.

Figure 18   SIP Trunk Profile panel

To open the SIP Trunk Profile panel, select *Administration -> Trunks -> SIP Profiles* from the Director Main Menu.

Parameters listed on the panel include:

- **Name**: This parameter is the label by which Director refers to the profile.
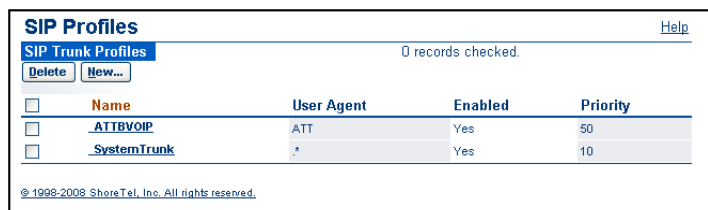
- **User Agent**: This parameter is the expression ShoreWare uses to identify devices covered by the profile. ShoreWare compares this expression to the User Agent field in the header of SIP packets handled by the system.

- **Priority**: This parameter determines the order by which the profiles are evaluated against the SIP packet header. Profiles with larger priority values are evaluated before profiles with smaller priority values.

  The each profile in the User Agent field is compared to the User-Agent field of the SIP packet header until a match is found. The profile containing the matching User-Agent field is then used to specify device configuration settings.

- **Enable**: This parameter lists the status of the profile. ShoreWare uses only profiles that are enabled when evaluating the characteristic set of a device.

- **System Parameters**: This field lists the device characteristics and default settings.

- **Custom Parameters**: This field lists additional device settings or overwrite default settings listed in the System Parameters field. Supported parameters include:

  — *DontFwdREFER*: When enabled, packets are inhibited from sending REFER messages.

Implementation

To view the available SIP Trunk Profiles, access the SIP Trunk Profile List, as shown in Figure 19, select *Administration -> Trunks -> SIP Profiles* from the Director Main Menu.

Figure 19   SIP Trunk Profile List

To view a SIP Trunk profile, open the Edit SIP Trunk Profile panel, as shown in Figure 20, click the name of the desired profile in the SIP Trunk Profile List.

To create a new SIP Trunk profile, open the Edit SIP Trunk Profile panel, as shown in Figure 20, press the New button in the upper left corner of the SIP Trunk Profiles list.

To implement a SIP Trunk profile into the definition of a SIP Trunk Group, perform the following:

Step 1 Open the Trunk Groups List by selecting *Administration -> Trunks -> SIP Profiles* from the Director Main Menu.

Step 2 Open the desired trunk group by clicking the name of the group.

Step 3 Select a profile from the Profile drop down list, as shown in Figure 21.

Figure 20   Edit SIP Trunk Profile panel

Figure 21   Implementing a SIP Trunk

DID Enhancements

Introduction

Definition

ShoreTel 9 modifies DID assignment fields and labels on User, Workgroup, Route Point, Menu, Hunt Group, and Bridge Call Appearance panels.

Refer to the Glossary for a definition of the following terms used in this release note:

- Available DID numbers
- DID Range
- Direct Inward Dialing

Usage Information

DID assignment sections on Director panels consist of two parameters: DID Range and DID Number. Figure 22 displays these parameters on the Edit User panel. Other affected panels are constructed similarly.

Figure 22   DID Parameters on Edit User panel

- The DID Range parameter displays the complete base phone number and trunk group name.

    — To authorize the user to use a DID number, select the checkbox located left of the DID Range text.

    — Access the drop-down menu to specify the DID Range from which the entity's DID number will be selected. Each DID Range corresponds to a trunk group and lists the number of available numbers, as shown in Figure 23.

- A link to the System Directory panel is located right of the DID Range data entry field.

    Administrators can assign a DID number by viewing the System Directory panel to find an available DID number, then selecting the number from the drop-down list.

Figure 23   DID Range parameter – drop-down menu

Unassigned numbers within a DID range may not be available if the number is assigned as a DNIS in the same trunk group.

- The DID Number parameter assigns the specified DID number to the entity. The prefix located left of the data entry field and the range located right of the data entry field are based on the selected DID range.

Client Features

Announced Find Me

Introduction

Definition

Announced Find Me is an enhancement of Find Me that provides for the recording of the caller's name for calls routed to Find Me destinations. This feature provides the capacity for all inbound callers to be identified when their call is routed to a Find Me destination.

Refer to the Glossary for a definition of the following terms used in this release note:

- Announced Find Me
- Find Me

Background

Find Me is a call handling method that allows a user to route inbound calls to a specified extension or phone number as an alternative to sending callers to voicemail.

Find Me call handling provides inbound callers with a method of connecting to their intended call recipient while listening to the recipient's voicemail greeting. Callers are routed to an extension or phone number by pressing "1" while listening to the recipient's voicemail greeting.

System users configured for Find Me can specify two numbers for receiving calls through Find Me. The standard voice mail greeting does not prompt the caller on the availability of Find Me call handling.

Find Me call handling is enabled through call handling mode settings. Find Me destinations are independent of the call handling modes that activate Find Me.

After the caller presses "1", the system informs the caller that Find Me destinations are being called. Calls not answered at either Find Me destination are sent to voice mail.

When a call is forwarded to a Find Me destination, the phone at the Find Me destination displays recipient's voice mail caller ID to the call originator. When answering a call, the recipient hears a prompt announcing the call and, if available, the caller's ID information. The recipient can then accept the call or route the caller to voicemail.

Description

Announced Find Me enhances the base Find Me feature such that:

- The caller's name is announced to the recipient of a Find Me call.

- Callers from external numbers or from internal extensions without a recorded name are prompted to record their name before the call is routed to the recipient.

Provisioning

Announced Find Me is available for users assigned to a class of service for which Find Me is authorized. ShoreWare provides three methods of enabling Announced Find Me for a user: from Director, from Call Manager, and from Web Access.

Users can receive Announced Call Me introductions for all callers or restrict the introductions to calls for which Caller ID is not available.

Enabling Announced Find Me from Director

Administrators enable Announced Find Me for system users from the Find Me and External Assignment panel.

To enable Announced Find Me for a user, perform the following:

Step 1 Access the user's **Edit User** panel by selecting *Administration -> Users -> Individual Users* from the Director Main Menu, then clicking the desired user's name in the I**ndividual Users list** panel.

Step 2 Access the user's **Find Me and External Assignment** panel, as shown in Figure 24, by selecting *Personal Options* in the selection bar at the top of the **Edit User** panel, then clicking *Find Me* at the bottom of the **Personal Options** panel.

Figure 24   Enabling Announced Find Me from Director

Step 3 Select the *Enable Record Caller's Name for Find Me* (When Caller ID is unavailable) checkbox.

To enable Announced Find Me when Caller ID is available, select the *Record Name Even If Caller ID* Is Present checkbox.

Enabling Announced Find Me from Call Manager

Users enable Announced Find Me from the Options and Preferences: Find Me panel in Call Manager.

To enable Announced Find Me from Call Manager, perform the following:

Step 1 Open the Options and Preferences panel by executing one of the following actions:

- Select *Tools -> Options* from the Main menu.
- Click the Application Button and select *Options*.
- Right click the ShoreTel icon in the System Tray and select *Options*.
- Press Ctrl+O.

Step 2 Open the Find Me panel, shown in Figure 25, by selecting *Find Me* from the Menu on the left side of the panel.
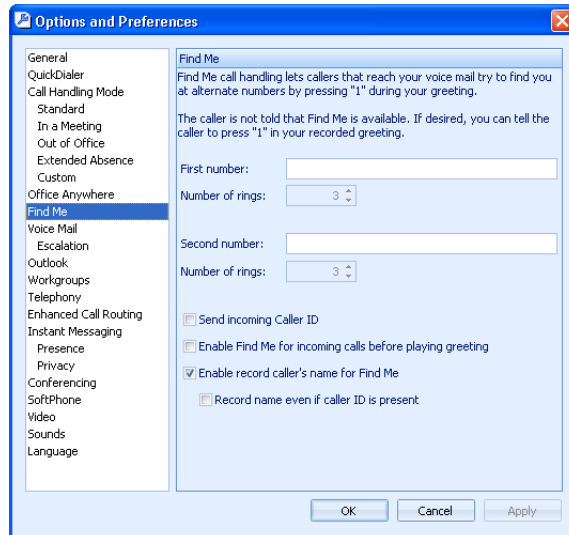
Figure 25   Enabling Announced Find Me from Call Manager

Step 3 Select the *Enable Record Caller's Name for Find Me* (When Caller ID is unavailable) checkbox.

To enable Announced Find Me when Caller ID is available, select the *Record Name Even If Caller ID* Is Present checkbox.

Enabling Announced Find Me from Web Access

Users enable Announced Find Me from the Find Me panel in Web Access.

To enable Announced Find Me from Web Access, perform the following:

Step 1 Open the Find Me panel, shown in Figure 26, by clicking the Find Me tab at the top of the page.

Step 2 Select the *Enable Record Caller's Name for Find Me* (When Caller ID is unavailable) checkbox.

To enable Announced Find Me when Caller ID is available, select the *Record Name Even If Caller ID Is Present* checkbox.
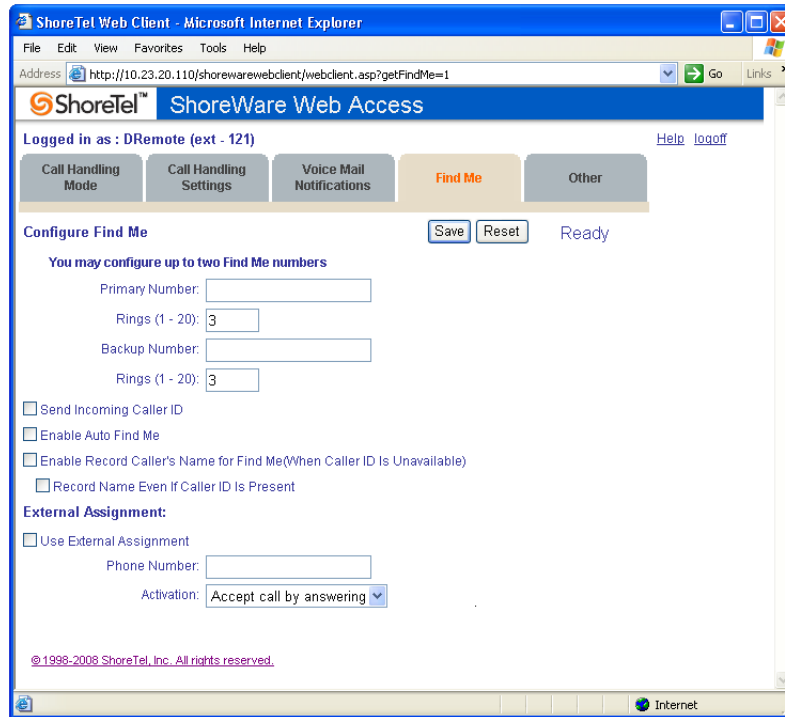
Figure 26   Enabling Announced Find Me from Web Access

Usage Information

Caller Functions

When the Announced Find Me parameter is enabled, callers that are routed to a Find Me extension are prompted to record their name under each of the following conditions:

- The call is from a source external to the ShoreTel system and the number is not available through Caller ID.

- The call is from a source external to the ShoreTel system and *Record Name Even if Caller ID is Present* option is selected.

- The call source is within the ShoreTel system, the caller's name recording is not available, and the *Record Name Even if Caller ID is Present* option is selected.

The prompt advises the caller to press the # button when finished with the name recording. Callers can press the # button without recording a message. Pressing the * button restarts the name recording process.

Call Recipient Functions

The base Find Me feature introduces the caller identity whenever available to recipients that have enabled the feature. This information is always available when receiving calls from ShoreTel extensions or from PSTN numbers identifiable through Caller ID. Announced Find Me extends this function to identify all callers regardless of the originating phone number by recording the name of callers whose identity is unavailable.

Callers that do not record their name when prompted are not identified when the system introduces the call to the Find Me recipient.

Personalized Call Handling

Introduction

Definition

Personalized Call Handling defines flexible handling methods for inbound calls from different callers received at various times and dates. Possible applications for Personalized Call Handling includes:

- Requiring unidentified callers to announce their name by routing them to Announced Find Me.

- Assigning different ringtones for selected callers, such as family, personal contacts, external contacts.

- Routing calls from non urgent sources directly to voicemail or to other extensions.

Personalized Call Handling filters and manages inbound calls on the basis of multiple criteria including time or date calls are received, end user status, and caller identity. Personalized Call Handling is implemented through *Call Routing Plans* and *Call Routing Rules*:

- The call routing plan specifies a user's call handling method. The plan prioritizes a list of enabled Call Handling Rules.

- A call handling rule is the base unit of a Call Routing Plan that consists of a condition and action. When a call handling rule is active and the condition is satisfied, the action specifies the method by which the ShoreTel system handles the user's call.

Refer to the Glossary for a definition of the following terms used in this release note:

- Active Call Handling Mode
- Announced Find Me
- Auto Find Me
- Call Handling Mode
- Call Handling Rule
- Call Routing Plan
- Find Me
- Off System Extensions
- Personalized Call Handling

Background

Call Handling Modes automate call routing on the basis of a user's schedule or activity. Personalized Call Handling defines call handling methods by considering, in addition to Call Handling Modes, conditions outside the scope of Call Handling Modes.

Description

Introduction

A Call Routing Plan manages a user's inbound voice calls. The plan consists of call handling rules, each of which specifies a method of handling a call when a condition set is valid. The plan enables and prioritizes selected rules. The user's inbound calls are evaluated against the call handling rules. The highest priority rule with conditions that are satisfied define the handling method for the call.

This section describes the structure and call handling rules, followed by a discussion of creating a call routing plan from these rules.

Call Handling Rules

Call handling rules define evaluation conditions and handling action. When the rule is active and the condition is satisfied, the action determines how the call is handled.

Three components comprise a call handling rule: name, condition, and action. The following sections describe call handling rule components.

Name

The name is the label by which Call Manager and Director refer to a call handling rule. Users specify the name when they create the rule.

Condition

The condition is the filtering criteria that determines if a corresponding call handling action is performed. When a condition statement consists of multiple criteria, each criterion must be satisfied or the action is not performed.

Call Handling Rules defines the following six types of criteria

- **Phone number match:** The phone number match is satisfied when the caller ID of the inbound call is a subset of the specified match type. Users can specify a maximum of ten *phone number match* entries.

  Users can select one of the following match types:

  — *specific number* – user specifies the number that must match the caller ID; numbers can be internal extension or phone number external to the system.

  — *off system extension* – user specifies the off system extension that must match the caller ID.

  — *any internal extension starting with* – user specifies the digits that must match the first digits of numbers originating from internal callers.

  — *any external extension starting with* – user specifies the digits that must match the first digits of numbers originating from phone numbers external to the system.

  — *private* – matches all calls that are identified by caller ID as *private*.

  — *out of area / unknown* – matches all calls that caller ID identifies as *out of area* or *unknown*.

  — *Every internal number* – matches all calls originating from a device within the ShoreTel network.

  — *Every external number* – matches all calls originating from a device not located within the ShoreTel network.

- **I am on the phone:** This criterion is satisfied when the user's phone is *busy*.

- **Call Handling Mode:** This criterion is satisfied when the user's active Call Handling Mode matches the specified mode.

- **Time of day:** This criterion is satisfied when the call is received during the specified time ranges. **Time of day** entries are based on the timezone setting of the site to which the user is assigned.

- **Day of week:** This criterion is satisfied when the call is received on one of the specified days. **Day of week** entries are based on the timezone setting of the site to which the user is assigned.

- **DNIS Match:** This criterion is satisfied when the DNIS of the inbound call matches the specified number.

  Workgroup and Hunt Group DNIS numbers are not propagated to members that answer group calls. This prevents the filtering calls on the basis of DNIS numbers not directly associated to the entity ultimately receiving the call.

Action

The action specifies the resolution for calls that match the specified condition. Call Handling Rules define the following five action types:

- **Forward Call to Specific Number:** This action routes the call to the specified number. Users can select one of the following number types:
  — Specific Number
  — Off System Extension

- **Forward Call to Voice Mail:** This action routes the call to the recipient's voice mail.

- **Forward Call to Auto Find Me:** This action routes the call to voicemail, which then forwards the call to the recipient's Find Me number.

- **Forward Call to Announced Find Me:** This action routes the call to voicemail, which then forwards the call to the recipient's Find Me number. The system attempts to announce the caller's name to the recipient, which may require the caller to record their name before the call is presented to the recipient.

- **Play Ringtone:** This action programs the ShorePhone to play the designated ring tone that announces the presence of the inbound call to the recipient.

Call Routing Plan

Definition

The Call Routing Plan is the data structure that determines the routing method of a user's inbound calls. The following sections describe the composition and operation of a call routing plan.

Components

A call routing plan consists of a maximum of ten call handling rules. The plan specifies the rules that are active and lists the rules in the order by which they are used to evaluate characteristics of the inbound call.

Execution

When a user receives an inbound call, the system evaluates the characteristics against the highest priority call handling rule that is enabled. If all of the criteria comprising the condition of that rule matches the call characteristics, the call is routed as specified by the rule's action and the plan execution is complete. If any of the criteria do not match the call characteristics, the system continues the plan execution by evaluating the call against the next highest priority call handling rule that is enabled.

This process is repeated for all enabled call handling rules. If the call characteristics do not match the conditions of any enabled call handling rule, the call is routed as specified by the active Call Handling Mode.

Licensing

Personalized Call Handling is available to all system users that are authorized for the following Call Manager types:

- Professional
- Operator
- Workgroup Agent
- Workgroup Supervisor

Personalized Call Handling does not require administrator authorization for users assigned to these Call Manager types.

Configuring Personalized Call Handling

The following sections describe the User Interface panels that configure Personalized Call Handling.

Call Manager User Interface Panels

The following Personalized Call Handling panels are available through Call Manager.

Option and Preferences Panels: Personalized Call Handling

The Personalized Call Handling panel, shown in Figure 27, configures the user's call routing plan.

To access the Personalized Call Handling panel, open the Options and Preferences window, then select Personalized Call Handling in the menu on the left side of the window.

Personal Call Handling panel parameters include:

- **Rule Table:** The rule table, located in the top half of the panel, lists the rules defined by the user. Rules are listed in the order that the system uses them to evaluate inbound calls. Table columns and components include:

  — *Rule Buttons:* Rule buttons are located at the top of the panel and control the creation, modification, and removal of Call Handling Rules from the Rule Table.

    ∗ Pressing the *New Rule* button opens the Condition Setup panel. A new rule is added to the Rule Table upon successful completion of the setup panels.

    ∗ Pressing the *Modify Rule* button opens the Condition Setup panel and fills the parameters with the settings of the rule highlighted in the Rule Table.
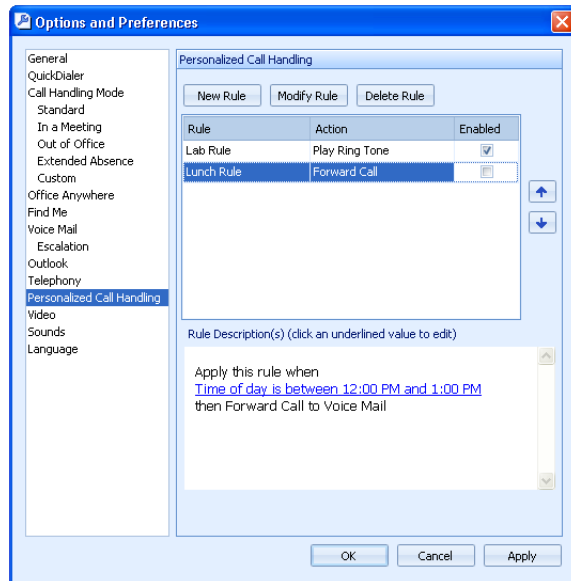
Figure 27   **Options and Preferences: Personalized Call Handling panel**

   ✳   Press the *Delete Rule* button to remove the highlighted rule from the Rule
        Table.

— *Rule List:* The Rule list displays the list of call handling rules defined by the user.
    Rules are listed in order of their usage priority; higher priority rules are listed first.
    List columns include:

   ✳   Rule: This column displays the name of the rule.

   ✳   Action: This column displays the call handling action triggered by the rule
        when the corresponding condition is satisfied.

   ✳   Enabled: This column indicates the status of the rule.

        To enable a rule, mark the Enabled box.
        To disable a rule, clear the Enabled box.

— *Priority button:* The buttons located right of the rule list changes the priority of the
    highlighted rule by moving it up or down in the rule list.

• **Rule Description:** The Rule Description field, located in the bottom half of the panel,
    displays the conditions and call handling actions of the highlighted rule in the Rule
    List. Clicking on hypertext accesses a dialog box that modifies the condition or action
    specified by the hypertext.

Condition Setup panel

The condition setup panel, as shown in Figure 28, specifies the filtering criteria that the
call characteristic must match before the corresponding action is performed. To access the
Condition Setup panel, press the New Rule or Modify Rule buttons in the Personalized Call
Handling panel.

Condition Setup panel components include:

• **Condition selection field:** The Condition selection field is located in the top half of the
    panel and contains six checkboxes for the six call condition types. Conditions selected
    in this field are displayed in the Condition description field. At least one checkbox
    must be selected; there are no other restrictions on the number of selected conditions.
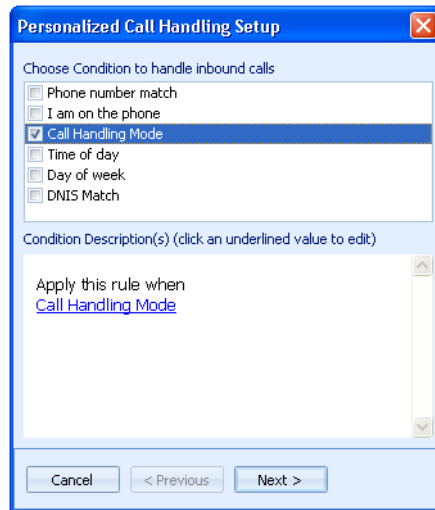
Figure 28   Condition Setup panel

- **Condition Description field**: The Condition Description field displays the selected conditions and the parameter setting that the call characteristic must match. Hypertext links denote a condition that requires a parameter setting. Clicking the link opens a dialog panel that assigns a value to the parameter.

- **Button bar**: The button bar is located at the bottom of the panel.

  — Pressing the **Cancel** button returns to the previously opened window without saving condition changes.

  — Pressing the **Next** button opens the Action Setup panel if all conditions listed in the Condition Description field are assigned parameter values.

Condition Selection dialog boxes

Call Manager displays a condition selection dialog box when the corresponding condition is selected in the Condition Description field of the Condition Setup panel. Figure 29 displays the available Condition Selection boxes.
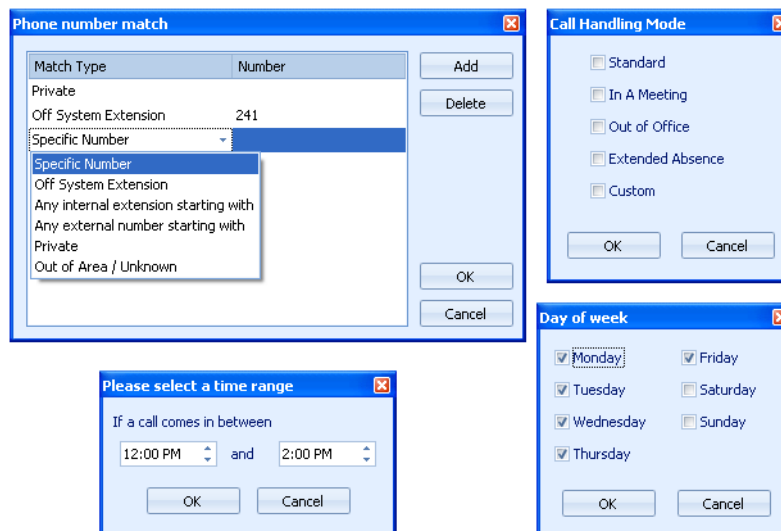
Figure 29   Condition Selection dialog boxes

Action Setup panel

The action setup panel, as shown in Figure 30, specifies the call handling action performed on the call when the rule conditions match the call characteristics. To access the Action Setup panel, press the Next button in the Condition Setup panel.
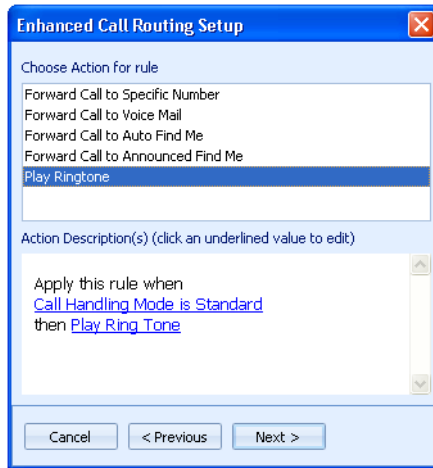
Figure 30   Action Setup panel

Action Setup panel components include:

- **Action selection field**: The Action selection field is located in the top half of the panel and contains five action lines. The action conditions selected in this field are displayed in the Action description field. One line is selected.

- **Action description field**: The Action description field displays the selected action and the parameter setting that describes the routing destination for the call. Hypertext links denote an action that requires a parameter setting. Clicking the link opens a dialog panel that assigns a value to the parameter.

- **Button bar**: The button bar is located at the bottom of the panel.
  - *Cancel*: returns to the Options and Preferences: Personalized Call Handling panel without saving panel changes to the Action Setup panel.
  - *Previous:* returns to the Condition Setup panel without saving changes to the Action Setup panel.
  - *Next:* opens the Name Setup panel if all actions listed in the Action Description field are assigned parameter values.

Action Selection dialog boxes

Call Manager displays an action selection dialog box when the corresponding action is selected in the Action Description field of the Action Setup panel. Figure 31 displays the available Action Selection boxes.
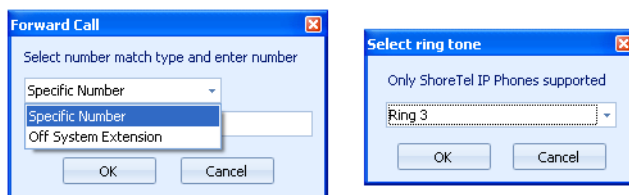
Figure 31   Condition Selection dialog boxes

Name Setup panel

The Name Setup panel, as shown in Figure 32, specifies the label by which the call handling rule is referred by the Personalized Call Handling panel. To access the Action Setup panel, press the Next button in the Action Setup panel.

Figure 32   Action Setup panel

Director User Interface Panels

The Personalized Call Handling Rules panel, as shown in Figure 33, displays the Call Handling Rules created by the specified user. The table displays the name, condition, action and enabled status of each rule. The rules are listed in the order that they were created; the table does not display the usage priority of the rules.

Figure 33   Personalized Call Handling Rules panel (Director)

To access the Personalized Call Handling panel:

Step 1 Open the Individual User list by selecting *Administration -> Users -> Individual Users* from the Director Main Menu.

Step 2 Open the Personal Options panel for the desired user by clicking the name of the desired user in the **Individual User List**, then selecting *Personal Options* on the menu bar toward the top of the **Edit User** panel.

Step 3 Click Personalized Call Handling Rules, located in the middle of the Personal Options panel, as shown in Figure 34.
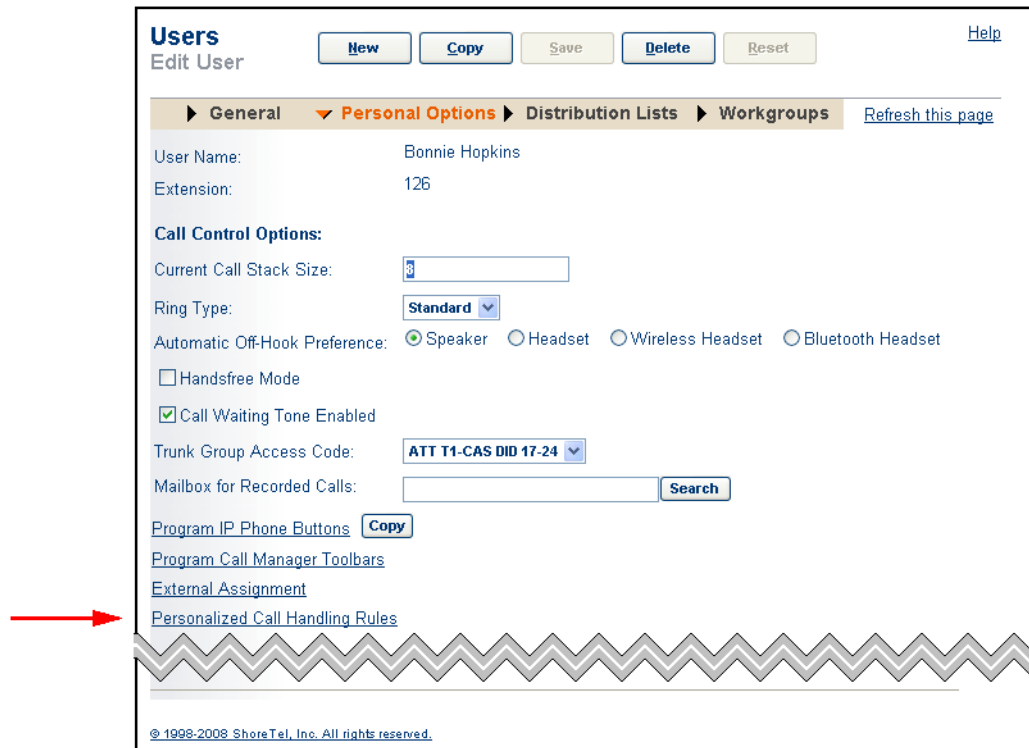
Figure 34   **Edit User Panel – Selecting Personalized Call Handling Rules**

Implementing Personalized Call Handling

The following steps are required to implement Personalized Call Handling for a system user:

- Receive Administrator Access to Personalized Call Permission

- Create and Edit Call Handling Rules

- Manage the Call Routing Plan

- Administrative Oversight of defined plans

The following sections describes the required steps.

Administrative Permission

All users that have access to Professional, Workgroup Agent, Workgroup Supervisor, or Operator Call Manager are authorized to use Personalized Call Handling.

Your system administrator can provide authorization for a Call Manager version that supports Personalized Call Handling.

Creating and Editing Call Handling Rules

Personalized Call Handling Rules are created or edited from the **Options and Preferences: Personalized Call Handling panel**, as shown in Figure 35.
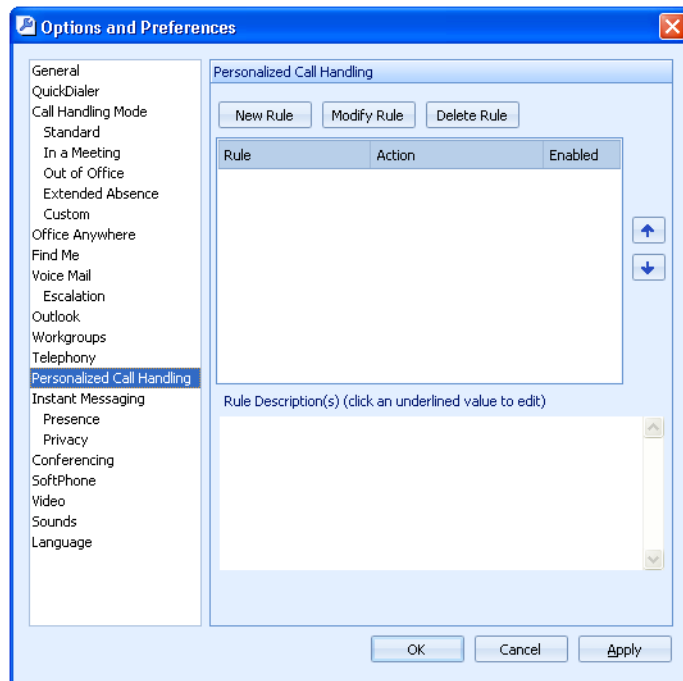
Figure 35   **Personalized Call Handling panel**

To create a Call Handling Rule:

Step 1 Press the New Rule button, located at the top of the panel.

Call Manager displays the Personalized Call Handling Setup panel, as shown in Figure 36.
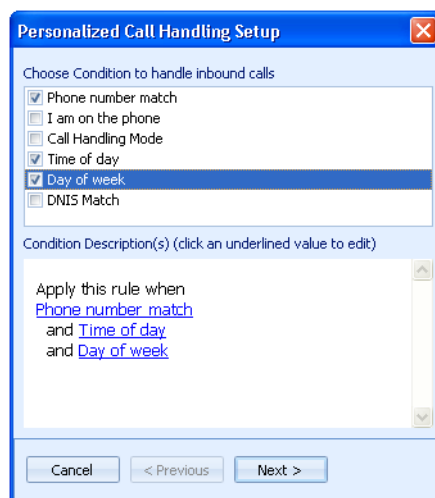
Figure 36   **Personalized Call Handling Setup panel – choosing condition**

Step 2 Select all conditions in the *Choose Condition to handle inbound calls* section located in the top half of the panel.

The *Condition Description* section, located in the bottom half of the panel, displays the set of conditions that an inbound call must meet to be filtered by the rule. Blue hypertext regions link to dialog boxes that define specific criteria for filtering calls.

Step 3 Click each hypertext region to enter filtering criteria in the dialog boxes.

Figure 37 displays the Phone Number match dialog box that Call Manager displays when the Phone Number Match hypertext is clicked. Pressing the OK button closes the dialog boxes and displays the selected parameters on the Condition Selection section.
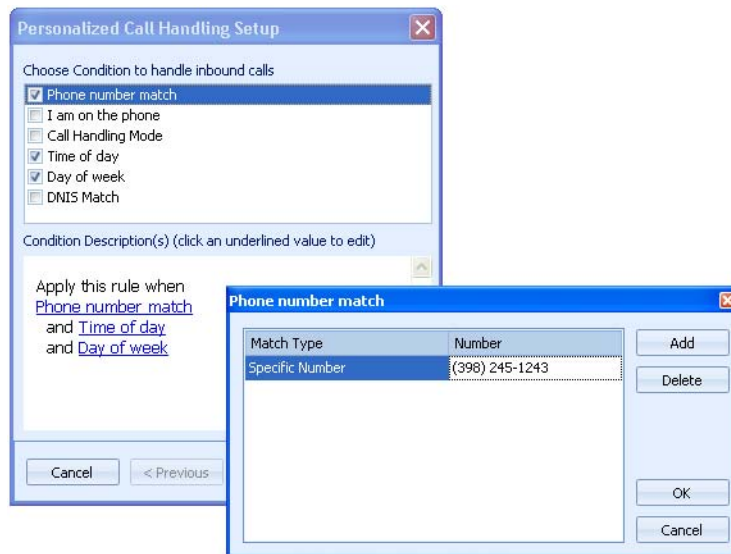
Figure 37   **Phone Number Match dialog box**

Step 4 Press the **Next** button located in the bottom right corner of the Personalized Call Handling Setup panel.

The top section displays *Choose Action for rule* options; and bottom section displays Action Description, as shown in Figure 38.

Step 5 Select the desired call handling action for calls from the *Choose Action for rule* list.

The **Action Description** section, located in the bottom half of the panel, displays the selected action.

Step 6 If the selected action in the Action Description section includes hypertext, click the link to display an action dialog box. Select the desired option in the dialog box and press the OK button.

Step 7 Press the Next button located in the bottom right corner of the Personalized Call Handling Setup panel.

Step 8 Enter a name for the new rule in the *Enter Rule Name* data entry field.

Step 9 Press the Finish button located in the bottom right corner of the Personalized Call Handling Setup panel.
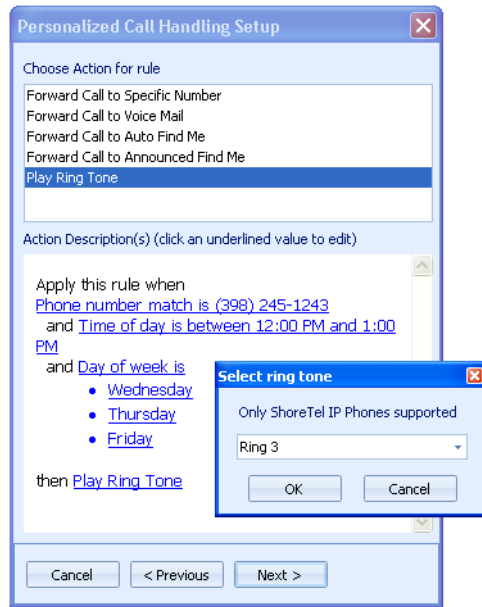
Figure 38   Personalized Call Handling Setup panel – choosing action

The new rule appears in the Rule list of the Options and Preferences: Personalized Call Handling panel, as shown in Figure 39.
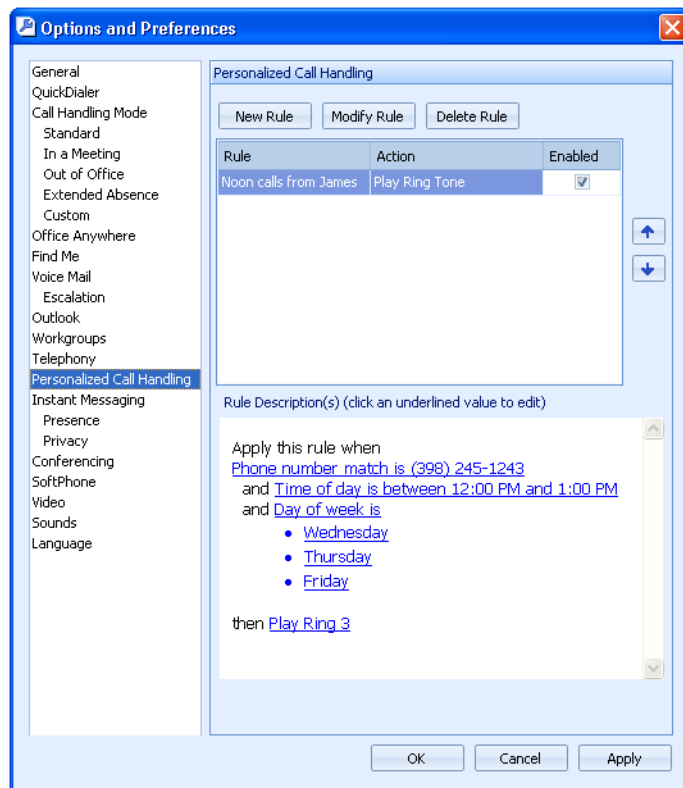
Figure 39   Personalized Call Handling Rule

To edit an existing Personalized Call Handling Rule:

Step 1 Highlight the desired rule in the rule list in the top half of the Personalized Call Handling panel.

Step 2 Press the Modify Rule button at the top of the panel.

Step 3 Modify rule parameters, using the same steps that create a Call Handling Rule.

Managing the Call Routing Plan

The Call Routing Plan determines the rules that are actively filtering calls and specifies the order that the rules are applied to calls. If the filtering criteria of more than one rule matches a call's characteristic, the first rule in the list that filters a call determines the handling action for that call.

To enable a Call Handling Rule, select the Enabled box located in the right column of the rule. In Figure 40, all of the call handling rules are selected.

To change the filtering order of a call handling rule, highlight the rule and press the Up or Down arrows located to the right of the call handling rule list.
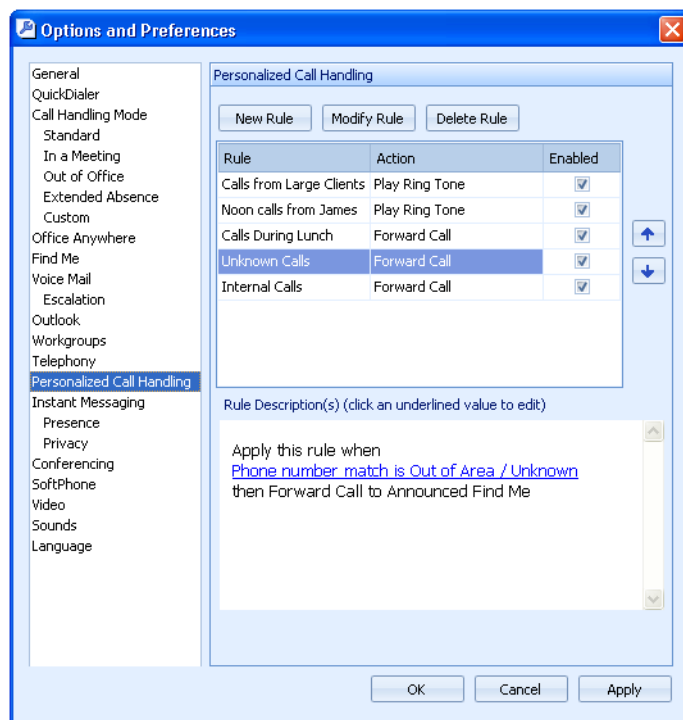
Figure 40   **Call Handling Plan with multiple rules**

Administrative Oversight

System administrators can view each user's call handling plan and enable or disable individual rules. Contact your system administrator for more information.

Parked Call Enhancements

Introduction

Definition

Parked call enhancements support the following changes to the parked call feature:

- Provide caller ID information to users attempting to pick up calls parked or held on any extension.

- Provide caller ID and return notification for bounced parked calls that are returned to the extension that parked the call.

- Extend the capability of Monitor Extension Programmable Buttons to access parked and held calls on the monitored extension's call stack.

Refer to the Glossary for a definition of the following terms used in this release note:

- Bounced Call
- Call Appearance
- Call Stack
- DN
- Monitor Extension
- Parking a Call
- Programmable Call Manager Toolbar Buttons
- Programmable IP Phone Buttons
- Unparking a Call

Unparking Selected Calls

Background

When an extension's call stack contains more than one held call, users from other extensions can retrieve calls from that stack through programmable button functions. The Monitor Extension function allows the user to view the caller ID of the call and select a call to unpark. The Unpark function only allows retrieval of the first suspended call that was placed on the stack.

Feature Description

ShoreTel 9 expands the Unpark programmable button capability, allowing users to view the caller ID of all calls on the specified extension's stack and select a call for retrieval.

This feature enhancement does not alter unpark star code and park star code behaviors. It also does not alter the Monitor Extension programmable button function.

Provisioning

Users must be authorized for the following:

- to view caller ID information for other extensions.
- to view individual calls through a Class of Service setting.

These options are enabled by selecting the *Show Caller ID Name and Number for Other Extensions* and *Enumerate Individual Held Calls for Unpark* options on the E**dit Telephony Features Permissions Class of Service** panel, as shown in Figure 41.

Figure 41   Enumerate Individual Held Calls for Unpark option

Implementation

Call Manager

Users unpark calls from a monitored user's call stack by pressing a Monitored Extension button. To perform the unparked call function, the Extension Monitor button must be appropriately configured by the system administrator and Call Manager cannot be servicing a connected call.

When the call stack of the monitored extension contains more than one call, the user can view a drop-down menu by pressing the arrow on the right side of the button. The drop-down menu displays contact information for each parked call on the stack. The desired call is unparked by selecting the corresponding entry in the menu.

The Call Manager window in Figure 42, contains a Monitored Extension button with an accessed drop-down menu.

Pressing the button unparks the call that was parked first.

ShorePhones

Pressing a programmable button configured for the Monitored Extension – Unparked function displays the list of parked calls on the telephone user interface. Press the cursor control to select the desired call, then press the appropriate soft button to unpark the call.
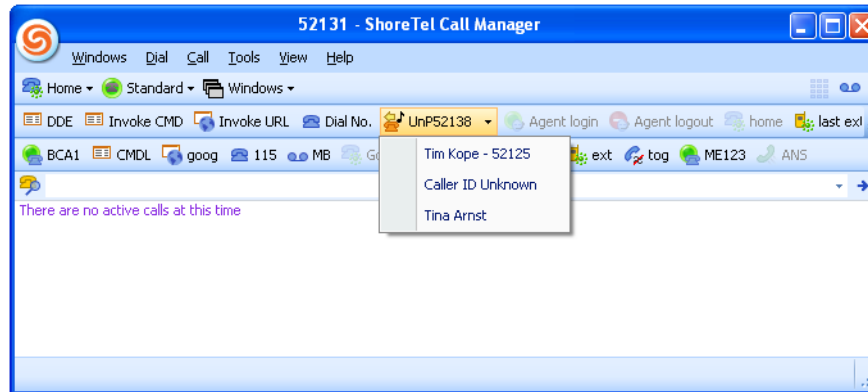
Figure 42   Unparked Call Button Drop-Down Menu

Distinguish Bounced Calls from New Calls

Background

Bounced calls are unanswered parked calls that are returned to the extension from where they were parked after a specified period. Bounced calls are returned as new calls; the extension is not notified that the call was previously parked.

Feature Description

This feature modifies the call bouncing process to distinguish new calls from calls bounced from another extension's stack.

Call Manager

Figure 43 displays a call cell of a bounced call.
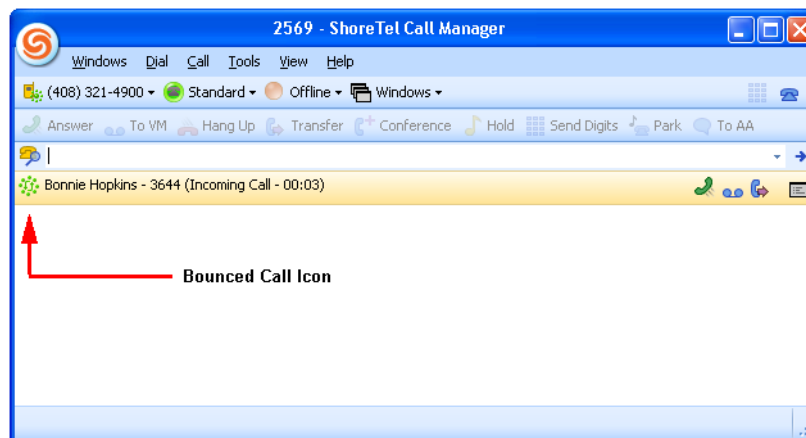
Figure 43   Call Manager – Bounced Call icon

ShorePhones

ShorePhone call appearance buttons indicate a call that was returned from another extension's call stack with the following LED pattern:

Green 200ms – Off 200ms – Green 200ms – Off 800ms

Monitoring Extensions: Parked Calls

Background

Extension monitoring is a ShoreTel feature that permits a user to view the extension status of another user and answer inbound or held calls to that extension.

Description

This feature extends the Extension Monitoring function to monitor parked calls on the subject extension. Users can unpark a call by pressing the programmable button. Multiple users can monitor the same extension's call stack.

Provisioning

This feature is enabled by configuring a Programmable Button (IP Phone or Call Manager) as shown in Figure 44.

Figure 44   Configuring Monitor Extension Button to monitor parked calls

Implementation

Call Manager

When a suspended call is placed on the monitored extension's stack, the programmable button displays an orange icon, as shown in Figure 45. The button displays this icon while the stack contains at least one suspended call and no other call on the stack is active.

The user retrieves a parked call from the monitored extension by pressing the programmable button.

ShorePhones

When a suspended call is placed on the monitored extension's stack, the programmable button blinks orange. The button continues blinking orange while the stack contains at least one suspended call and no other call on the stack is active.The button blinks orange until all the calls are unparked and there are no active calls.

The button quits blinking if the call is resumed or another call becomes active on the subject extension. The button resumes blinking orange if the active call is placed on hold.
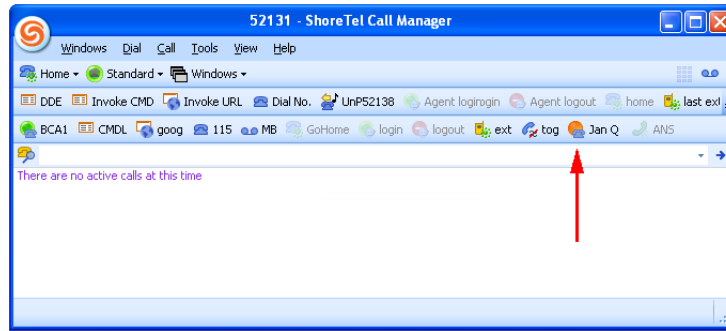
Figure 45   Extension Monitor – Park button

The user retrieves a parked call from the monitored extension by pressing the blinking button.

Call Handling Mode Delegation

Introduction

Definition

ShoreTel 9 expands Call Handling Rule Delegation by permitting users to designate other users that can change their current call handling mode. As originally implemented, CHM delegation permissions were managed by an administrator through Director.

Users modify the current call handling mode of other users through the following tools:

- **Operator Call Manager**, by right clicking a user in the Contact Viewer.
- **Web Access Client**, by selecting *Other -> CHM Delegation*.

Refer to the Glossary for a definition of the following terms used in this release note:

- Active Call Handling Mode (or Current Call Handling Mode)
- Call Handling Mode

Implementation

The table at the bottom of the **Options and Preferences: Call Handling Mode** panel, shown in Figure 46, lists the users that can change the subject's current call handling mode. The table includes users added to the table by the subject and users that received access to the subject's current call handling mode through Director.
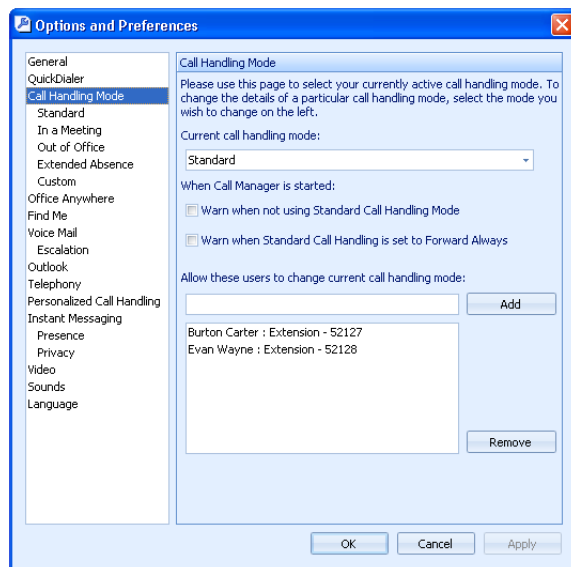
Figure 46   Call Handling Mode panel

The following procedure adds a user to the list of users allowed to change the current Call Handling Mode.

Step 1 Select the Call Handling Mode in the panel directory on the left side of the window.

Step 2 Type a name or number in the edit box, as shown in Figure 47.

A drop down menu displays a list of system users, filtered by the edit box contents.
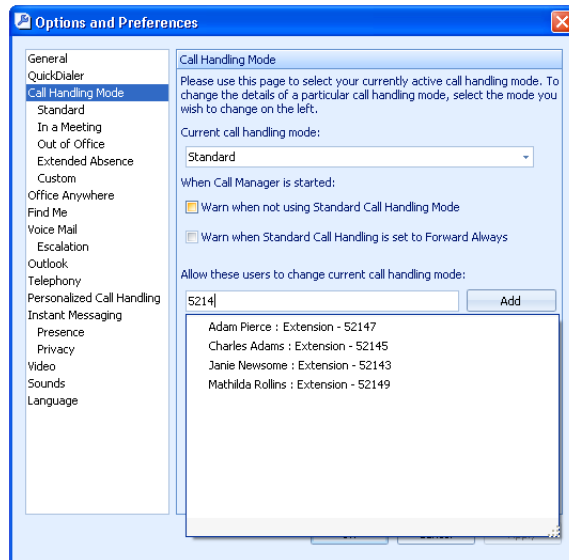
Figure 47   Entering the Names of Users allowed to Change the Mode

Step 3 Select the Add button to add a user to the list:

Parameters added to the Call Handling Mode panel include:

- **Allow these users to change current call handling mode:** The edit box is a Quick Dial type window. Entering a name or number in the data entry field results in a drop down menu that lists all matching user names or numbers. The drop down only displays user extensions. Workgroups and system extensions are not displayed.

  The table below the edit box contains the list of users allowed to change the current call handling mode of the subject.

  — **Add button:** Click this button to add the user listed in the edit box to the table.

  — **Remove button:** Select this button to remove the highlighted user/users from the list of users.

Voicemail Enhancements

Introduction

Definition

ShoreTel 9 Voicemail enhancements include:

- Voicemail Timestamps standardization
- Voicemail Deletion Notification Control

Refer to the Glossary for a definition of the following terms used in this release note:

- Site

Voicemail Timestamps

Background

The time stamp of voice messages is based on the time of the server where the message is received. For example:

- The timestamp on messages viewed in Call Manager or Outlook is adjusted to match the time zone setting on the user's computer.

- The timestamp on messages accessed though voicemail is based on the time of the server handling the voicemail call.

Feature Description

When a user accesses voice mail from a telephone, message timestamps are based on the time zone setting of the site to which the phone is associated. If a phone is not assigned to a ShoreTel site, such as an external phone, the message timestamps are based on the site to which the user is assigned.

Message timestamps displayed by Call Manager are based on the computer's time zone setting.

Implementation

The timestamp setting is not configured or controlled from Director.

Voicemail Deletion Notification Control

Background

The **Auto-delete by Number of Days** feature allows a system administrator to set a maximum time limit for retaining messages. When the feature is enabled and a user has messages approaching the retention limit, the user receives a message warning of the imminent message deletion. The range of valid retention periods is between 30 and 2000. days.

The first warning is sent two weeks before the expiration deadline. A second message is sent one week prior to the deadline. After the time limit passes, the user receives a message stating that the messages were deleted.

Description

ShoreTel 9 provides administrator control over Voicemail deletion notification messages. Voicemail deletion message notification control is a Class of Service setting.

Implementation

Voicemail Deletion Notification is controlled from the Class of Service: Voice Mail Permissions panel, shown in Figure 48. To access the Class of Service: Voice Mail panel, select *Administrator -> Users -> Class of Service* from the Director Main Menu, then click the desired service class in the *Voice Mail Permissions* section at the bottom of the list.

To enable the sending of voice mail deletion notification messages, select **Enable Auto-Delete Notification** at the bottom of the panel. This option is available only if **Delete Saved / Unheard Messages after (30 - 2000) days** or **Delete Heard Messages after (30 - 2000) days**.

When at least one message options is selected, the *Enable Auto-Delete Notification* default setting is *enabled*.

Figure 48   Enable Auto-Delete Notification

Client Devices

IP 110 – On-Hook Dialing

Introduction

ShoreTel 9 adds On-hook Dialing to the IP110 ShorePhone.

Description

On-hook dialing supports number dialing by pressing keyboard digits without picking up the handset. When dialing a number without picking up the handset, ringback and the connected call media stream is played through the IP110 speaker.

Because the IP110 does not have a microphone, users must pick up the handset to speak to the other party. The mute button remains lit while the IP110 is on-hook; pressing the mute button at this time has no affect.

On-hook dialing on the IP110 is typically used when checking voicemail through the speakerphone or to avoid picking up the headset until a call is answered.

The Redial button can initiate calls while the IP110 is on-hook. The Mute key is red when the audio path is through the speaker.

The IP110 cannot initiate Intercom calls on-hook.

Implementation

IP110 Phone firmware version 2.4.0 supports on-hook dialing. Any firmware older than 2.4.0 does not support this feature.

Call Manager – IM Privacy

Introduction

Definition

IM Presence Privacy is a ShoreTel 9 feature that provides users the capacity to manage the visibility of their IM presence status. Restricting access to IM Presence information also prevents blocked users from sending instant messages to users restricting their access.

Refer to the Glossary for a definition of the following terms used in this release note:

- Instant Messaging
- Presence
- QuickDial Field

History

ShoreTel 8 introduced Instant Messaging as a Call Manager feature available on Professional, Workgroup Agent, Workgroup Supervisor, and Operator Call Manager.

Description

Privacy States

Presence privacy states define the IM interaction status between two system users. Users restrict access to their IM presence state by assigning a privacy state to other users. ShoreWare defines two presence privacy states:

- **Allowed**: This state indicates that the requested party has received access to the user's IM presence status.

- **Blocked**: This state indicates that the requested party was denied access to the user's IM presence status.

  A user's IM presence state appears as *Offline* to all users whose state is *Blocked*.

- **Pending:** This state indicates that the user has not responded to the party's request for IM presence status.

  Until the requested user responds to a presence request, the presence state of that user depends on the type of presence server that the user accesses:

  — **OCS 2007:** Contact's presence is displayed until access is blocked
  — **Conference Bridge 7.1:** Presence state is offline until access is allowed

The default setting is *Blocked.*

Requesting Presence Access

Call Manager provides the following methods of requesting access to a user's presence state:

- adding the user to the Contact list
- calling the user
- sending the user an Instant Message

Administrators can configure Class of Service options to require users to approve privacy requests or to automatically accept all requests. Users that are required to approve privacy requests are only able to view other users privacy from the Contact list.

Contacts that are denied access to a user's presence information appear as *Offline* in the user's Contact list and QuickDialer fields. Contacts can send instant messages to only users that grant them access to presence privacy information.

A popup window notifies the recipient concerning a presence access request. The recipient responds to the request by marking the checkboxes of contacts, then pressing the OK button. Contacts that are not checked when the OK button is pressed are denied access to the user's presence information. Figure 49 displays a privacy request notification popup.
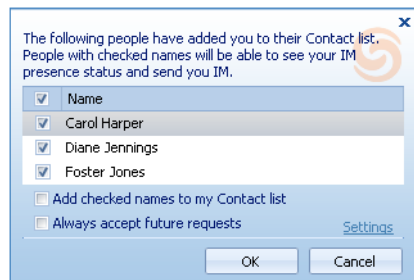
Figure 49   Notification popup

Users do not receive instant messages from other users for whom the privacy state is *Blocked.* Presence access requests are also blocked from these users.

Implementation

Although presence privacy settings are configured by each user, ShoreWare provides tools for administering IM presence access requests on a system or user basis. Presence access requests for the entire ShoreTel system are administered through Class of Service settings. Presence access requests for users are configured through Call Manager.

System Privacy Invitation Settings

System IM presence privacy is a Telephony Class of Service parameter. Class of Service settings have priority over settings configured by individual users.

To set the Presence Invitation Handling parameter for a telephony class of service:

Step 1   Open the Class of Service panel by selecting *Administration -> Users -> Class of Service* from the Director main menu.

Step 2   Select the desired Telephony Features Permission Class.

Director opens the Edit Class of Service panel, as shown in Figure 50.

Step 3   Select the desired option from the IM Presence Invitation Handling drop-down.

Valid setting options for IM Presence Invitation Handling include:

- **User defined**: Each user's method for handling presence requests is specified by the Call Manager Options and Preferences setting.

Figure 50   Presence Invitation Handling parameter

- **Auto accepts Invitation**: All user invitations are accepted. Notification popups are displayed when a user receives a request to indicate a requestor was granted access to the recipient's presence settings.

- **Prompt to Accept Invitation**: Users receive a popup when another user requests access to their presence. The recipient processes the request by clicking an option on the popup.

The Class of Service setting does not affect the user's Call Manager configuration. The Call Manager Invitation Handling setting persists even when overridden by the Class of Service. The Call Manager setting becomes active if the CoS service is set to *User Defined.*

User Privacy settings

Users control their IM presence access settings from the Options and Preferences: Instant Messaging-Privacy panel, as shown in Figure 51.

Figure 51   Options and Preferences: Instant Messaging – Privacy panel

Privacy Invitation settings

The Privacy Invitation settings section, located at the top of the Instant Message-Privacy panel, determines the user's Presence access request method when the CoS for the user is set to *User Defined.*

The invitation handling section provides the following options:

- **auto accept invitation**: All requests are accepted. When a user receives a request, a notification popup indicates a requestor was granted access to the user's presence.

- **prompt to accept invitation**: The user receives a popup when a another user requests presence access. The request is processed by clicking a popup option.

When the Class of Service is not set to *User Defined*, this option is read only.

Presence Permissions table

The Presence Permissions table, located at the bottom of the Instant Message-Privacy panel, configures the presence access setting for listed users. Users in the table are assigned one of the following permissions:

- **Allowed**: Presence information is available to users that are set to this value.

- **Blocked**: Presence information is not available to users that are set to this value. Instant Messages and presence access requests from the user are blocked.

- **Pending:** This state indicates that the user has not responded to the party's request for IM presence status.

To add a user to the list, press the Add button located below the table.

To edit a user's permission setting, select the user in the list and press the Edit button.

To remove a user from the list, select the user in the list and press the Delete button.

To sort by name or permission, click on the column heading of the desired key.

To search for a name, click the Name column heading, then start typing the desired name.

Presence Change Alerts

Users can mark a contact to determine when that contact has terminated a phone call or an instant message session. Call Manager then informs the user when the contact has changed their presence. Users that can access a contact's IM presence information receive notification of IM or telephony presence changes. Users that are denied access to a contact's presence information can only receive notification of that contact's telephony presence change.

To mark a contact for a presence change alert, right click the desired contact in the Contact List and select Alert When Available on the context menu. If that contact is on the phone or in an Instant Message session, Call Manager displays the popup shown in Figure 52 when that contact completes the call or session. If that contact is not on the phone or a session, the popup is displayed after the contact subsequently begins a call or session, then terminates it.

Pressing the snooze button closes the popup for the period listed on the button. If the contact is still available after the period elapses, the popup is displayed again. If the contact is not available, the popup is displayed immediately after the contact becomes available.
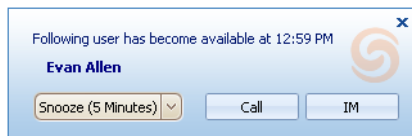
Figure 52   **Presence Change Alert popup**

Installation

New Installations

In newly installed systems:

— Invitation handling for all users is set to *Prompt*.
— IM Presence Invitation Handling for all Service Classes is set to *Prompt*.

Upgrade

Upgrading a ShoreTel system performs the following actions:

• Server upgrade from Version 8.1

— Invitation handling for all users is set to *Prompt*.
— IM Presence Invitation Handling for all Service Classes is set to *Auto Accept*.

• Server upgrade from Version 7.5

— Invitation handling for all users is set to *Prompt.*
— IM Presence Invitation Handling for all Service Classes is set to *Prompt*.

• Call Manager upgrade

— Call Manager sends requests to everyone in the user's Contact list.

When an upgrade changes the CoS or individual user mode setting to *prompt after server upgrade,* users may initially receive popups listing multiple presence access requests.

Presence Server Support

Presence servers differ in maintaining privacy list and generating requests. This section lists the privacy differences between servers that support IM presence.

	OCS 2007	**eDial**
List types	Three lists are maintained: 1.New subscription list 2.Permissions 3.Contact list	One list is maintained.

Table 5   **Presence Access Settings for Supported Presence Servers**

	OCS 2007	eDial
Presence state of new contacts	Contact's presence is displayed until access is blocked.	Presence state is offline until access is allowed.
Request Generation	Each time new subscribers enter.	Only first time new subscribers enter.
Privacy and Contact lists	Privacy and Contact lists are separate.	Permission and Contact lists are same entity.
	Subscriber and permission lists are separate. Deleting user permission list does not generate new notification.	Permission list displays only users on contact list.
	State of users deleted from permission list is *Show Status*.	Users removed from Contact list are removed from Permission list; presence state does not change.
		Delete operation does not remove entry from Permission list. Delete operation sets presence state to *Don't Show Status*.

Table 5   Presence Access Settings for Supported Presence Servers

Call Manager – Contact Import

Introduction

ShoreTel 9 Call Manager supports the import of data records from CSV or XML files for display in the Directory Viewer. The CSV and XML files contain lists of personal contacts and are formatted specifically for integration with Call Manager.

The CSV and XML files are not modified by the import process, nor are the contacts permanently added to the user's Call Manager database.

Description

Call Manager caches CSV or XML file contents at start-up and after each file change. The data is available in the Directory Viewer, Contacts Viewer, and QuickDialer. Call Manager reports errors during the cache process to the user and in log files. Call Manager receives records from all properly formatted CSV and XML files in the target directory.

Implementation

The following sections describes the steps required for Call Manager to import records from a data file. File Properties on page 105 describes the properties of CSV and XML import files.

Editing the Registry

Call Manager reads data files located in a directory specified by the following registry key:

Location: HKEY_CURRENT_USER\Software\Shoreline Teleworks\ShoreWare Client
Key: ContactImportLocation.

The value in this registry is a string. The default value of this key is a string that points to the Contacts directory in the user profile directory:

C:\Documents and Settings*username*\Application Data\ ShoreWare Client\Contacts

The registry entry can point to a PC location or a server path.

WARNING   Windows registry changes are effective immediately, and backups are not created automatically. Only experienced personnel should attempt registry changes.

Figure 53 displays the registry editor after insertion of the ContactImportLocation key. This registry is set up such that Call Manager will import records from CSV and XML files located in Bonnie Hopkin's CM_Import folder

Placing the File

Properly configured CSV and XML files placed in the folder specified by the ContactImportLocation key are immediately cached to Call Manager. Changes to these files are visible when the edited file is saved.

When a file is removed from the folder, the contacts listed in that file remain in the Directory Viewer until Call Manager is exited. Contacts removed from a file also remain in the Directory Viewer. When Call Manager is started again, all records removed by contact deletion or file removal do not appear in the Directory Viewer.
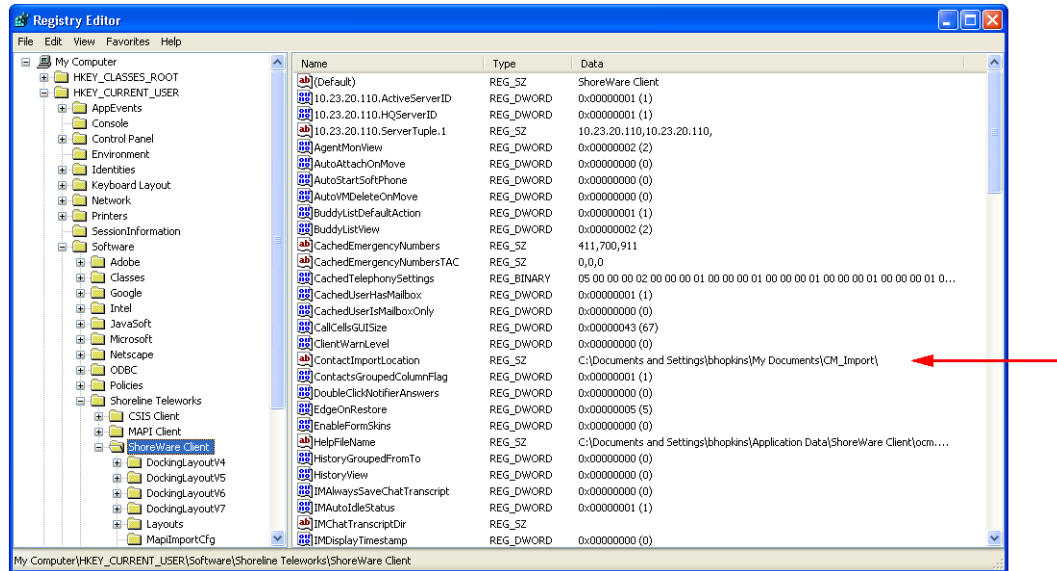
Figure 53   ContactImportLocation key viewed in the Registry Editor

Viewing the Contacts

Directory View

Contacts imported from CSV or XML files appear in the Directory Viewer, as shown in Figure 55. When contacts are grouped by data source, they appear under a heading that lists the Data Source. When the contacts are grouped by company or not grouped, the Data Source column indicates either the name of the originating file or the contents of the Name field in the originating file.
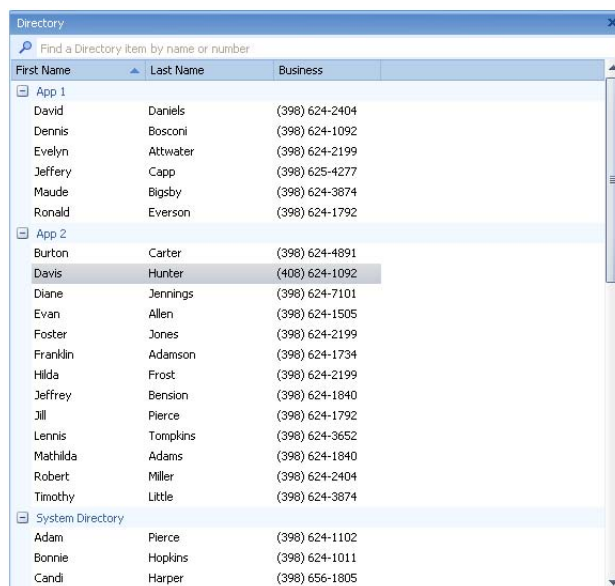
Figure 54   Directory Viewer containing Imported Records

Directory Item Details

Details of contacts imported from the CSV or XML files are visible from the Directory Item Details panel, access by right clicking a contact and selecting **View Directory Item Detail**. The Directory Item Details panel, as shown in Figure 55, indicates the source of the file in the first data field and states that the record contents are not editable.

Figure 55   Directory Item Details

Quick Dialer

The imported CSV/XML file contacts will be available in all QuickDialer controls. They will appear in the list just like any other contact.

File Properties

Data Fields

File Heading Fields

File heading fields provide a description of the record source within the Directory Viewer. The Source and Version fields are typically listed in the same CSV or XML line. Only one instance of each field should be provided in a contact file.

The following are the subdirectory heading fields:

- **Source**: This field is associated with all file records in Call Manager and corresponds to the *Data Source* column in the Directory Viewer. Typically, this value is set to the original source of the file contents.

  When this field is not included, Call Manager uses the CSV or XML file name as the *Data Source* contacts imported into the Directory Viewer.

- **Version**: This field displays the version of the contact information. When included, this field must be set to 1.0.

Column Heading Fields

Unless otherwise specified, a contact record should contain only one instance of each field. The only mandatory data entry field is **Contact ID**. At least one name field and one other column heading field must contain information for each contact.

The column heading fields include the following:

- **Contact ID**: This field uniquely identifies the contact record within the file. The Contact ID is a string with a maximum of 126 characters. Call Manager does not display this field. All contact records require a Contact ID. If multiple contact records contain identical Contact IDs, the last such contact in the list is imported into Call Manager and all other contacts with the same ID are ignored.

- **First name**: This field contains the contact's first name.

- **Middle name**: This field contains the contact's middle name.

- **Last name**: This field contains the contact's last name.

- **Company**: This field contains the contact's company name.

- **Department**: This field contains the contact's department name.

- **Phone numbers**: This field contains the contact's phone numbers. A contact record may contain more than one phone number as follows:
    - *Business:* two fields (Business, Business 2)
    - *Home:* two fields (Home, Home 2)
    - *Mobile:* one field (Mobile)
    - *Pager:* one field (Pager)
    - *Fax:* one field (Fax)

- **Email addresses**: This field contains the contact's addresses. A contact record may contain three email addresses (Email Address, Email Address 2, Email Address 3).

- **IM**: This field contains the contact's instant messaging address.

- **Categories**: This field provides a method of grouping contacts.

CSV Files

CSV files contains records, each of which consists of data fields. The following sections describe the composition of CSV file fields and records.

Field Composition

Each field denotes one property for the file or for one contact. The field entries must conform to the following syntax rules:

- Data is of type *strings* and supports UTF-16 encoding.

- Fields that contain a double quote must be surrounded by double quotes. Double quotes are indicated by two double quotes.

    Example 1: A "tiny" space -> "A ""tiny"" space""
    Example 2: "Joe" -> """Joe"""
    Example 3: "Red" Wagon -> """Red"" Wagon"

- Fields that contain commas must be surrounded by double quotes.

    Example 1: "ShoreTel, Inc."

◎ ShoreTel®

- Fields that do not contain double quotes or commas with double quotes may be surrounded with double quotes.

- Data fields with no information translate into blank entries in Call Manager.

Record Types

Each line in a CSV files corresponds to one data record. The end of a record is denoted by a Carriage Return and Line Feed.

Call Manager CSV integration files define three types of records

- **File Information Record**: The File Information Record denotes the Source of the data and the Version of the file. Inclusion of this record in the CSV file is optional. When it is included, the File Information Record must be the first record in the file.

  — **Source**: This field is associated with all file records in Call Manager and corresponds to the *Data Source* column in the Directory Viewer. Typically, this value is set to the original source of the file contents.

  When this field is not included, Call Manager uses the CSV or XML file name as the *Data Source* contacts imported into the Directory Viewer.

  — **Version**: This field displays the version of the contact information. When included, this field must be set to 1.0.

  Source and Version variable declarations must conform to the following:

  — Syntax for the Source variable is `Source=sourcetext`.
  — Syntax for the Version variable is `Version=versionname`.
  — The Source and Version variables are optional.

     Example 1: "Source=Lotus","Version=1.0"
     Example 2: Source=Lotus, Version=1.0

- **Contact Header Record**: The Contact Header Record is mandatory and lists the names of the fields that the file lists for the contacts. The Contact Header Record is located immediately after the File Information Record. If the file does not contain a File Information Record, the Contact Header Record is the first record in the file.

  Although field names correspond to Directory Viewer heading names, the field name and heading name are not identical.

  The following is a list of valid field names for CSV import files:

  — **Contact ID**: This field uniquely identifies the contact record within the file. The Contact ID is a string with a maximum of 126 characters. Call Manager does not display this field. All contact records require a Contact ID. If multiple contact records contain identical Contact IDs, the last such contact in the list is imported into Call Manager and all other contacts with the same ID are ignored.

    Call Manager does not display the contents of this field.

  — **First name**: Directory Viewer displays contents under the First Name column.

  — **Middle name**: Directory Viewer displays contents under the Middle Name column.

  — **Last name**: Directory Viewer displays contents under the Last Name column.

  — **Company**: Directory Viewer displays contents under the Company column.

  — **Department**: Directory Viewer displays contents under the Department column.

  — **Business Phone**: Directory Viewer displays contents under the Business column.

— **Business Phone 2**: Directory Viewer displays contents under the Business 2 column.

— **Home Phone**: Directory Viewer displays contents under the Home column.

— **Home Phone 2**: Directory Viewer displays contents under the Home 2 column.

— **Mobile Phone**: Directory Viewer displays contents under the Mobile column.

— **Pager**: Directory Viewer displays contents under the Pager column.

— **Business Fax**: Directory Viewer displays contents under the Fax column.

— **Email Address**: Directory Viewer displays contents under the Email column.

— **Email2 Address**: Directory Viewer displays contents under the Email2 column.

— **Email3 Address**: Directory Viewer displays contents under the Email3 column.

— **IM Address**: Directory Viewer displays contents under the IM column.

— **Categories**: Directory Viewer displays contents under the Categories column.

Example 1: "Contact ID","First Name","Last Name", "Business Phone"

- **Contact Record**: The file contains one record for each contact that is integrated into the Directory viewer. The order of data fields in each contact record must be identical to the fields in the Contact Header Record.

Example 1: "ID_100","Johnny","Fracas", "398-212-0012"
Example 1: ID_100,Johnny,Fracas, 398-212-0012

CSV Examples

The following is an example of a CSV file where all fields are surrounded by double quotes:

"Source=Lotus","Version=1.0"

"Contact ID", "First Name", "Middle Name", "Last Name", "Company", "Department", "Business Fax", "Business Phone", "Home Phone", "Mobile Phone", "Pager", "Categories", "Email Address"

"1234","Maude","June","Bigsby","Anycorp, Inc.","",,"(398) 777-8888"

"1235","David","""Doc""","Daniels","Anycorp, Inc.","Software Engineering","(398) 331-9999","(408) 331-3662","(650) 999-1212","(398) 218-9898","(398) 222-3434","New Customer","Ddaniels@anycorp.com"

The following is an example of a CSV file where only fields with commas and double quotes are surrounded by double quotes:

Source=Lotus,Version=1.0

Contact ID,First Name,Middle Name,Last Name,Company,Department,Business Fax,Business Phone,Home Phone,Mobile Phone,Pager,Categories,Email Address,IM Address

1234,Maude,June,Bigsby,"Anycorp, Inc.",,,(398) 777-8888,,,,,,

1235,David,"""Doc""",Daniels,"Anycorp, Inc.",Software Engineering,(398) 331-9999,(398) 331-3652,(398) 929-1212,(398) 888-9898,(398) 222-3434, New Customer, Ddaniels@anycorp.com, Ddaniels5000@yahoo.com

XML Files

XML files contain a structure set of elements. The following sections describe required file components and XML elements recognized by Call Manager.

XML File Name

Elements

The following elements are recognized by Call Manager Contact XML files.

Level 1 Elements

Each file contains one **Contacts** element.

- **Contacts**: The Contacts element specifies the source name and version number and contains one Contacts element for each contact in the file.

  — *valid attributes*: source, version

  Example: <contacts source = "File 1" version = "1.0"> </contacts>

Level 2 Elements

The *Contacts* element contains one *Contacts* element for each user defined by the XML file. Each Contacts element contains Level 3 elements that define the field contents for the user. Each Contacts element must contain one ContactID element and one other Level 3 element.

Refer to the Example on page 111 for an example of the Contacts element.

Level 3 Elements

Level 3 elements are contained with the Contacts element and specify field contents for contacts imported to Call Manager. The following is a list of Level 3 elements.

- **contactID**: This field uniquely identifies the contact record within the file. The Contact ID is a string with a maximum of 126 characters. Call Manager does not display this field. All contact records require a Contact ID. If multiple contact records contain identical Contact IDs, the last such contact in the list is imported into Call Manager and all other contacts with the same ID are ignored.

  Example: <contactID>1234</contactID>

- **name**: This element specifies the contact's name. Each contact element may contain only one name element.

  — *valid attributes*: first, middle, last

  Example: <name first="Sarah" middle="Jane" last="Clauser"/>

- **company**: Each contact element may contain only one company element.

  — *valid attributes*: value

  Example: <company name="Anycorp, Inc."/>

- **department**: Each contact element may contain only one department element.

  — *valid attributes*: value

  Example: <department value="Sales"/>

- **categories**: Each contact element may contain only one categories element.

— *valid attributes*: value

Example: <categories value="Austin"/>

- **phone**: This element specifies the contact's phone numbers. A contact element may contain multiple phone elements, subject to the following:

    — *valid attributes*: type, name, value

    Type: The type attribute must be equal to one of the following: Business, Home, Mobile, Pager, and Fax.

    - ✳ An element may contain 2 phone elements with name is equal to **Business**
    - ✳ An element may contain 2 phone elements with name is equal to **Home**
    - ✳ An element may contain 1 phone elements with name is equal to **Mobile**
    - ✳ An element may contain 1 phone elements with name is equal to **Pager**
    - ✳ An element may contain 1 phone elements with name is equal to **Fax**

    Name: The name attribute specifies the label of the Call Manager Directory Viewer column heading. If a name value does correspond to a standard column heading label, Call Manager creates a new heading.

    Value: The value attribute specifies the phone number that appears in the Directory Viewer data field label of the Call Manager Directory Viewer column heading. If a name value does correspond to a standard column heading label, Call Manager creates a new heading.

    Example 1: <phone type ="Business" name="Business 2" value= "+1 (398) 244-2489"/>
    Example 2: <phone type ="Pager" name="Pager" value= "+1 (398) 298-231"/>

    If multiple Phone Type elements have the same name attribute, Call Manager uses the first string and ignores all duplicate entries.

- **email**: This element specifies the contact's email addresses. A contact element may contain a maximum of three email elements, subject to the following:

    — *valid attributes*: name, value

    Name: The name attribute specifies the label of the Call Manager Directory Viewer column heading. If a name value does correspond to a standard column heading label, Call Manager creates a new heading.

    Value: The value attribute specifies the email address that appears in the Directory Viewer data field.label of the Call Manager Directory Viewer column heading. If a name value does correspond to a standard column heading label, Call Manager creates a new heading.

    Example 1: <email name="email 2" value= "apierce@anycorp.net"/>
    Example 2: <email name="email" value= "adam.pierce521@yahoo.net"/>

- **IM**: This element specifies the contact's instant messaging address. An contact element may contain only one IM element.

    — *valid attributes*: name, value

    Name: The name attribute specifies the label of the Call Manager Directory Viewer column heading. If a name value does correspond to a standard column heading label, Call Manager creates a new heading.

    Value: The value attribute specifies the IM address that appears in the Directory Viewer data field label of the Call Manager Directory Viewer column heading. If a name value does correspond to a standard column heading label, Call Manager creates a new heading.

Example

The following is an example of a Call Manager Contact Integration XML file:

```xml
<?xml version="1.0" encoding="utf-8"?>
<contacts source="Lotus" version="1.0">
  <contact>
    <name first="Sarah" middle="" last="Clauser"/>
    <company value="Anycorp, Inc."/>
    <department value="Finance"/>
    <contactID>1234</contactID>
    <phone type="Business" name="Business" value="+1 (398) 122-2558"/>
    <phone type="Business" name="Business 2" value="+1 (398) 122-2558"/>
    <email name="Email" value="Sclauser1021@anycorp.org"/>
    <email name="Email Address 2" value="sclauser@yahoo.com"/>
    <IM name="IM" value="sclauser1021@aol.com"/>
  </contact>
  <contact>
    <name first="Tammy" middle="" last="Masoon"/>
    <company value="Anycorp, Inc."/>
    <department value="Sales"/>
    <contactID>2234</contactID>
    <phone type="Home" name="Home" value="+1 (398) 962-2552"/>
    <phone type="Pager" name="Pager" value="+1 (398) 529-8670"/>
  </contact>
  <contact>
    <name first="Greg" middle="" last="Thilmonda"/>
    <company value="ShoreTel, Inc."/>
    <department value="Sales"/>
    <contactID>3234</contactID>
    <email name="Email" value="gthilmonda@anycorp.com"/>
  </contact>
  <contact>
    <name first="Patrick" last="Farrington"/>
    <contactID>4234</contactID>
    <phone type="Business" name="Business" value="+1 (398) 331-3642"/>
    <phone type="Mobile" name="Mobile" value="+1 (398) 666-5113"/>
    <phone type="Fax" name="Fax" value="+1 (398) 331-3642"/>
    <email name="Email" value="PFarrington@anycorp.com"/>
    <IM name="IM" value="PFarrington@aol.com"/>
  </contact>
</contacts>
```

Mobile Call Manager – Location Based Service

Introduction

Definition

ShoreTel 9 adds Location Based Service functions to Mobile Call Manager (MCM).

Refer to the Glossary for a definition of the following terms used in this release note:

- Active Call Handling Mode
- Call Handling Modes
- Coordinate
- Global Positioning System
- Location based service
- Office Anywhere
- Office Anywhere Extension
- Waypoint

History

MCM, introduced in ShoreTel 7.5 provides mobile device access to selected Call Manager features. The MCM implementation includes the client application that runs on cell phones and the server component – Mobile Call Manager Server (MCMS) – that runs on any ShoreWare application server.

ShoreTel 8.1, extended Mobile Call Manager access to new audiences through carrier independence and support of additional European and American languages.

Description

Definition

MCM Location Based Services (LBS) uses GPS to identify device location. MCM users can customize call management on the basis of the device location.

Users define waypoints based on known locations and associate a Call Handling Mode (CHM) or Office Anywhere (OA) destination with each waypoint. When the device moves into a region covered by a waypoint, MCM changes the active CHM or OA destination as specified by the waypoint.

WARNING   Calls placed through ShoreTel to Office Anywhere numbers are dropped if the OA setting changes during the calls. Scenarios that may result in dropped OA calls include:

- Moving through different waypoints when MCM is running – even if only in the background – and LBS is enabled while both phone and network are capable of simultaneous data and voice communications.

- OA is set for a home or office phone and MCM is turned on in a location identified by a waypoint as valid for a different calling device.

Process Description

Preparation

Before a mobile device can run MCM LBS, the user must configure the polling method and waypoint set.

- **Polling Method**: The polling method specifies the conditions under which the device searches for a GPS signal. Before LBS can be enabled, the polling method and frequency must be configured.

  MCM LBS defines two polling conditions:

  — After an *On-Use interrupt*.

    An On-Use interrupt is an event that enables MCM as the foreground application. MCM becomes the foreground application when the user accesses any MCM function or moves MCM to the foreground. In this case, MCM polls for LBS coordinates after each event that enables MCM as the foreground application.

    This method is the default setting and is recommended because it has the smallest device battery life impact.

  — After periodic intervals

    Users can configure MCM to poll once each hour or once each fifteen minutes. Periodic polling can significantly affect the device battery life.

- **Waypoint Set**: A waypoint is an MCM data point that associates an action with a specified location. When the device receives a GPS signal in the location specified by a waypoint while MCM is the foreground application, MCM performs the action defined by the waypoint.

  Each waypoint defines a region in terms of a point (longitude and latitude) and range (radius). MCM actions associated with waypoints include changing the active Call Handling Mode or the active Office Anywhere extension.

  MCM allows the configuration of multiple waypoints.

Algorithm

The following describes the MCM LBS algorithm:

1. MCM polls for LBS as configured.

2. When MCM receives GPS coordinates that fall within a region specified by a waypoint, MCM changes the active CHM or OA destination settings to those associated with the waypoint. The ShoreTel system routes calls to the destination specified by the new setting.

   When LBS coordinates do not fall within the range of any waypoint, MCM sets the active CHM and OA destination as follows:

   - If the user has specified an OA Default Destination, MCM sets the OA destination to that value.

   - If the user has not specified an OA Default Destination, MCM sets the OA destination to value specified by Call Manager or Web Access.

ShoreTel®

- The CHM setting remains unchanged.

Manual CHM or OA setting changes have higher priority than GPS generated settings. Manual settings remain in effect until the next GPS poll that meets the following criteria:

- LBS and waypoint are re-initiated.

- The new LBS coordinate either maps to a new waypoint or does not map to a waypoint.

  If the coordinate does not match a known waypoint, the default Office Anywhere extension is used.

Availability

MCM supports LBS features on the following devices (depending on carrier support):

- BB 9000 series
- BB 8300 series (requires a GPS dongle)
- BB 8800 series
- Nokia N95
- Nokia E90
- Nokia E61i

Devices supporting LBS must either have internal GPS hardware or the capability of connecting to an external device that provides GPS functionality such as dongles. The carrier must allow GPS on the device and allow third party applications, such as MCM, to use GPS functionality. External GPS devices may be used to enable LBS features on these devices, depending on carrier limitations.

Configuring LBS

LBS parameters are configured on the Location-based Services panel, as shown in Figure 56. To open the Location-based Services panel, select *Settings -> Location-based Services* from the Main Menu.

Figure 56   Location-based Services

Managing Location Based Services Activity

The **Enable Location-based Services** parameter, located at the top of the panel, controls activation of Location-Based Services. The checkbox located left of the text indicates the status; when the box is filled, Location-Based Services is enabled.

The parameter is a toggle setting – the LBS is enabled and disabled through the same procedure.

To change the Location Based Services activity:

Step 1 Select Enable Location-based Services with the cursor.

Step 2 Press the Menu button to display the context menu, as shown in Figure 57.
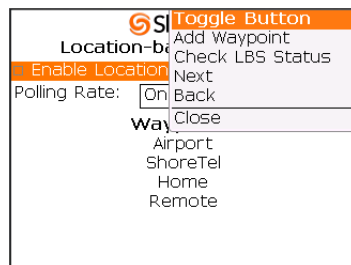
Figure 57   **Toggling Location-based Services Activity**

Step 3 Select Toggle button.

Step 4 Press the Trackball.

Polling Rate Selection

The **Polling Rate** parameter, located below the Enable Location-based Service parameter, specifies the condition and rate that MCM searches for a GPS signal. Valid parameter settings include

- **On Use**: Select this option to poll when any event that enables MCM as the foreground application – when the user accepts a call, accesses voicemail, or manually moves MCM to the foreground.

- **Every Hour**: Select this option to poll on 60 minute intervals.

- **Every 15 Minutes**: Select this option to poll on 15 minute intervals.

The Polling Rate selection significantly impacts the device battery life.

To change the Polling Rate:

Step 1 Select Polling Rate with the cursor.

Step 2 Select the Polling Rate drop-down menu, as shown in Figure 58.
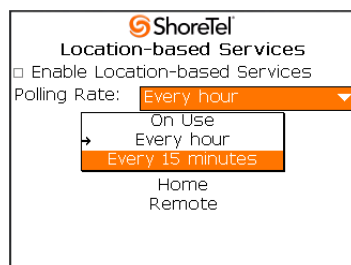
Figure 58   **Setting the Polling Rate**

Step 3 Scroll to, and select, the desired option.

Managing Waypoints

Waypoints are accessed from the Location-based Services panel, as shown in Figure 59. All configured Waypoints are listed below the Waypoint text. Office Anywhere numbers referenced by waypoints should be defined before configuring the waypoint.
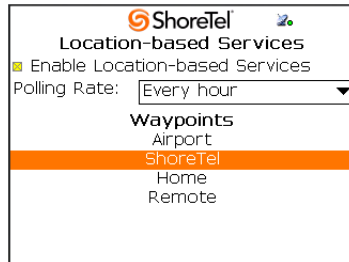
Figure 59   Selecting a Waypoint

- **To add a new waypoint**, press the Menu button and select *Add Waypoint*.

  The Waypoints Settings panel opens for the new waypoint.

- **To modify a waypoint's name or settings**, select the desired Waypoint, press the Menu button, and select *Edit Waypoint*.

  The Waypoints Settings panel opens for the specified waypoint.

- **To remove a waypoint**, select the desired Waypoint, press the Menu button, and select *Delete Waypoint*.

Adding or editing a waypoint opens the Waypoint Settings panel.

Waypoints Settings

The Waypoint Settings panel specifies the name, location, range, and action of the specified waypoint, as shown in Figure 60.
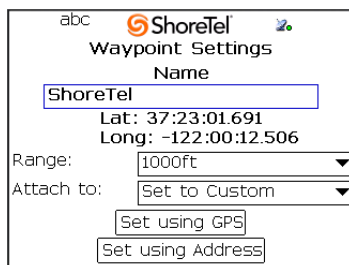
Figure 60   Waypoint Settings panel

- The **Name** is the label by which other panels refer to the waypoint.

- The **Lat** and **Long** denote the center of the waypoint. MCM waypoints do not reference altitude.

  — To set these parameters to the current location of the device, press the Set using GPS button.

  — To set these parameters to the location of a street address, press the Set Using Address button. MCM responds by displaying a form for specifying the desired location.

- The **Range** specifies the radius of the waypoint. Valid parameter settings depend on the language setting:

    — For English US or English UK, valid settings are 100 feet and 1000 feet.
    — For all other languages, valid settings are 100 meters and 1000 meters.

- The **Attach to** parameter specifies the parameter setting selected by MCM when it receives a GPS signal that is located within the region defined by the waypoint.

    Valid settings include all Call Handling Modes and all Office Anywhere numbers. The setting is activated when the device receives a GPS signal at the location specified by the waypoint.

LBS Indicators

MCM panels displays LBS icons that indicate activity and GPS reception. The Main Menu also displays LBS rule implementation status.

LBS Activity status

MCM panels displays a satellite dish icon in the top right corner when LBS is enabled, as shown in Figure 61.
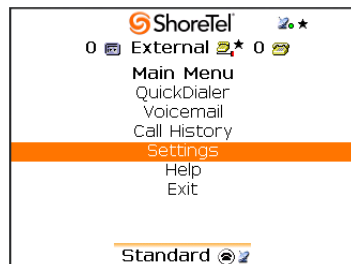
Figure 61   Indication Icons

GPS Reception Status

The GPS Reception Status icon appears as an appendage of the LBS Activity icon. The following icons denote reception results of the last polling attempt:

- **green circle**: indicates that coordinates from the most recently received GPS signal matched a waypoint.

    The icon in Figure 61 contains the green circle.

- **empty circle**: indicates that coordinates from the most recently received GPS signal did not match a waypoint.

- **dish (rotating)**: indicates MCM is searching for a GPS signal.

- **no icon**: indicates the device is not configured for LBS.

- E (**three red bars**): indicates a GPS or LBS error condition.

LBS Implementation Status

When the current Office Anywhere or Call Handling Mode is set because a waypoint matched a GPS signal, a satellite icon appears next to the setting. In Figure 61, the satellite icon appears next to the In a Meeting indicator at the bottom of the panel.

When manually selecting a current Call Handling Mode or Office Anywhere destination, the LBS initials indicate an option that is attached to at least one waypoint. Figure 62 displays three Call Handling Modes – Standard, Extended Absence, and Custom – that are attached to at least one waypoint.
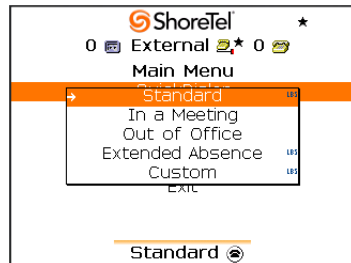
Figure 62   LBS Rule Indicators

Mobile Call Manager – Enhancements

Introduction

Definition

ShoreTel 9 enhances the following Mobile Call Manager (MCM) features:

- Office Anywhere
- Voicemail
- Call History
- QuickDialer
- Installation enhancements
- Navigating through messages using the existing TUI when using visual voicemail.

Refer to the Glossary for a definition of the following terms used in this release note:

- Active Call Handling Mode
- Call Handling Modes
- Office Anywhere
- Office Anywhere Extension
- Active Office Anywhere Extension
- Default Office Anywhere Extension

History

MCM, introduced in ShoreTel 7.5, provides mobile device access to selected Call Manager features. The MCM implementation includes the client application that runs on cell phone and the server component – Mobile Call Manager Server (MCMS) – that runs on any ShoreWare application server.

ShoreTel 8.1 extended Mobile Call Manager access to new audiences through carrier independence and support of additional European and American languages.

Feature Enhancements

Office Anywhere

ShoreTel 9 expands MCM to support the following Office Anywhere (OA) enhancements:

- Definition of multiple destinations for selection as the active Office Anywhere destination.

- Designation of a Default Office Anywhere number.

- Automatic enabling of Office Anywhere when MCM is activated.

Multiple Office Anywhere Numbers

MCM defines multiple OA extensions for each user. OA extensions are categorized as *Permanent* and *User Defined*.

- **Permanent Extensions:** Two permanent OA extensions are available for each user. Permanent extensions cannot be deleted or renamed. MCM permanent extensions include:

  — *Home Extension:* The Home Extension refers to the device connected to the user's home port, as configured through Director. You cannot modify, rename, or delete the Home Extension.

  — *External Extension:* The External Extension is specified from Call Manager or Web Access. A user cannot modify the External Extension from the MCM.

  Call Manager and Web Client specifies an active OA extension. The External Extension is set to this number if it is not assigned to one of the *User Defined Extensions*. Otherwise, the External Extension is set to the null value.

- **User Defined Extensions:** User defined extensions are created by the user. They differ from Permanent Extension if the destination is specified by the user and that the user can modify or delete them.

  Upon initial use, MCM provides an User defined OA extension named **Mobile Extension.** The Mobile Extension is specified during initial setup and provisioning by the user to the mobile device's phone number. The user can modify and delete the Mobile Extension setting.

To access the Office Anywhere Extensions panel, select *Settings -> Office Anywhere* from the Main Menu. The Office Anywhere Extensions, as shown in Figure 63, displays the names of all available OA extensions.
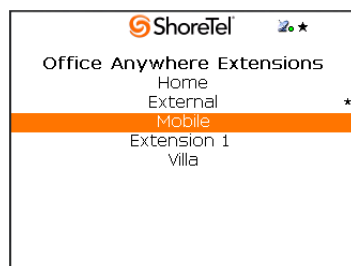
Figure 63   Office Anywhere Extensions panel

To add an Office Anywhere extension, press the Menu button in the Office Anywhere Extensions panel, then select *Add Extension* in the context menu.

To modify an existing Office Anywhere Extension, scroll to the desired extension in the Office Anywhere Extensions panel, press the Menu button, then select *Edit Extension* in the context menu.

MCM displays an edit panel for creating new extensions or modifying existing extensions, as shown in Figure 64. The user assigns a label and specifies the phone number in this panel. You can specify the default extension from this panel.

Some fields are not editable for various Permanent Extensions. These fields display a grey background.

Automatic Office Anywhere

This feature facilitates the receipt of calls on an MCM device without requiring execution of the OA configuration process every time a user turns on the device. When a user places a call or accesses voicemail through MCM, the *Active Call OA extension* is set to the *Default Office Anywhere Extension* number unless one of the following conditions is present:

Figure 64   Edit panel – User Defined Extensions

- A default OA extension is not selected.
- LBS is active and the Active OA Extension was specified by entry into the current waypoint.

Users can change the Active Office Anywhere extension by pressing the Menu button and selecting *Set Office Anywhere*. Manual changes to the Active OA extension have priority over changes generated by LBS but are lost when the user places a call or plays a voice message.

A maximum of one OA extension can be designated as the default extension. Initially, the Mobile Extension is set as the default; users can change the Default OA Extension through the Extension Edit Panel, as shown in Figure 64.

MCM denotes that a Default AO destination is defined by placing a star icon in the banner line at the top of all MCM panels. MCM denotes that the Active AO Extension is set to the Default extension with a star icon next to the Active Office Anywhere extension name in the status line of the Main Menu. Figure 65 displays the banner and status lines on the Main Menu.

Figure 65   Denoting Default OA Extension Status in Banner and Status Lines

Voicemail

ShoreTel 9 supports the following MCM voicemail access enhancements:

- After playing voicemail messages, users can access other voicemail menus and messages without reconnecting to voicemail.

- Voicemail preview messages are available through either the internal or external speakers.

- Voicemail message items in the mailbox are boldface when the message is marked *unheard*.

- When using the Advanced Voicemail or DTMF VM feature, the user can access all voicemail menu operations.

Call History

ShoreTel 9 supports the following MCM Call History access enhancements:

- Call History supports Delete and Delete All commands.

- Call History maintains 50 entries after changing OA settings or restarting the MCM server.

- The Missed Call counter is reset when the user views Call History.

- Call History displays the most recent missed call in bold.

QuickDialer

ShoreTel 9 supports the following MCM QuickDialer enhancements:

QuickDialer: Wild Card Search "e#b#"

MCM QuickDialer recognizes wild card characters for narrowing searches. Wild card usage is consistent with that of the "Directory" button on ShorePhones.

QuickDialer wildcard usage is subject to the following:

- Applies to both Directory and PIM
- Case and Diacritical insensitive
- Wild card characters used are "#", "*" and the space character " "

Wildcard character scope:

- # and space character replaces all remaining characters in the string
- The * character replaces only one character within the string

Example: The following strings filter the name "Mark Halsteam":

> M#H , Ma#H, M H, Ma H, M**k H, .

Settings – Disable PIM Entries

Users can enable or disable the loading of PIM entries into the Quickdialer list.

Installation Changes

Version Control

When MCM client is initiated by a user, it compares its software version to that of the MCM server. Software upgrades are initiated on the basis of that comparison.

- The Client and Server versions are identical.

  The client launches or resumes normally. No upgrade is required

- The Client and Server versions are different but compatible.

  MCM client displays a panel with an upgrade button and an *out of date* warning. The user can press the button to upgrade immediately or continue using the application. The panel is displayed each time the application starts until the user upgrades MCM.

- The Client and Server versions are different and incompatible.

MCM client displays an incompatibility warning message indicating that an upgrade is required. The panel includes an Upgrade button that sends the user to the URL that provides download access to updated application.

The MCM Client will not run until the new version has been installed and launched.

When a user initiates an upgrade, the device launches an Internet browser while exiting or moving MCM to the background. If the device is unable to launch a browser, it displays a URL link and instructs the user to open the link manually.

The following device types support automatic browser launching:

- Motorola
- Nokia
- Window Mobile

Permanent Configuration Storage

MCM stores configuration settings for a user's client device in the ShoreTel database. When a user changes mobile devices, these settings can be downloaded to the new device. While the user must still provision MCM on the new device, re-entering user information is obviated.

These settings are available to users who replace a device upon which MCM was installed or resets MCM to change the provisioning. The stored configuration does not replace the provisioned settings of an existing MCM device unless explicitly instructed by the user.

When a user provisions a replacement MCM device, settings for the new device are stored in the ShoreTel database after the provisioning is complete. MCM settings not required by the second device, such as LBS settings for a non-LBS device, are not retained.

ShoreWare Director does not indicate the existence or status of these settings.

Screen Size Notifications: Multi-Screen and Slider Devices
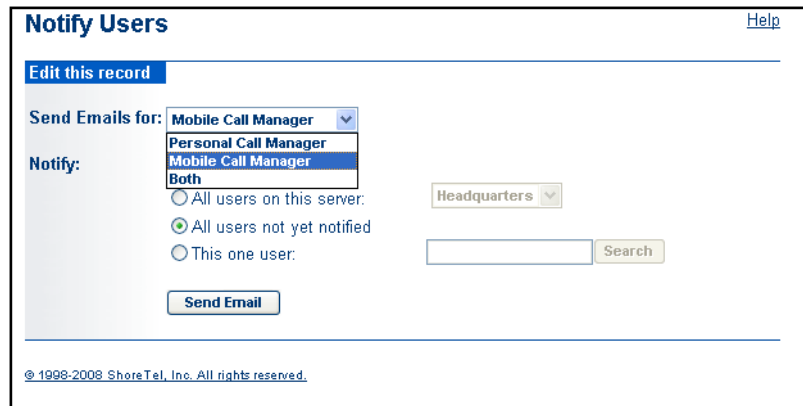
Although MCM support is provided for multi-screen and slider device, MCM is available in only one screen size or slider mode. On these devices MCM displays a message on the unsupported screen instructing the user to *Open the Phone* (multi-screen device) or *Move the Slider to the top* (slider device).

Client Notification of Upgrade

ShoreTel 9 MCM supports the automated disbursement of email messages to inform end users of an upgrade. The process is similar to that for Call Manager upgrades: the process is manually initiated through Director, after which the system sends an email message to all specified MCM end users.

To initiate an upgrade notification:

Step 1 Access the Notify Users panel in Director, as shown in Figure 66, by selecting *Administration -> Call Manager -> Notify Users* from the Main Menu.

Step 2 Select either *Mobile Call Manager* or *Both* from the **Send Emails for** drop-down menu.

Step 3 Specify the desired recipients by selecting a **Notify** radio button and completing the associated data entry fields.

Step 4 Press the **Send Email** button.

Figure 66   Notify Users panel – Selecting Mobile Call Manager

Director displays an Internet Explorer panel indicating that the notifications were sent.

Provisioning Changes

The provisioning server entry text field accepts alphanumeric characters for supporting DNS name entries.

Usage Changes

Character Input Mode indicator

MCM displays a character mode indicator in the upper right corner of the panel as follows:

- MCM displays **abc** in the upper right corner of the screen when the user selects a data entry field and the device is configured to enter alphanumeric characters.

- MCM displays **123** in the upper right corner of the screen when the user selects a data entry field and the device is configured to enter only numeric characters.

- MCM displays no indicator when a data entry field is not selected.

Support Information

Supported Devices

ShoreTel Version 9 supports MCM on the following mobile devices:

- Motorola RAZR V3
- Motorola RAZR V3xx
- Blackberry 7200 Series
- Blackberry 7290
- Blackberry 8100 Series (Pearl)
- Blackberry 8300 Series (Curve)
- Blackberry 8700 Series
- Blackberry 8800 Series
- Blackberry 9000 Series

- Nokia E61i Series
- Nokia E65 Series
- Nokia E90 Series
- Nokia N95 Series
- HTC Mogul Series (Sprint PPC – 6800 version only)

Feature Support

Although basic MCM functions are available on all supported devices, the implementation of some functions may vary between devices because of the inherent differences of the devices. The following sections list features that are available on selected models and the significant implementation differences between devices.

Location Based Services

MCM supports LBS features on the following devices (depending on carrier support):

- BB 9000 series
- BB 8800 series
- Nokia N95
- Nokia E90
- Nokia E61i

Devices supporting LBS must either have internal GPS hardware or the capability of connecting to an external device that provides GPS functionality such as dongles. The carrier must allow GPS on the device and allow third party applications, such as MCM, to use GPS functionality. External GPS devices may be used to enable LBS features on these devices, depending on carrier limitations.

Voicemail Preview

The following devices support Voicemail Preview over the speaker phone:

- Blackberry 8100 Series (Pearl)
- Blackberry 8300 Series (Curve)
- Blackberry 8700 Series
- Blackberry 8800 Series
- Blackberry 9000 Series
- Nokia E61i Series
- Nokia E65 Series
- Nokia E90 Series
- Nokia N95 Series
- Motorola RAZR V3
- Motorola RAZR V3xx

The following devices support Private Preview of Voicemail on the phone:

- Blackberry 8100 Series (Pearl)
- Blackberry 8300 Series (Curve)
- Blackberry 8800 Series
- Blackberry 9000 Series

PIM Integration

All listed Blackberry and Nokia devices support PIM entry import. The MCM settings panel provides an option to disable PIM loading for these devices.

RAZR V3 and Mogul devices do not support PIM.

Network Speed Setting

The default network speed setting on the Blackberry 7290 and Motorola RAZR devices is *Slow 2/2.5G/CDMA*. The default setting on all other devices is *High Speed/Wi-Fi*.

DTMF Handling

Some devices do not support DTMF signaling during a call when MCM is the foreground application.

In the Nokia N95, users can send DTMF signaling during a call as follows:

After pressing the Call button to answer a the call, press the Menu key twice; the first time places MCM in the background while the second time displays the dialer for sending DTMF signals.

Fonts

MCM displays text through custom font (bitmaps) or native OEM fonts.

- The Motorola RAZR V3 uses a custom font and includes a setting that specifies the font size.

- Native OEM fonts are used by all other devices that support MCM.

Glossary

802.1x A component of IEEE 802.1 group of networking protocols that addresses port-based Network Access Control. It provides an authentication mechanism for devices attaching to a LAN port to either establish a point-to-point connection or prevent the device from accessing the port if authentication fails. 802.1x is based on the Extensible Authentication Protocol (EAP).

ACD *see Automatic Call Distributor*

Active Call Handling Mode The active call handling mode is the CHM that is designated to specify the current method of handling a user's inbound calls. One mode is always active for each user. The active CHM is selected manually by the user or changes automatically based on the user's schedule.

Active Directory (AD) *Active Directory* is a Mircosoft technology that provides various network services, including LDAP-style directory services and authentication, for Windows environments. Administrators assign policies, deploy software, and apply critical updates to an organization from a single Active Directory database.

Active Office Anywhere Extension An OA Extension is the phone number where a user's callers are routed when the user has enabled Office Anywhere. *See Office Anywhere Extension and **Default Office Anywhere Extension**.*

AD *see Active Directory*

Advanced Encryption Standard (AES) *Advanced Encryption Standard* is a United States Encryption standard defined in Federal Information Processing Standard (FIPS) 192, published in Nov. 2001. AES is a symmetric block cipher which can process fixed 128-bit data blocks, using 128, 192 or 256-bit keys.

AES *see Advanced Encryption Standard*

Announced Find Me Announced Find Me is an option where the identity of an inbound caller is provided to the Find Me call recipient. Inbound callers may be required to record their spoken name before the call is connected.

Automatic Call Distributor (ACD) An Automatic Call Distributor is a system that distributes inbound calls to members, or agents, of the system.

Auto Find Me Auto Find Me is a Find Me option where a call recipient can program the system to immediately forward inbound call without requiring the caller to press "1".

Available DID numbers DID numbers within a range that are not assigned to a user or entity within the context of that range.

DID number availability within a range does not consider DNIS assignments. Numbers assigned as a DNIS number are still enumerated as *available* within a DID range; attempts to assign these DID numbers will be unsuccessful.

Bounced Call A bounced call is a parked call that is returned to the extension that parked the call because is was not picked up within a specified period.

Call Appearance A VoIP data structure that supports one voice call session.

Call Detail Record (CDR) A Call Detail Record is a data record containing statistics of a call that passed through a PBX or telephone exchange.

Information provided by a CDR includes the number of the originating party, the number of the recipient, the time that the call started, and the duration of the call. ShortTel CDRs contain additional information.

Call Handling Mode A call handling mode is a ShoreTel variable that defines a method of handling specified inbound calls. Each user is assigned five call handling modes, one of which is active and determines the user's current call handling method. *See Active Call Handling Mode.*

The five call handling modes assigned to each user are Standard, In a Meeting, Extended Absence, Out of Office, and Custom.

Call Handling Rule A call handling rule is the base unit of a Call Routing Plan that consists of a condition and action. When a call handling rule is active and the condition is satisfied, the action specifies the method by which the ShoreTel system handles the user's call.

Call Manager (client application) Call Manager is the ShoreWare client application that manages a user's calls, voicemail, and personal system settings through a graphical user interface.

Call Manager (switch) Call Manager is a ShoreGear module that handles MGCP information from the IP phones to which the switch is assigned.

This hardware module is not directly related to the Call Manager client application.

Call Routing Plan The Call Routing Plan is the Personal Call Handling component that contains rules that specifies a user's call handling method. The plan prioritizes a list of enabled Call Handling Rules.

Call Stack A data structure that manages an extension's call appearances. The Call Stack Size defines the maximum number of calls – including active and held calls – that an extension can handle simultaneously.

CDR *see Call Detail Record*

CDR Database A CDR database contains all CDRs generated by a ShoreTel system over a specified period of time. The CDR database is maintained on the Main server.

CHM *see Call Handling Mode*

Codec A codec is a device or program that encodes and decodes a digital data stream or signal. Codecs encode a data stream or signal for transmission, storage, or encryption and decode it for viewing or editing. Codecs are typically used in videoconferencing and streaming media applications.

Coordinate Location Based Services data point that identifies a specific location in terms of longitude, latitude, and elevation. *See Location Based Services.*

Current Call Handling Mode *see Active Call Handling Mode.*

DBImport DBImport is a ShoreTel utility that uses the contents of a CSV file to update the ShoreWare user database. DBImport.exe adds, deletes, and modifies user account records based on the CSV file contents.

Default Office Anywhere Extension The Default Office Anywhere Extension is the MCM component that can specify the Active Office Anywhere Extension when a user places a call or plays a voice message through MCM. *See Active Office Anywhere Extension and Office Anywhere Extension.*

Dial Number (DN) Dial Number – the number dialed by a user.

DID *see Direct Inward Dialing*

DID Range A DID range is a list of consecutive DID numbers assigned to a Trunk Group. Ranges assigned to a trunk group cannot overlap. A DID number can be assigned to multiple trunk groups.

Differentiated Services Differentiated Services is a computer networking architecture that specifies a method for managing network traffic and providing Quality of Service (QoS) guarantees on IP networks.

Differentiated Services can provide low-latency, guaranteed service for critical network traffic (voice or video) while providing simple best-effort traffic guarantees to less critical services (web traffic or file transfers).

Direct Inward Dialing (DID) *Direct Inward Dialing* is a feature offered by telephone companies where they allocate a range of numbers to a customer's PBX. As calls are presented to the PBX, the number that the caller dialed is also given, which the PBX uses to route the call to the correct recipient.

Distributed Routing Service (DRS) a ShoreTel system feature that increases system switch capacity by moving inter-site switching routing decisions from the individual switches to the ShoreWare servers. ShoreTel systems normally have a capacity of 60 switches – enabling DRS increases the system capacity to 500 switches.

DN *see dial number.*

DRS *See Distributed Routing Service.*

DSCP Differentiated Services Code Point is a 6-bit value, contained in the 8-bit DiffServ/ ToS field of the IP packet header, that indicates the data traffic Per-Hop Behavior (PHB).

Explicit Authentication Explicit Authentication is an LDAP process where an application prompts users for credentials when they log into a network, then verifies those credentials through a call to the LDAP server.

Failback Failback is the process of restoring a server, system, component, or network to the original, pre-failover state. *See failover.*

Failover Failover is the action of automatically transferring operations to a redundant or standby server, system, component, or network to continue normal operation after the base device fails. The failover process initiates without human intervention and typically without warning.

Find Me Find Me is a call handling feature that allows callers who are routed to a user's voice mailbox to contact the user at alternate devices by pressing "1" while listening to the voicemail greeting. See *Auto Find Me* and *Announced Find Me*.

Global Positioning System The Global Positioning System (GPS) uses a constellation of 24 and 32 satellites that transmit microwave signals to GPS receivers, which they use to determine their current location, the time, and their velocity. GPS usually requires line of sight access between the transmitter and the device.

GPS *see Global Positioning System*

IM *see Instant Messaging*

Instant Messaging (IM) Instant Messaging is the real-time transmission of text between at least two parties.

Internet Telephony Service Provider (ITSP) An *Internet Telephony Service Provider* is a vendor that offers Internet data services for making telephone calls.

IP Phone Configuration Switch In each ShoreTel installation, one switch is responsible for assigning, to each IP phone, a switch that performs call manager activities.

IP Phone Failover IP Phone Failover is a ShoreTel feature that continues a voice call after the ShorePhone loses communication with the its call manager switch.

When IP Phone Failover is implemented, ShorePhones are configured to send a signal to their ShoreGear Call Manager switch every four minutes and to expect an acknowledgment from the switch. When a phone does not receive the return signal, it connects to another switch located at the same site.

IP Phone Keep Alive A signal that voice switches send to the IP phones for which they provide Call Manager services. The system considers phones that acknowledge the signal as functioning. The signal is also referred to as a heartbeat.

ITSP *see Internet Telephony Service Provider*

LBS *see Location based service.*

LDAP *see Lightweight Directory Access Protocol.*

LDAPExport LDAPExport is a ShoreTel utility that exports AD directory information to a CSV file, whose contents can be imported to a ShoreWare user database. LDAPExport was introduced in ShoreTel to support AD Integration.

Lightweight Directory Access Protocol (LDAP) *Lightweight Directory Access Protocol* is an application protocol for querying and modifying directory services running over TCP/IP.

LLDP-MED An enhancement to the basic LLDP protocol that addresses the discovery of endpoints by networks supporting LLDP.

Location based service Location based service (LBS) is a component feature that receives data identifying the position of the device in terms of latitude, longitude, and altitude. Data reception methods include GPS access and through Mobile Cell device service transmitters.

MCM location based services does not use altitude to specify the location of the device.

Monitor Extension Extension monitoring is a ShoreTel feature that permits a user to view another user's extension status and answer inbound or held calls to that extension.

MySQL MySQL is a relational database management system that runs as a server providing multi-user access to a number of databases. MySQL is owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, which is a subsidiary of Sun Microsystems. The project's source code is available under terms of the GNU General Public License, as well as under a variety of proprietary agreements.

MySQL is officially pronounced *My S Q L*, not *My sequel*. This adheres to the official ANSI pronunciation.

OA *see Office Anywhere.*

ODBC The *Open Database Connectivity* specification provides a standard software API method for using database management systems (DBMS). The designers of ODBC aimed to make it independent of programming languages, database systems, and operating systems.

ODBC Connectors Drivers that provide connectivity to the MySQL server for client programs. There are currently five MySQL Connectors – Connector/ODBC, Connector/NET, Connector/J, Connector/MXJ, Connector/PHP.

Off System Extensions Off System Extensions are ShoreTel extensions that, when dialed, route calls from the trunk group to which they are associated. A ShoreTel system typically uses Off System Extensions to connect with a legacy PBX system.

Office Anywhere (OA) Office Anywhere is a ShoreWare user feature that forwards calls to a designated device – either a system IP phone device or a remote telephone connected to the PSTN. Office Anywhere requires administrative authorization.

Office Anywhere Extension An OA Extension is a phone number to which a user's callers can be routed when the user has enabled Office Anywhere. An OA number can be any system extension or PSTN number that is accessible from the ShoreTel system. Users can define multiple OA extensions, of which only one can be active at any time. *See Active Office Anywhere Extension and Default Office Anywhere Extension*.

Parking a Call Parking a call places a call on hold on another extension's call stack.

Per-Hop Behavior Per-Hop behaviors define packet forwarding properties associated with a class of traffic. Different PHBs may be defined to offer low-loss, low-latency forwarding properties or best-effort forwarding properties.

Personalized Call Handling Personalized Call Handling is a ShoreTel feature that defines flexible handling methods for inbound calls. Calls are filtered and managed on the basis of caller identity, time or date or receipt, end user status, and caller identity.

Presence Presence is a feature that identifies and distributes the availability of system users and other personal contacts. ShoreWare defines two types of Presence: IM presence and telephony presence.

Programmable Call Manager Toolbar Buttons Programmable Toolbar buttons is a Call Manager feature that provides access to ShoreTel call management functions. Each User Interface button is programmed by the administrator to perform a specific function when clicked and contains text that provides function status.

Programmable IP Phone Buttons Programmable IP Phone buttons is a ShorePhone feature that provides access to ShoreTel call management functions. Each button is programmed by the user or administrator to perform a specific function when pushed and contains an LED indicator that displays function status.

QoS A traffic engineering term that refers to resource reservation control by providing different priorities to different applications, users, or data flows to guarantee a performance level for a data flow.

QuickDial Field A QuickDial field is a data entry field requesting contact information for a system user, extension, or external contact. Upon the entry of alphanumeric characters, the field expands vertically to display all possible valid entries, filtered by the input. Users fill the field by selecting one of the options with the cursor.

Real-time Transport Control Protocol (RTCP) *Real-time Transport Control Protocol*, defined in RFC 3550, is a sister protocol of the Real-time Transport Protocol (RTP) that provides out-of-band control information for an RTP flow. It accompanies RTP in the delivery and packaging of multimedia data, but does not transport any data itself. It is used periodically to transmit control packets to participants in a streaming multimedia session, primarily to provide feedback on the quality of service being provided by RTP media stream.

Real-time Transport Protocol (RTP) *Real-time Transport Protocol* defines a standardized packet format for delivering audio and video over the Internet. RTP is described by IETF RFC 3550.

RTCP *see Real-time Transport Control Protocol*.

RTP *see Real-time Transport Protocol*.

SDP *see Session Description Protocol*.

Secure Real-Time Transport Protocol (SRTP) *Secure Real-Time Transport Protocol* defines a profile for providing encryption, message authentication and integrity, and replay protection to RTP data streams.

Session Description Protocol (SDP) *Session Description Protocol* is a format for describing streaming media initialization parameters. The IETF published a revised specification as an IETF Proposed Standard as RFC 4566 in July 2006. SDP is intended for describing multimedia communication sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. SDP does not provide the content of the media form itself but simply provides a negotiation between two end points to allow them to agree on a media type and format.

Session Initiated Protocol (SIP) *Session Initiation Protocol* is a signalling protocol that is typically used for setting up and tearing down multimedia communication sessions including voice and video calls. SIP also supports video conferencing, streaming multimedia distribution, instant messaging, and presence information.

Single Sign On (SSO) *Single Sign On* (SSO) is an LDAP process where applications automatically authenticate LDAP users that are logged into the network domain through their current network credentials. Such users logged into the network are not prompted to re-enter their credentials.

SIP *see Session Initiated Protocol.*

SIP Extensions SIP Extensions are ShoreTel extensions that provide calling services through SIP devices. By default, ShoreTel extensions support MGCP devices.

SIP Trunk A SIP trunk is an ITSP service that supports business VoIP sessions to endpoints outside of an enterprise network through the connection that accesses the Internet.

Site A site is a ShoreWare data structure that is identified by a geographic location and characterized by transmission capabilities, device extensions, and other parameters required by ShoreTel devices. Switches, servers, users, and other ShoreWare entities are associated with a site.

SRTP *see Secure Real-Time Transport Protocol.*

SSO *see Single Sign On.*

System Database The ShoreTel system database is the data structure that retains system operational information concerning user accounts, system architecture, switches, servers, sites, and status. Changes made through ShoreWare Director are stored in the system database.

ToS An eight-bit field in the IP Packet Header, previously referred to as Type of Service, that is used to accommodate applications that require real-time data streaming, as specified by RFC 3168. The ToS fields contains a six-bit Differentiated Services Code Point and a two-bit Explicit Congestion Notification field.

Unparking a Call Unparking a call is the retrieval of a parked call to the extension that parked the call.

Waypoint A known location specified by coordinates, associated with a coverage area (radius), and identified by a descriptive label.

Workgroup Workgroups is a ShoreWare entity that performs ACD functions for inbound calls. Calls are routed to a workgroup through an extension which, in turn, routes them to workgroup agents. Each workgroup is assigned an extension, mailbox, and other parameter settings.