

OpenScape Contact Center Enterprise V9 R1 Call Director SIP Service Installation Guide

Installation Guide

A31003-S2291-J102-01-7631

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

Copyright © Unify Software and Solutions GmbH & Co. KG 05/2017
Mies-van-der-Rohe-Str. 6, 80807 Munich/Germany

All rights reserved.

Reference No.: A31003-S2291-J102-01-7631

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products.

An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.

Availability and technical specifications are subject to change without notice.

Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG. All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.

Contents

1 About this guide	5
1.1 Who should use this guide	5
1.2 Formatting conventions	5
1.3 Documentation feedback	6
2 Installing the Call Director SIP Service software	7
2.1 System requirements for a stand-alone server machine	7
2.2 Installing the Call Director SIP Service software	7
2.3 Upgrading the Call Director SIP Service software	12
2.4 Installing a patch	12
3 Configuring the Call Director SIP Service	17
3.1 Using the Default Accounts	17
3.2 Logging on to the Call Director SIP Service server machine	18
3.3 Configuring the Call Director SIP Service	19
3.3.1 Configuring the Call Director SIP Service server machine	20
3.3.2 Configuring the network	20
3.3.3 Applying a license file	22
3.3.4 Configuring the communication platform settings	25
3.3.5 Configuring the SIP timers	28
3.3.6 Configuring the ports	29
3.3.6.1 Configuring the extensions	29
3.3.6.2 Configuring the codec settings	33
3.3.6.3 Configuring security settings	35
3.3.7 Configuring user accounts	39
3.3.8 Backing up or restoring your configuration	41
3.3.9 Configuring security credentials	42
3.4 Viewing system information	44
3.4.1 Viewing system information and statistics	44
3.4.2 Viewing the security status	46
3.4.3 Viewing the port status	47
3.4.4 Viewing the logs	49

Contents

1 About this guide

This guide describes how to install, upgrade, and configure the Call Director SIP Service software.

1.1 Who should use this guide

This guide is intended for installation technicians or anyone else in the organization who is responsible for installing and configuring the Call Director SIP Service software.

1.2 Formatting conventions

The following formatting conventions are used in this guide:

Bold

This font identifies Call Director SIP Service components, window and dialog box titles, and item names.

Italic

This font identifies references to related documentation.

`Monospace Font`

This font distinguishes text that you should type, or that the computer displays in a message.

NOTE: Notes emphasize information that is useful but not essential, such as tips or alternative methods for performing a task.

IMPORTANT: Important notes draw special attention to actions that could adversely affect the operation of the application or result in a loss of data.

1.3 Documentation feedback

To report an issue with this document, call the Customer Support Center.

When you call, be sure to include the following information. This will help identify which document you are having issues with.

- **Title:** Call Director SIP Service Installation Guide
- **Order Number:** A31003-S2291-J102-01-7631

2 Installing the Call Director SIP Service software

This chapter provides an overview of the Call Director SIP Service and includes detailed instructions on how to install the Call Director SIP Service software on a stand-alone server machine.

2.1 System requirements for a stand-alone server machine

The minimum system requirements for installing the Call Director SIP Service software on a stand-alone server machine are described in the following table.

Requirement	Description
Processor	Intel Xeon 3065
Memory	2 GB
Hard Drive	160 GB, 7200 RPM, SATA
Display settings	1024 x 768 pixels with 16-bit color
Other	100 Mbps Ethernet network interface card DVD-ROM drive

Table 1 System requirements for a stand-alone server machine

2.2 Installing the Call Director SIP Service software

This section provides detailed instructions on how to install the Call Director SIP Service on a stand-alone server machine.

If you are upgrading from an earlier version, see [Section 2.3, “Upgrading the Call Director SIP Service software”](#), on page 12.

The Call Director SIP Service installer is based on a modified version of the installer for openSUSE, which is an open-source distribution of Linux. The installer has been modified to include the Call Director SIP Service software and to configure openSUSE as securely as possible.

For more information about openSUSE, see <http://www.opensuse.org>.

IMPORTANT: To maintain security, only use the Call Director SIP Service installer. Do not use any other version of the openSUSE installer such as a version downloaded from the opensuse.org Web site.

Installing the Call Director SIP Service software

Installing the Call Director SIP Service software

Before installing the software, use the openSUSE hardware compatibility list on <https://en.opensuse.org/Hardware> to check that openSUSE 13.2 is supported on the Call Director SIP Service server machine. Also check your machine's manufacturer's Web pages for updated device drivers.

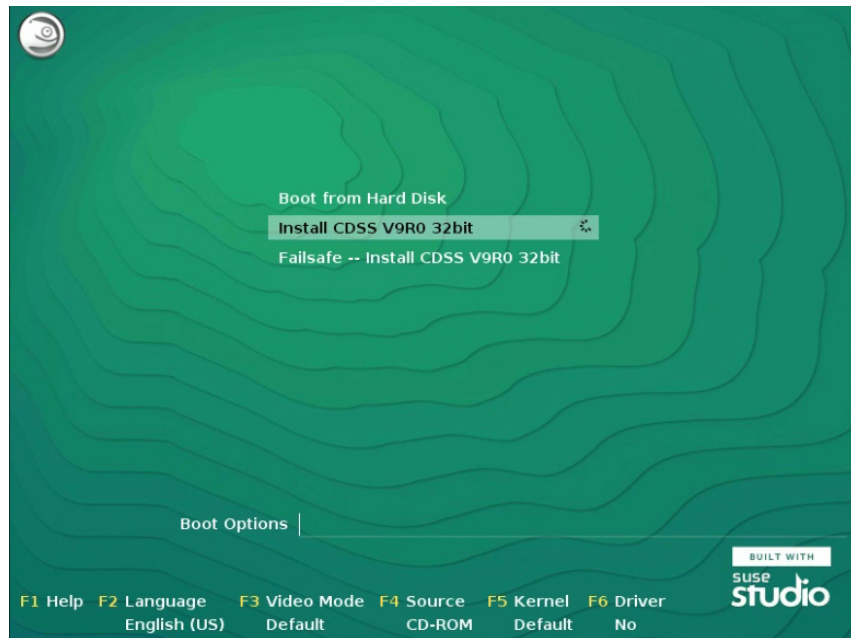
To install the Call Director SIP Service software:

1. Insert the Call Director SIP Service DVD into the DVD-ROM drive.
2. Restart the server machine and choose to boot from the DVD, not from the hard drive.

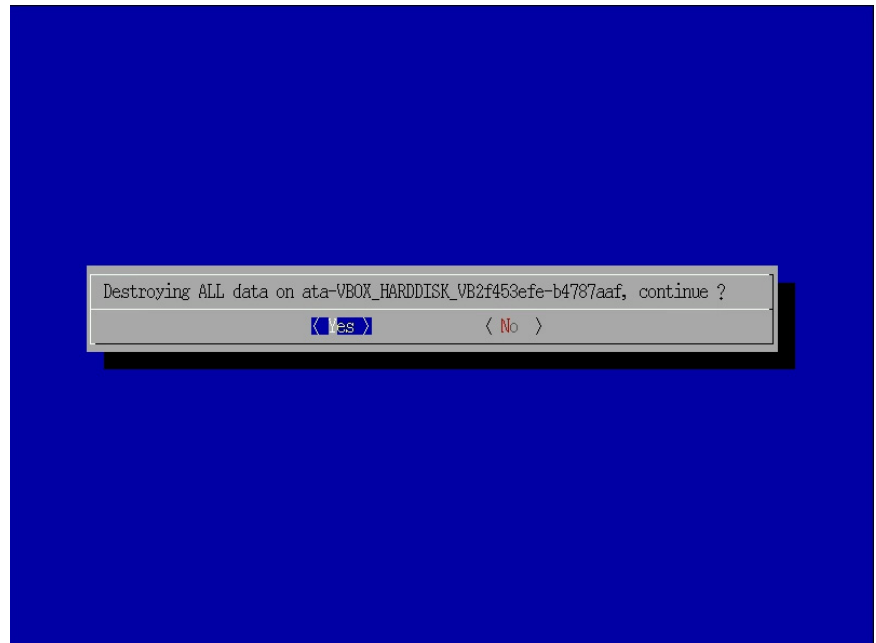
How to do this will vary slightly depending on the server machine hardware.

Normally, when you restart the server machine, it will boot from the hard drive even if a DVD is present. To make it boot from the DVD, watch the screen that first appears for a message that describes which key to press to configure the boot process. Typically, this requires pressing **F2** or the **Delete** key.

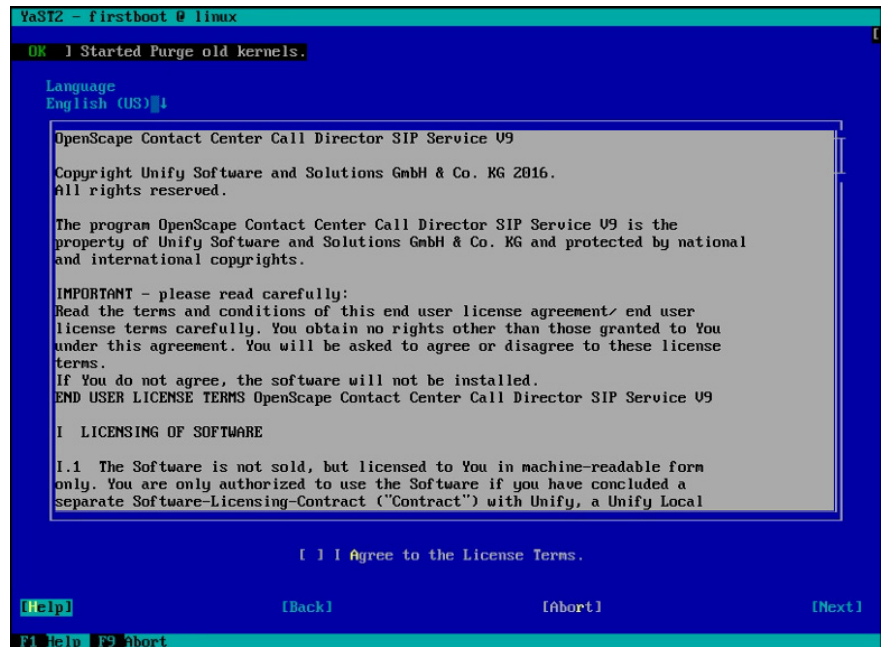
3. After you press the key, select the option to boot from the DVD-ROM drive. (The appearance of this screen will vary depending on the server machine hardware.) This launches the openSUSE installation program, which will guide you through the rest of the installation process.
4. In the installer's initial screen, use the keyboard arrow keys to select **Install CDSS V9R0 32bit**, and then press **Enter**.



5. The installation will destroy all the data on the hard disk, select **Yes** to continue.



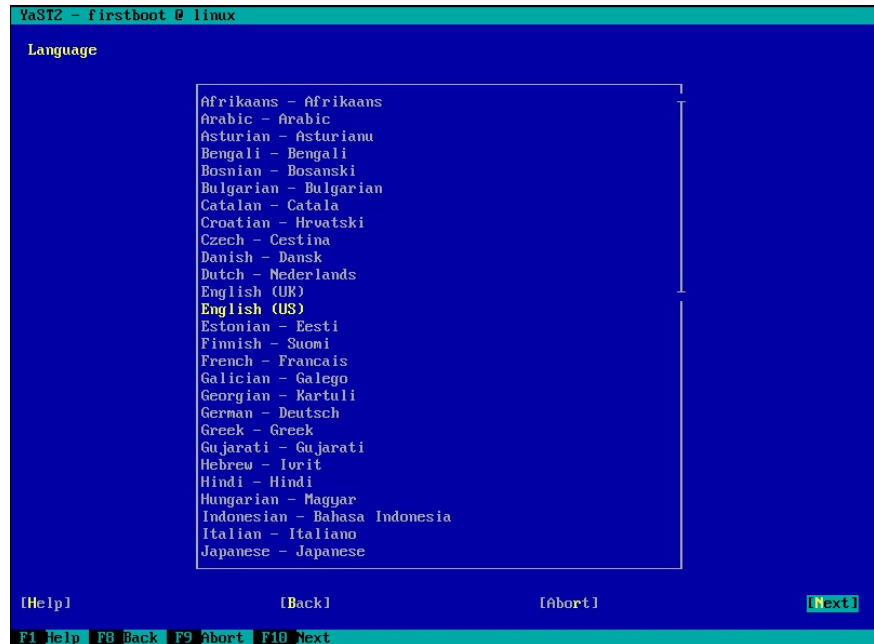
6. In the License Agreement screen, read the license agreement carefully, and then select **I Agree to the License Terms** and click **Next**.



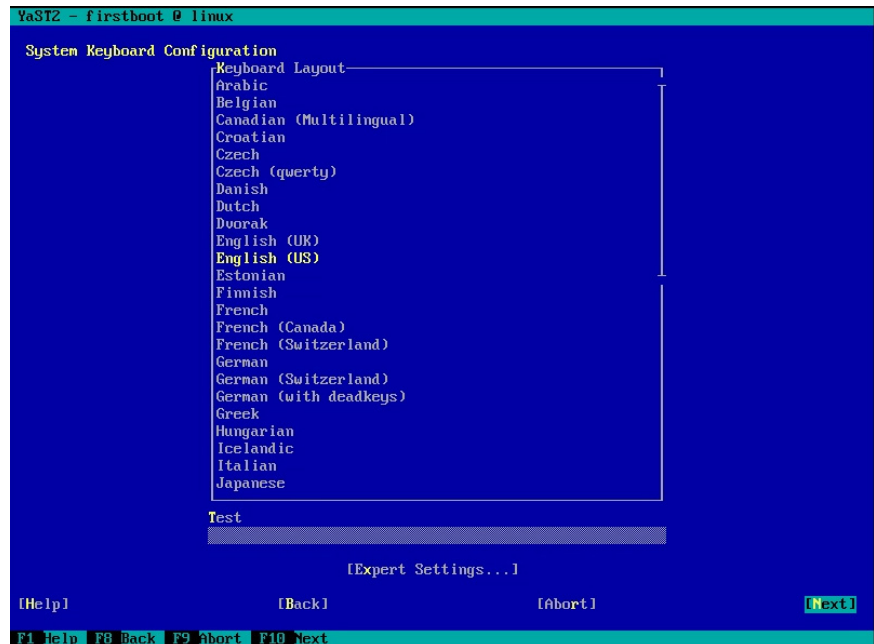
Installing the Call Director SIP Service software

Installing the Call Director SIP Service software

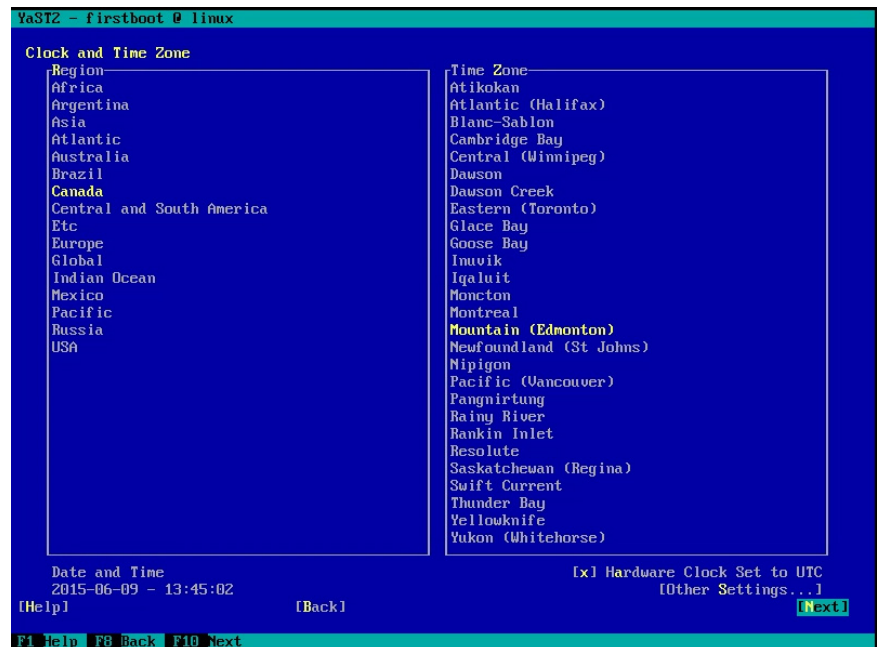
7. In the language screen, select the language you want to use and click **Next**



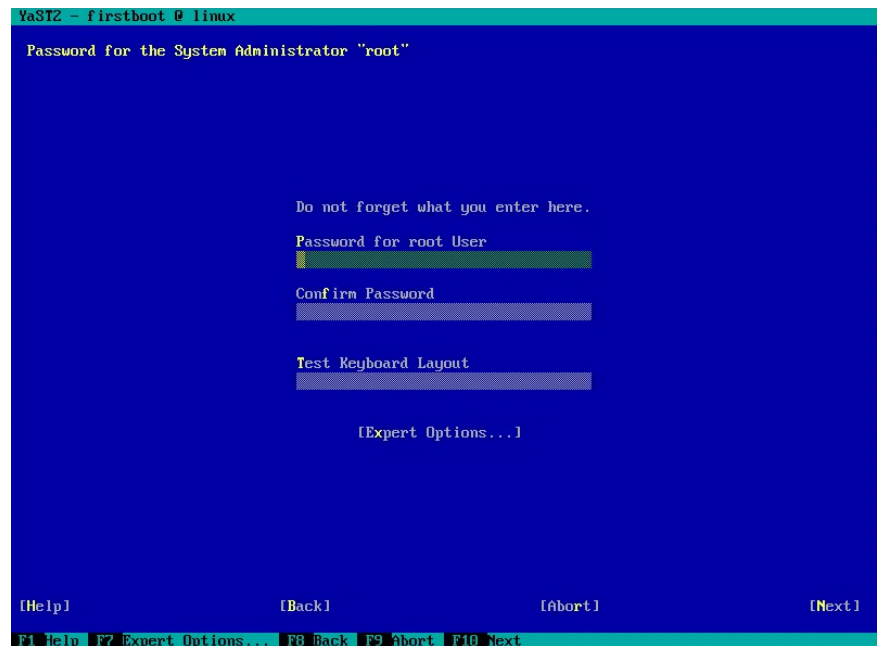
8. In the System Keyboard Configuration screen, select the keyboard settings and click **Next**.



9. In the Clock and Time Zone screen, select region and time zone and click **Next**.



10. In the Password setting screen, input the password for root and click **Next**.



IMPORTANT: We strongly recommend that you specify a password that meets the security requirements of your organization.

Installing the Call Director SIP Service software

Upgrading the Call Director SIP Service software

11. After setting the root password, the system will reboot automatically. Remove the DVD from the DVD drive and the system will boot from hard disk. The installation process is completed after the system reboot.

IMPORTANT: To maintain security, do not install any other applications on the Call Director SIP Service server machine.

2.3 Upgrading the Call Director SIP Service software

To upgrade the Call Director SIP Service software:

1. Save your configuration information, as described in [Section 3.3.8, “Backing up or restoring your configuration”](#), on page 41.
2. Boot from the installation DVD and install the new version, as described in [Section 2.2, “Installing the Call Director SIP Service software”](#), on page 7.
Be sure to choose **New Installation** on the **Installation Mode** screen.
3. Restore your configuration information, as described in [Section 3.3.8, “Backing up or restoring your configuration”](#), on page 41.
4. Re-upload the license file, as described in [Section 3.3.3, “Applying a license file”](#), on page 22.

2.4 Installing a patch

It is important to keep the Call Director SIP Service software up to date.

The Call Director SIP Service supports two kinds of software updates: *general* patches and *private* patches. General patches are released on a predetermined schedule and are designed for all customers. Private patches include ones designed for specific customers and ones for all customers if there are issues that need to be addressed between general patches. Consult the release notes to see if you need to apply any private patches.

Installing a patch

When installing a patch, consider the following:

- General patches require the presence of all previous general patches. For example, if the latest general patch is GP4, you must also upload GP1, GP2, and GP3, but only need to install GP4. The update process will warn you if it encounters problems such as not having enough disk space to complete the update.

- You can revert to an earlier patch level by selecting it and clicking **Apply Patch Level** in the Software Version section of the Call Director SIP Service Web interface. This just deactivates the old patch level. It does not delete it. You can delete a patch that is not currently installed by clicking **Delete this patch**. For example, if you have GP1 to GP3 uploaded, but are currently using GP2 or a private patch based on GP2, you can delete GP3.

Current Patch Level

- ☐ Base Install
- ☐ GP1
- ☐ GP2
- ☐ GP2_B1234
- ☒ GP2_B2345
- ☐ GP3 [Delete this patch](#)

- When you apply a general patch to version GP3 or later, you can select **Delete private patches when upgrading** to remove any private patches. If you do not remove the private patches, the patches will not be active but you can reactivate them by selecting them and clicking **Apply Patch Level**.

Current Patch Level

- ☐ Base Install
- ☐ GP1
- ☐ GP2
- ☐ GP2_B1234
- ☐ GP2_B2345
- ☒ GP3 [Delete this patch](#)

☐ Delete Private Patches when upgrading?

- For information about upgrading from one major version to another (for example, from V8 to V8 R1), see [Section 2.3, “Upgrading the Call Director SIP Service software”](#), on page 12.

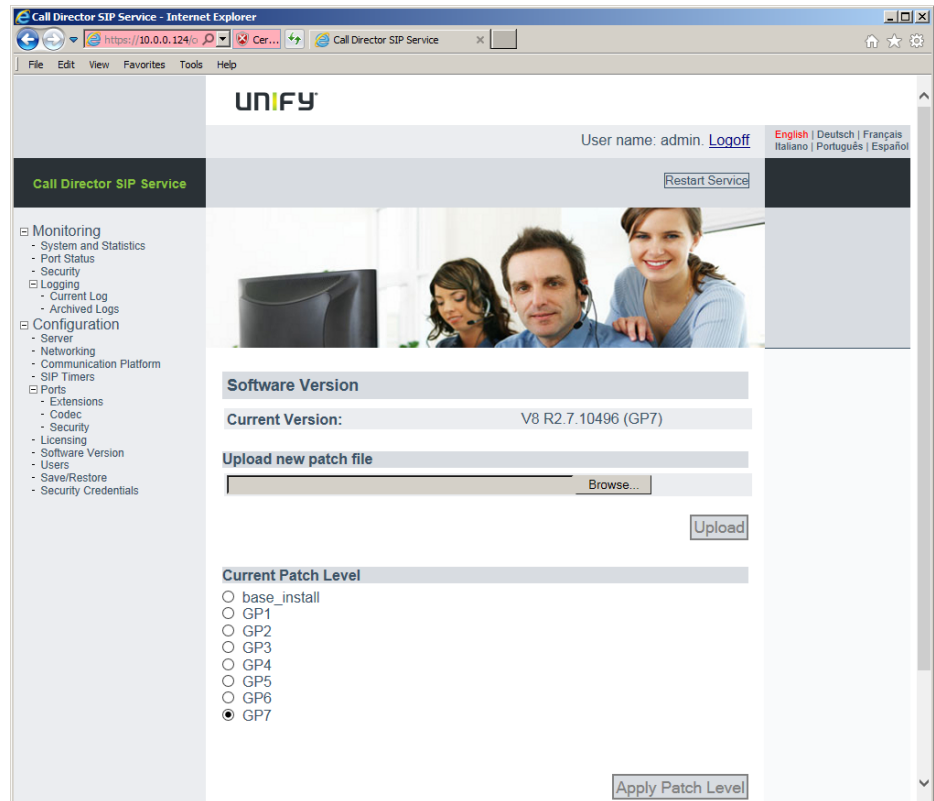
NOTE: Before installing a patch, back up the configuration. See [Section 3.3.8, “Backing up or restoring your configuration”](#), on page 41.

Installing the Call Director SIP Service software

Installing a patch

To install a patch:

1. Log on to the Call Director SIP Service Web interface. (See [Section 3.2](#), “Logging on to the Call Director SIP Service server machine”, on page 18.)
2. In the left pane, expand **Configuration**, and then click **Software Version**. The **Current Patch Level** section lists the patches that are available and indicates which patch is currently installed.



3. Click **Browse** to locate and select the patch that you want to install.

IMPORTANT: To maintain security, do not apply any operating system patches obtained from other sources, including any from the opensuse.org Web site. Since the Call Director SIP Service server machine uses a special version of openSUSE, only the Call Director SIP Service installer and updater should be used.

4. Click **Upload** to upload the patch. Press **F5** to refresh the Web page.

5. Select the patch that you uploaded, and then click **Apply Patch Level**.

NOTE: Uploading the patch does not install it. For the patch to be installed, you must click **Apply Patch Level**.

6. When the system prompts you to restart the Call Director SIP Service server machine, click **Restart Service**.

NOTE: To revert to an earlier patch level, select the patch and click **Apply Patch Level**. If you are prompted to restart the Call Director SIP Service software, click **Restart Service**. This does not delete the newer patch, it just stops installing it. If you want to install the patch at a later date, you do not have to upload it again. Simply select the patch and click **Apply Patch Level**.

Installing the Call Director SIP Service software

Installing a patch

3 Configuring the Call Director SIP Service

This chapter describes how to configure the Call Director SIP Service software.

3.1 Using the Default Accounts

By default, the Call Director SIP Service installer creates two accounts with the following settings:

User Name	Password
admin	11111111
guest	11111111

Table 1

Default user names and passwords

NOTE: To ensure system security, both the admin and guest users should change their password when they first log in.

To create more accounts, change passwords, or change account permissions, see [Section 3.3.7, “Configuring user accounts”, on page 39](#).

Configuring the Call Director SIP Service

Logging on to the Call Director SIP Service server machine

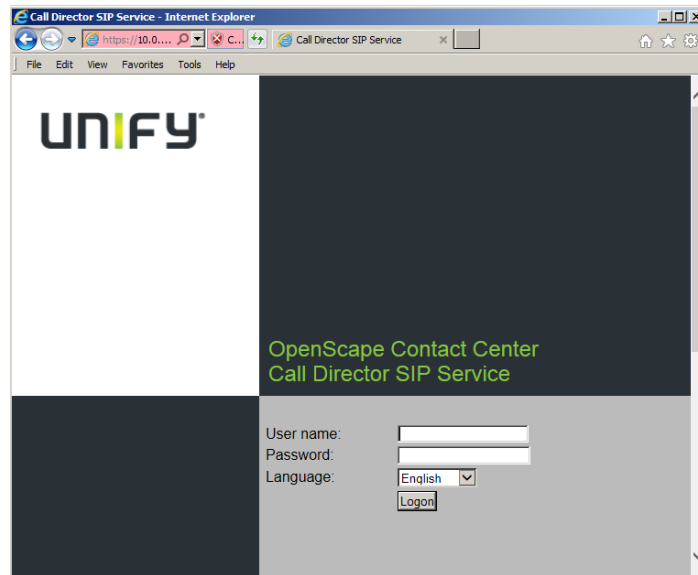
3.2 Logging on to the Call Director SIP Service server machine

To log on to the Call Director SIP Service server machine:

1. Open a Web browser and type the following URL:

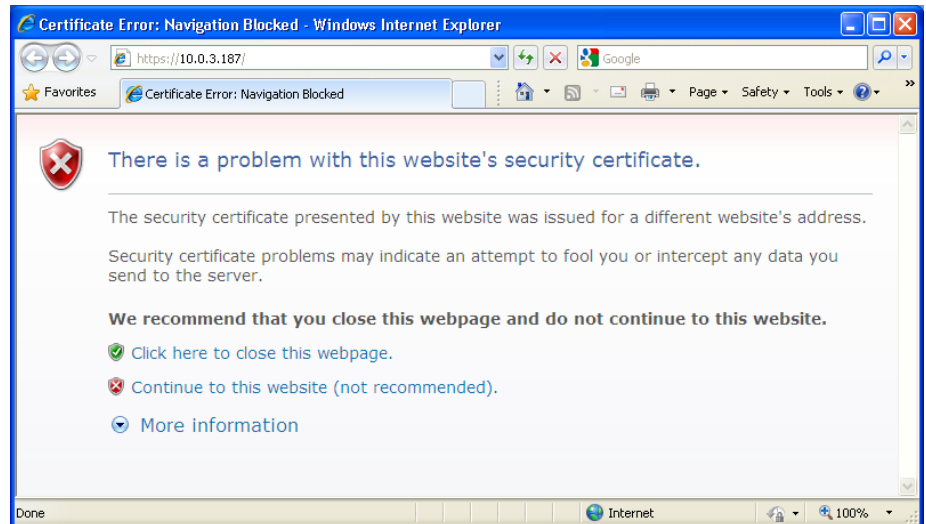
`https://servername`

where *servername* is the IP address or host name of the Call Director SIP Service server machine.



2. In the **User name** box, type your user name.
3. In the **Password** box, type your password.
4. In the **Language** box, select the language for the interface.
5. Click **Logon**.

You may see a message in the Web browser warning you that the security certificate used to establish a secure (HTTPS) connection is not known to be trustworthy. This is due to the fact that the Web browser does not know whether to automatically trust the certificate that was generated by the CDSS installer. You can ignore this warning.



To prevent this message, you can purchase and install your own HTTPS certificates which are signed by Certificate Authorities (CAs) that the Web browser knows to be trustworthy. See [Section 3.3.9, “Configuring security credentials”](#), on page 42.

3.3 Configuring the Call Director SIP Service

If any changes require restarting the Call Director SIP Service software, the Web interface will prompt you to restart it. Do so by clicking **Restart Service** in the upper right-hand corner of the screen.

3.3.1 Configuring the Call Director SIP Service server machine

To configure the Call Director SIP Service server machine:

1. In the left pane, expand **Configuration**, and then click **Server**.



2. In the **Server name** box, type the name of the Call Director SIP Service server.
3. In the **Primary time server** box, type the IP address or fully-qualified domain name of the Authoritative Time Server to which you want to connect. This ensures that the server machine receives time updates from a central location. This should be the same time server used by the OpenScape Contact Center system.
4. In the **Secondary time server** box, type the IP address or fully-qualified domain name of the time server to be used if the primary one is unavailable.
5. Click **Save**.

3.3.2 Configuring the network

You can configure the network that is used by the Call Director SIP Service.

To configure the network:

1. In the left pane, expand **Configuration**, and then click **Networking**.



2. To obtain a network address from a Dynamic Host Configuration Protocol (DHCP) server, select the **Use DHCP** check box.
3. To manually configure the network settings:
 - a) Clear the **Use DHCP** check box.
 - a) In the **IP address** box, type the IP address of the Call Director SIP Service server machine.
 - b) In the **Subnet mask** box, type the subnet used by the Call Director SIP Service server.
 - c) In the **Default gateway** box, type the gateway that connects the SIP system to the phone network.
 - d) In the **Primary DNS** box, type the IP address or fully-qualified domain name of the primary DNS (Domain Name Server).
 - e) In the **Secondary DNS** box, type the IP address or fully-qualified domain name of the secondary DNS. This DNS is used if the primary one does not respond.

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

- f) To enable two Ethernet network cards to act as one, select the **Bonded NICs** check box. Doing so increases the throughput and adds redundancy in case one card fails.

NOTE: This option is only shown if you have two Ethernet network cards enabled and configured (as eth0 and eth1). They must also be both plugged in to the network at boot time.

4. Click **Save**.

The changes made here are propagated to the openSUSE operating system automatically.

NOTE: If you change the IP address, you will need to point your Web browser to the new address to continue using the Web interface.

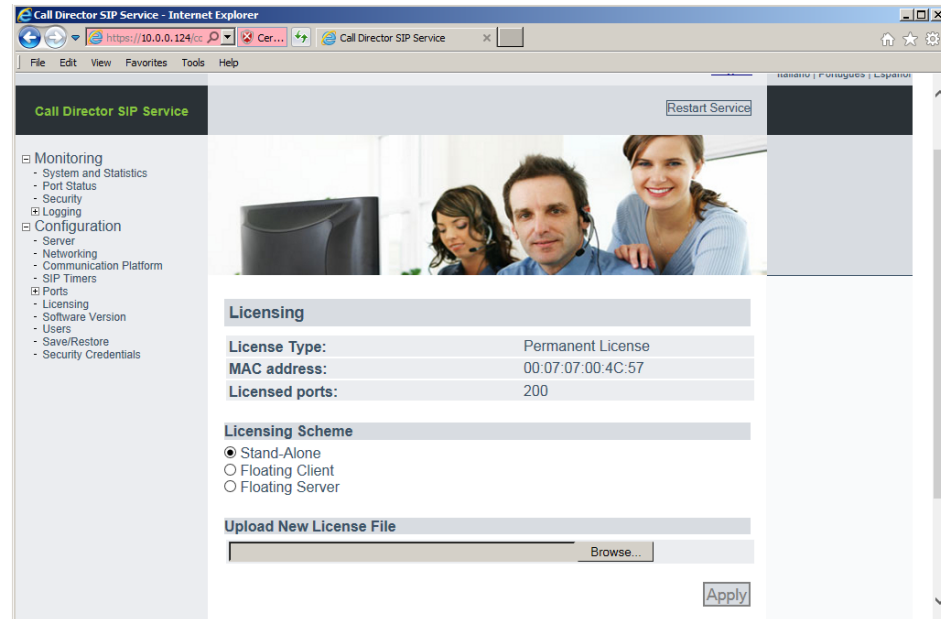
3.3.3 Applying a license file

The license controls how many ports you can use and may also specify a time limit.

When multiple Call Director SIP Service voice processors are configured in a single OpenScape Contact Center environment, a single license file is used to host the license for all the Call Director SIP Service server machines. The license file can be loaded to any server running a CLA (Client License Access) service. This includes a CLA running as part of an OpenScape Voice or HiPath 4000 environment or a CLA running on one of the Call Director SIP Service server machines. (Note that each Call Director SIP Service server machine runs the CLA service by default.)

To apply a license file:

1. In the left pane, expand **Configuration**, and then click **Licensing**.



The following information is displayed:

- **License Type** — The type of license. Regular licenses enable a fixed number of ports and have no expiry date. Grace period licenses enable one port for 30 days.
- **MAC address** — The MAC address of the machine hosting the Call Director SIP Service software.

NOTE: A license only works with one MAC address, so if you move the Call Director SIP Service software to a different machine, or change network cards on the Call Director SIP Service server machine, you will need to obtain a new license file.

- **Licensed ports** — The maximum number of ports that can be used with this license.
- **Licenses Available on Server** — The number of licenses available on the server. (This is only shown if **Licensing Scheme** is set to **Floating Client** or **Floating Server**.)
- **Days left on license** — The number of days before the license expires.

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

2. Under **Licensing Scheme**, select one of the following:
 - **Stand Alone** — Select this option when using a single Call Director SIP Service server machine. The license file will be loaded to the CLA running on this Call Director SIP Service server machine. All of the ports contained in the license file will be allocated to the server machine.
 - **Floating Client** — Select this option to connect to a CLA running on another server machine and request port licenses from the license file hosted there. Enter the IP Address/host name and port number of the machine running the CLA service you wish to connect to, along with the number of ports to request.
 - **Floating Server** — Select this option to host a floating license file on this Call Director SIP Service server machine. This allows you to allocate a portion of the port licenses from the license file to the server machine. The remainder of the port licenses can be allocated to other Call Director SIP Service server machines.
3. If you selected the **Stand Alone** licensing scheme, click **Browse** to select the license file, and then click **Upload**.
4. If you selected the **Floating Client** licensing scheme, enter the following:
 - **Server Address** — The address of the floating server.
 - **Server Port** — The port number for the floating server.
 - **Number of Licenses to Request** — The number of licenses to request from the floating server.

Licensing Scheme

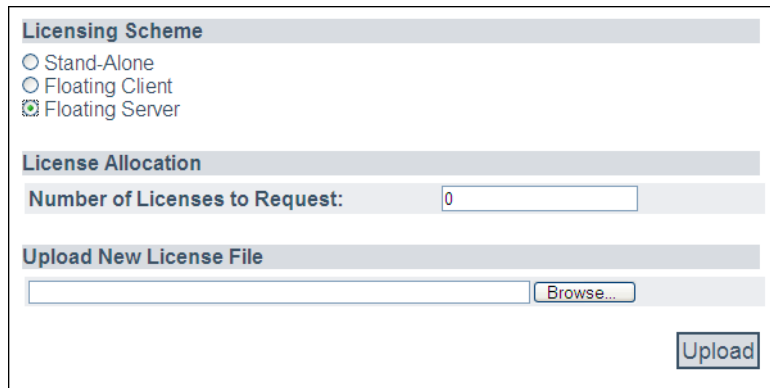
☐ Stand-Alone
☒ Floating Client
☐ Floating Server

Licensing Server Parameters

Server Address:	<input type="text" value="127.0.0.1"/>
Server Port:	<input type="text" value="61740"/>
Number of Licenses to Request:	<input type="text" value="0"/>

Click **Apply**.

5. If you selected the **Floating Server** licensing scheme, enter the number of licenses to use for *this* Call Director SIP Service machine in the **Number of Licenses to Request** box. (The remainder of the license are available for floating clients.)



The screenshot shows a configuration window with three main sections:

- Licensing Scheme:** Contains three radio buttons: ☐ Stand-Alone, ☐ Floating Client, and ☒ Floating Server.
- License Allocation:** Contains a label "Number of Licenses to Request:" followed by a text input field containing the value "0".
- Upload New License File:** Contains a text input field, a "Browse..." button, and an "Upload" button at the bottom right.

Click **Browse** to select the license file, and then click **Upload**.

3.3.4 Configuring the communication platform settings

You can configure how the Call Director SIP Service communicates with the SIP communication platform.

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

To configure the communication platform settings:

1. In the left pane, expand **Configuration**, and then click **Communication Platform**.

The screenshot shows the Unify Call Director SIP Service web interface in Internet Explorer. The browser address bar shows <https://10.0.0.124/>. The page title is "Call Director SIP Service - Internet Explorer". The Unify logo is at the top. The user is logged in as "admin" with a "Logoff" link. Language options are available: English, Deutsch, Français, Italiano, Português, Español. The left navigation pane shows "Monitoring" and "Configuration" expanded, with "Communication Platform" selected. The main content area is titled "Communication Platform" and contains the following fields:

SIP server:	<input type="text"/>
SIP port:	<input type="text" value="5060"/>
SIP domain:	<input type="text"/>
Registrar host:	<input type="text"/>
Registrar port:	<input type="text" value="5060"/>
Registration time to live:	<input type="text" value="3600"/> seconds
Outbound proxy host:	<input type="text"/>
Outbound proxy port:	<input type="text" value="5060"/>
RTP Start Port:	<input type="text" value="9000"/>

Below the fields is the "Transport Type" section with three radio buttons:

- ☒ UDP
- ☐ TCP
- ☐ TLS

A "Save" button is located at the bottom right of the form.

2. In the **SIP server** box, type the IP address or host name of the SIP communication platform. If connecting to a geo-separated OpenScope Voice system, enter the host name of the DNS SRV record.
3. In the **SIP port** box, type the TCP/IP port number used by the Call Director SIP Service to contact the SIP Server. The default is 5060. (If you are using TLS and wish to use the typical port for TLS traffic, 5061, you will need to set this manually.)
4. In the **SIP domain** box, type the IP address or fully-qualified domain name of the SIP Server.
5. In the **Registrar host** box, type the IP address or fully-qualified domain name of the SIP Registrar server. The registrar handles location registration messages.
6. In the **Registrar port** box, type the port number used by the SIP Registrar server. The SIP registrar listens for SIP REGISTER messages on this port so that it can associate an endpoint DN (the phone number) with its IP address.

7. In the **Registration time to live** box, type the expiry time for registrations as requested by the SIP Registrar. (The actual expiry times may not be what the SIP Registrar requests.)

The default is 3,600 seconds (1 hour).

8. In the **Outbound proxy host** box, type the IP address or fully-qualified domain name of the SIP proxy for outbound messages.

This can be left empty if there is no outbound proxy.

9. In the **Outbound proxy port** box, type the TCP/IP port number used by the Outbound Proxy.

This can be left empty if there is no outbound proxy.

10. Set the **RTP Start Port** to the port number that will be used as the starting point for RTP traffic. This number must be even and must be greater than 1024.

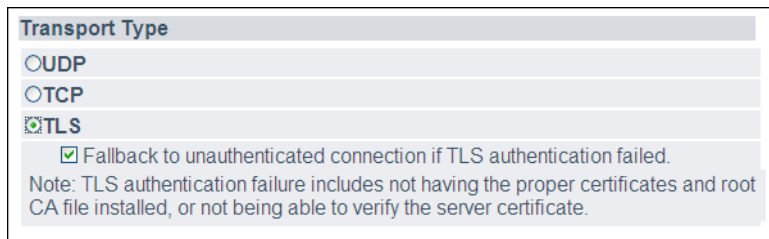
By default, the starting port is 9000. Each call uses a pair of ports (for example, 9000 and 9001) so the upper limit of the ports used depends on the traffic. As calls end, ports will be reused. This port reuse does not happen immediately, so during periods of heavy load the Call Director SIP Service may use up to 3,000 ports (For example, from 9000 to 12000.)

Make sure your firewall will not block these ports.

11. Under **Transport Type**, specify whether the signaling portion of the phone call will be transmitted by UDP, TCP, or TLS protocol.

NOTE: This setting must match that configured in the SIP settings for the subscriber in the communication platform.

If you choose TLS, a check box appears which determine whether the Call Director SIP Service should fallback to an unauthenticated connection if anything prevents TLS security from being established. (If this check box is not selected and TLS security cannot be established, the Call Director SIP Service will halt operations.)



Transport Type

☐ UDP

☐ TCP

☒ TLS

☒ Fallback to unauthenticated connection if TLS authentication failed.

Note: TLS authentication failure includes not having the proper certificates and root CA file installed, or not being able to verify the server certificate.

If TLS security is not established, you can use the Monitoring section to get useful diagnostic information. See [Section 3.4.2, “Viewing the security status”](#), on page 46.

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

12. Click **Save**.

3.3.5 Configuring the SIP timers

You can configure how frequently SIP messages will be repeated if a response is not received.

To configure the SIP timers:

1. In the left pane, expand **Configuration**, and then click **SIP Timers**.



2. In the **T1** box, type the estimated round trip time (RTT) that it normally takes for a SIP client to get a response back to a SIP request.

This timer affects many other internal timers that control how often SIP messages are retransmitted.

The default is 500 milliseconds. You can use a lower value within closed, private networks that do not permit general Internet connection, although this is not recommended.

It is recommended that you use a larger value for networks where the latency is known to be large.

3. In the **T2** box, type the maximum time to wait before retransmitting a non-INVITE request (all requests except INVITE or ACK) or a response to an INVITE request.

The default is 4,000 milliseconds (4 seconds).

4. In the **T4** box, type the time the network will take to clear messages between client and server transactions.

The default value is 5,000 milliseconds (5 seconds).

5. Click **Save**.

For more information about these timers, see Section 17 in RFC 3261 “SIP: Session Initiation Protocol”, available from <http://www.ietf.org/rfc/rfc3261.txt>.

3.3.6 Configuring the ports

This section describes how to configure the ports.

NOTE: You must configure the communication platform settings before configuring the port settings. For more information, see [Section 3.3.4, “Configuring the communication platform settings”, on page 25](#). The Call Director SIP Service also needs a valid license before the ports can be configured. See [Section 3.3.3, “Applying a license file”, on page 22](#).

To view the ports’ status, see [Section 3.4.3, “Viewing the port status”, on page 47](#).

3.3.6.1 Configuring the extensions

You can configure the extensions associated with each Call Director SIP Service port.

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

To configure the extensions:

1. In the left pane, expand **Configuration**, then **Ports**, and then click **Extensions**.

The screenshot shows the 'Call Director SIP Service' web interface in Internet Explorer. The left navigation pane is expanded to 'Configuration' > 'Ports' > 'Extensions'. The main content area displays a table for configuring extensions. The table has three columns: 'Port', 'Extension', and 'Name'. The first five rows are pre-filled with extension numbers 4311 through 4315. The 'Name' column for the first five rows contains the same numbers. The 'Port' column is empty for all rows. The 'Extension' column for the first five rows contains the numbers 14035554311 through 14035554315. The 'Name' column for the first five rows contains the numbers 4311 through 4315. The 'Port' column is empty for all rows. The 'Extension' column for the first five rows contains the numbers 14035554311 through 14035554315. The 'Name' column for the first five rows contains the numbers 4311 through 4315. The 'Port' column is empty for all rows. The 'Extension' column for the first five rows contains the numbers 14035554311 through 14035554315. The 'Name' column for the first five rows contains the numbers 4311 through 4315.

Port	Extension	Name
1	14035554311	4311
2	14035554312	4312
3	14035554313	4313
4	14035554314	4314
5	14035554315	4315
6		
7		
8		
9		

2. For each port type the following:
 - **Extension** — Enter the full phone number.
 - **Name** — Optionally, enter a descriptive name for this port. Typically this is part of the phone number. For example, “4200” or “ext01”.
3. Click **Save**.

Using the configuration wizard to configure ports

The configuration wizard provides a quick way to populate the fields for the extensions and/or the names.

To use the configuration wizard:

1. If the configuration wizard is not visible, click **Show/Hide Config Wizard**.

The screenshot shows a configuration wizard with three main sections:

- Port Range:** Contains two input fields labeled "Start:" and "End:".
- Extension Pattern:** Contains a "Pattern to apply:" dropdown menu set to "Increment". Below it are "Incrementing Parameters" with "Increment from:" and "Increment steps:" input fields, and a "Populate" button.
- Name Pattern:** Contains a "Pattern to apply:" dropdown menu set to "Increment". Below it are "Incrementing Parameters" with "Increment from:" and "Increment steps:" input fields, and a "Populate" button.

2. In the **Port Range** boxes, type the numbers of the first and last port to change. (These are the port numbers, between 1 and 200, not the phone numbers.)
3. In **Extension Pattern**, use the **Pattern to apply** drop-down menu to choose how to automatically generate extension names. For examples, see [Table 2 on page 32](#).
 - **Increment** — Enter the starting number in the **Increment from** box and the change in each extension in the **Increment steps** box.

This screenshot is a close-up of the **Extension Pattern** section of the configuration wizard. It shows the "Pattern to apply:" dropdown menu set to "Increment", the "Incrementing Parameters" section with "Increment from:" and "Increment steps:" input fields, and the "Populate" button.

- **Prepend Extension** — Enter the common suffix for the names in the **Prepend string** box. The wizard will create user names by concatenating the extension list number with the string.

Extension Pattern

Pattern to apply:

Prepend Extension

Prepending Parameters

Prepend string:

Populate

- **Append Extension** — Enter the common prefix for the names in the **Append string** box. The wizard will create user names by concatenating the string with the extension list number.

Extension Pattern

Pattern to apply:

Append Extension

Appending Parameters

Append string:

Populate

- **Constant String** — Enter the user name in the **Use constant string** box. The wizard will fill the user names with that string.

Extension Pattern

Pattern to apply:

Constant String

Constant String Parameters

Use constant string:

Populate

Table 2 on page 32 shows examples of how the **Pattern to apply** setting populates the fields.

Pattern and Parameters	Resulting Fields (for Start Extension = 1 and End Extension = 3)
Pattern to apply = Increment Increment from = 10 Increment steps = 1	10, 11, 12
Pattern to apply = Prepend Extension Prepend string = "user"	1user, 2user, 3user
Pattern to apply = Append Extension Append string = "user"	user1, user2, user3
Pattern to apply = Constant String Use constant string = "user"	user, user, user

Table 2 Comparison of "pattern to apply" choices for the configuration wizard

4. Click **Populate**.

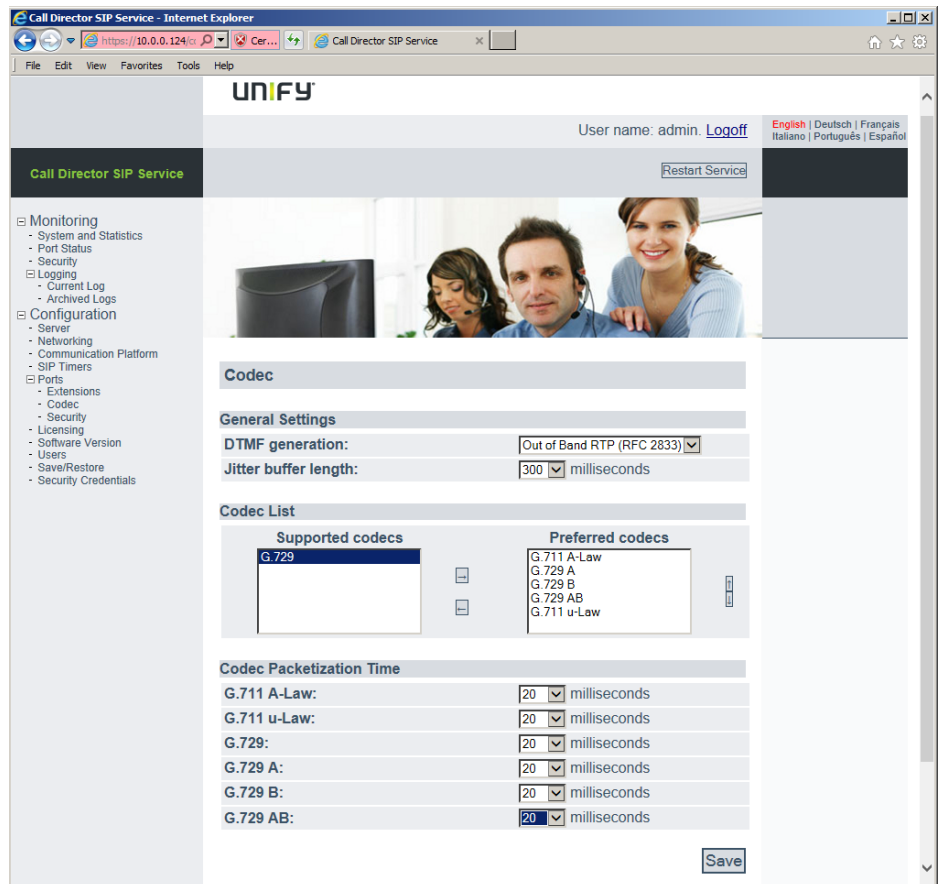
- Similarly, in **Name Pattern**, use the **Pattern to apply** drop-down menu to choose how to automatically generate the friendly names, and then click **Populate**.

3.3.6.2 Configuring the codec settings

You can configure how the audio portions of calls are transmitted.

To configure the codec settings:

- In the left pane, expand **Configuration**, then **Ports**, and then click **Codec**.



- In the **DTMF generation** list, select how DTMF (dual-tone multi-frequency) tones are transmitted.

DTMF tones are generated when users press touch-tone keys on their phone's keypad after a call has been established, for example to enter an extension number or PIN number. The codecs used to compress voices can

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

distort these tones and prevent the user agent at the other end from recognizing them, so special measures must be taken to transmit these tones.

Two choices are available:

- **Out of Band RTP (RFC 2833)** — The DTMF tones are encoded and transmitted as part of the RTP audio stream of the call.
- **SIP Info Messages** — The DTMF tones are sent via separate SIP messages.

For more information, see:

- RFC 2833 “RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals”, available from <http://www.ietf.org/rfc/rfc2833.txt>.
 - RFC 2976 “The SIP INFO Method”, available from <http://www.ietf.org/rfc/rfc2976.txt>.
3. Packets transmitted over TCP/IP may arrive out of order, a phenomenon known as “jitter”. Set **Jitter buffer length** to the length of time the Call Director SIP Service should wait for packets to arrive.

Increase this value if there are many noticeable dropouts in calls and reduce it if not.

NOTE: Higher values may increase the voice delay.

4. Add the codecs you would like to use to the **Preferred Codecs** list by selecting them in the **Supported codecs** list and clicking the right arrow.

To remove a codec from the **Preferred codecs** list, select it in the list and click the left arrow.

To change the order of priority of a codec, selected it in the **Preferred codecs** list and click the up arrow or down arrow.

The actual codec that gets used will depend on the capabilities of the user agent at the other end.

- For a comparison of the G.711 and G.729 codecs, see [Table 3 on page 35](#).
 - For a comparison of the variations of the G.711 codec, see [Table 4 on page 35](#).
 - For a comparison of the variations of the G.729 codec, see [Table 5 on page 35](#).
5. For each codec, set the **Codec Packetization Time** to the length of the voice packet in each RTP message.

Using a smaller packet length reduces the latency but increases the CPU processing requirements and the bandwidth.

6. Click **Save**.

Codec	Uses Compression?	Advantages	Disadvantages
G.711 μ -law G.711 A-law	No	<ul style="list-style-type: none"> Higher voice quality. Lower CPU processing requirements. 	<ul style="list-style-type: none"> Uses more bandwidth
G.729 G.729.A G.729.B G.729.AB	Yes	<ul style="list-style-type: none"> Uses less bandwidth. 	<ul style="list-style-type: none"> Lower voice quality. Higher CPU processing requirements.

Table 3 Comparison of G.711 and G.729 codecs

Codec	Notes
G.711 μ -law	Used in North America.
G.711 A-law	Used in Europe.

Table 4 Comparison of variations of the G.711 codec

Codec	Advantages	Disadvantages
G.729	<ul style="list-style-type: none"> Best voice quality. 	<ul style="list-style-type: none"> Highest CPU requirements.
G.729.A	<ul style="list-style-type: none"> Lower CPU requirements than G.729. 	<ul style="list-style-type: none"> Slightly lower voice quality than G.729.
G.729.B	<ul style="list-style-type: none"> Uses silence-detection to reduce bandwidth compared to G.729. 	
G.729.AB	<ul style="list-style-type: none"> Lower CPU requirements than G.729. Lower bandwidth requirements than G.729. 	<ul style="list-style-type: none"> Slightly lower voice quality than G.729.

Table 5 Comparison of variations of the G.729 codec

3.3.6.3 Configuring security settings

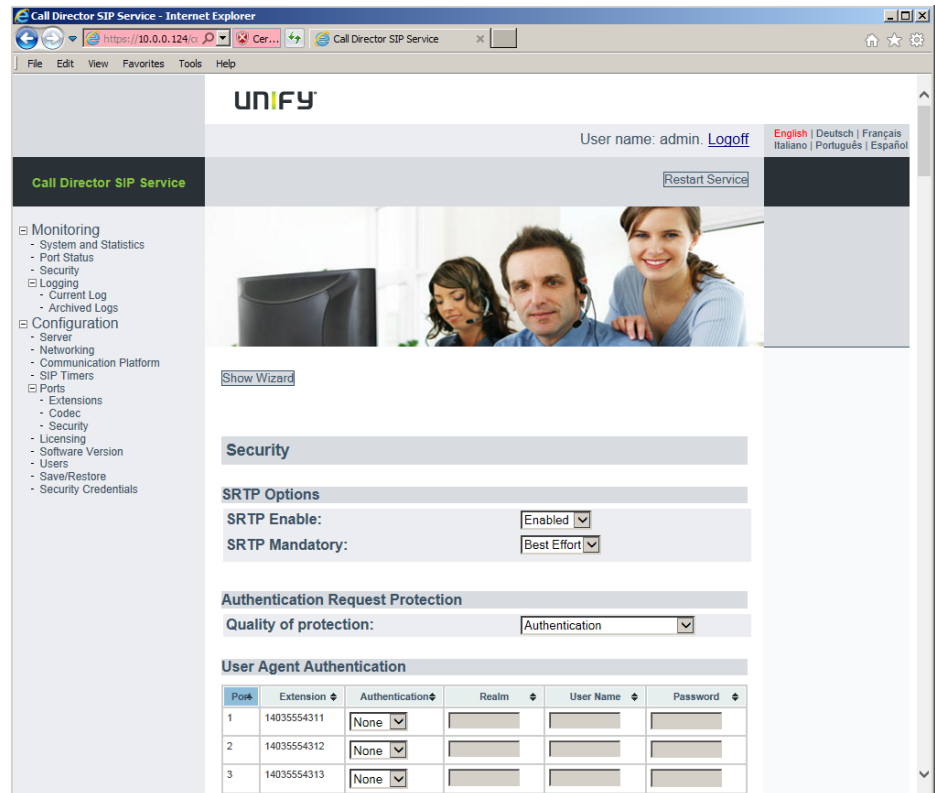
You can configure the security settings that are used when the Call Director SIP Service communicates with the communication platform.

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

To configure security settings:

1. In the left pane, expand **Configuration**, then **Ports**, and then click **Security**.



2. In the **SRTP Options** section, select either **Enabled** or **Disabled**.
 - **Enabled** — Uses SRTP (Secure Real Time Protocol) to encrypt the audio of the phone calls.
For more information on SRTP, see RFC 3711, "The Secure Real-time Transport Protocol (SRTP)", available from <http://www.ietf.org/rfc/rfc3711.txt>
 - **Disabled** — Does not use SRTP.If you choose **Enabled**, the **SRTP Mandatory** choice appears.
 - **Always** — The call will not proceed if SRTP cannot be established.

- **Best Effort** — SRTP will be used if possible, but the call will still proceed if it cannot be established.

NOTE: SRTP is not enabled unless a TLS connection can be established, and this requires a root CA certificate. See [Section 3.3.9, “Configuring security credentials”](#), on page 42.

3. In the **Quality of protection** list, select the level of security.

- **Authentication** — Provides compatibility with older implementations.
- **Authentication Plus Integrity** — Uses a more recent specification with higher security.

NOTE: This setting must match the client quality of protection set for this port in the communication platform.

4. For each port, do the following:

- a) In the **Authentication** list, select the type of security for the communication between the Call Director SIP Service and the communication platform. (As required by RFC 3261, digest authentication is always used for the signaling portion of the phone call.)

The choices are:

- **None** — uses no authentication. User names and passwords are not used.
- **Basic** — uses HTTP basic authentication. User names and passwords are sent in cleartext. This can be acceptable if the communication channel between the Call Director SIP Service and the communication platform is secure.
- **Digest** — uses HTTP digest authentication. User names and passwords are encrypted for security.

NOTE: The **Authentication** setting must match the corresponding setting in the communication platform.

- b) In the **Realm** box, type the name of the security domain.
- c) In the **User Name** box, type the user name for this port. This must be 6 to 64 characters long (inclusive).

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

- d) In the **Password** box, type the password for this port. This must be 6 to 20 characters long (inclusive).

NOTE: The **Realm**, **User Name**, and **Password** settings must match the settings for this port in the communication platform.

5. Click **Save**.

Using the configuration wizard to configure security settings

The configuration wizard provides a quick way to populate the fields for the realms, user names, and/or passwords. It works similarly to the configuration wizard for ports, described in [Section 3.3.6.1, “Using the configuration wizard to configure ports”](#), on page 31.

To use the configuration wizard:

1. If the configuration wizard is not visible, click **Show/Hide Config Wizard**.

The screenshot shows a 'Configuration Wizard' window with several sections for configuring security settings. Each section has a 'Pattern to apply' dropdown and an 'Incrementing Parameters' section with 'Increment from' and 'Increment steps' text boxes, followed by a 'Populate' button.

- Port Range:** Includes 'Start' and 'End' text boxes.
- Authentication Pattern:** 'Authentication to apply' dropdown is set to 'None'. A 'Populate' button is to the right.
- Realm Pattern:** 'Pattern to apply' dropdown is set to 'Increment'. An 'Incrementing Parameters' section follows with 'Increment from' and 'Increment steps' text boxes, and a 'Populate' button.
- User Name Pattern:** 'Pattern to apply' dropdown is set to 'Increment'. An 'Incrementing Parameters' section follows with 'Increment from' and 'Increment steps' text boxes, and a 'Populate' button.
- Password Pattern:** 'Pattern to apply' dropdown is set to 'Increment'. An 'Incrementing Parameters' section follows with 'Increment from' and 'Increment steps' text boxes, and a 'Populate' button.

2. Set the range of channels to configure via the **Start** and **End** boxes. (These are the channel numbers, from 1 to 200, not the phone numbers.)

3. Set the wanted authentication in the **Authentication to apply** drop-down menu and click **Populate**.
4. For each remaining section that you want to auto-fill (realms, user names, or passwords), use the **Pattern to apply** drop-down menu to choose how to automatically generate names, and enter the parameters for that choice. For examples, see [Table 2 on page 32](#). Then click **Populate**.

3.3.7 Configuring user accounts

You can create, modify, and delete user accounts.

NOTE: The default user names and passwords are listed in [Section 3.1, “Using the Default Accounts”](#), on page 17.

To configure user accounts:

1. In the left pane, expand **Configuration**, and then click **Users**.

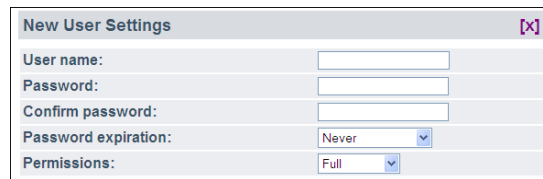


2. Click **Create a New User** to create a new account, **Edit** to alter an existing account, or **Delete** to delete an account.

Configuring the Call Director SIP Service

Configuring the Call Director SIP Service

3. If you chose **Create a New User** or **Edit**, the account settings are shown.

A screenshot of a 'New User Settings' dialog box. It has a title bar with the text 'New User Settings' and a close button (X). The dialog contains five rows of input fields: 'User name:' with a text box, 'Password:' with a text box, 'Confirm password:' with a text box, 'Password expiration:' with a dropdown menu showing 'Never', and 'Permissions:' with a dropdown menu showing 'Full'.

Enter the following information:

- **User name** — Enter the user name for the account you want to create or modify.
- **Password** — Enter the new password.

The Call Director SIP Service Interface checks that the new password meets some basic security criteria:

- It must be at least 8 characters long.
- It cannot reuse an old password.
- It cannot use easily guessed passwords (such as the account name or "abcdef").

NOTE: This password is unrelated to the password for the openSUSE administrator which is set when installing openSUSE. (See [Section 2.2, "Installing the Call Director SIP Service software"](#), on page 7.)

- **Confirm password** — Confirm the password.
- **Password expiration** — Specify whether the password should expire, and if so, when it should do so.
- **Permissions** — Select the permission level for this account. A user with **Full** permission can change Call Director SIP Service configuration settings. A user with **Read-only** permission can view information but cannot change settings.

4. Click **Save**.

3.3.8 Backing up or restoring your configuration

We strongly recommend that you periodically back up your configuration.

NOTE: You should always back up your configuration before migrating to a new major version (for example, from V8 R1 to V8 R2) as otherwise you will have to re-enter all your configuration settings.

To back up or restore your configuration:

1. In the left pane, expand **Configuration**, and then click **Save/Restore**.



2. To save the configuration, click **Download**.
The file `cdss_configuration.tar` is downloaded.
3. To restore your configuration, select the saved configuration file and click **Upload**.
4. You will be prompted to restart the Call Director SIP Service.

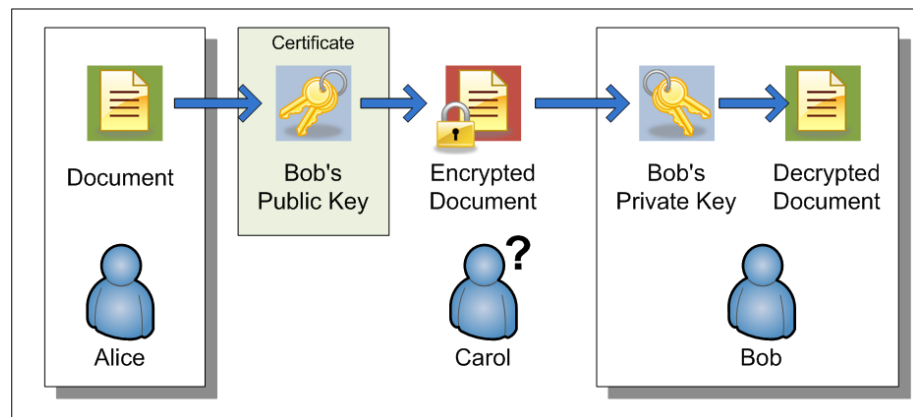
3.3.9 Configuring security credentials

The Call Director SIP Service supports the following security features:

- Communication between machines is encrypted using secure FTP (SFTP) and SSH tunnelling.
- The Web browser administration interface is authenticated using a secure HTTPS connection.
- SIP signalling connections can optionally be encrypted using TLS (Transport Layer Security). See [Section 3.3.4, “Configuring the communication platform settings”](#), on page 25.
- The audio portion of calls can optionally be encrypted using SRTP (Secure Real Time Protocol). See [Section 3.3.6.3, “Configuring security settings”](#), on page 35.

To accomplish the encryption, the Call Director SIP Service uses industry-standard *public key encryption*. This uses *public keys* and *private keys*.

Suppose, for example, that Alice wants to send a private message to Bob. She can use Bob's *public key* to encrypt the message. Bob can then use his corresponding *private key* to decrypt the message. Carol, an eavesdropper, cannot read the encrypted message even if she knows Bob's public key.



Certificates are used to establish that a public key actually belongs to the person it purports to belong to. For example, Bob's public key can use a certificate that establishes it really does belong to Bob. This prevents Carol from pretending that her public key is Bob's, thereby being able to read messages intended for Bob.

When you install the Call Director SIP Service, the installer automatically generates a public certificate and a private key. You can continue to use these, or you can use your own.

You can generate your own public certificate and private keys by using the OpenSSL package tools on Linux. Or you can purchase keys and certificates from third-party commercial companies (Certificate Authorities). In order to have the best security, it is recommended to acquire a certificate from a well known Certificate Authority (for example, Verisign).

IMPORTANT: it is strongly recommended that customers procure a third-party certificate instead of using the default system generated one (which is not secure).

To configure security credentials:

1. In the left pane, expand **Configuration**, and then click **Security Credentials**.



2. Click **Replace** beside the item you want to change.

- **HTTPS Credentials**

- **Public Certificate** — the public certificate for HTTPS encryption.
- **Private Key** — the private key for HTTPS encryption.

- **TLS Credentials**

- **Public Certificate** — the public certificate for TLS encryption.
- **Private Key** — the private key for TLS encryption.

Configuring the Call Director SIP Service

Viewing system information

- **Root Certificate Authority** — the root CA certificate that is used to validate the server certificate when establishing a TLS connection with a SIP communication platform.

IMPORTANT: A root CA certificate must be installed to successfully establish a TLS connection with a SIP communication platform. You must obtain the root CA certificate from the service technician of the SIP communication platform.

NOTE: Certificates and keys must be in PEM (Privacy Enhanced Mail) format.

3. Click **Save**.

You can use the same public certificates and private keys for both HTTP and TLS, or use different ones.

3.4 Viewing system information

This section describes how to view information about the Call Director SIP Service hardware and software.

3.4.1 Viewing system information and statistics

You can view system information and statistics related to your Call Director SIP Service configuration.

To view system information and statistics:

- In the left pane, expand **Monitoring**, and then click **System and Statistics**.



This screen shows:

- **IP address** — The IP address of the Call Director SIP Service server machine.

NOTE: The IP address must match the one configured in the voice processor settings in the Manager application.

- **Software version** — The version number of the Call Director SIP Service software.
- **CPU information** — Information about the processor in the Call Director SIP Service server machine.
- **Memory information** — Information about the RAM in the Call Director SIP Service server machine.
- **Disk Information** — Information about the disk storage in the Call Director SIP Service server machine.
- **Active since** — How long the Call Director SIP Service server machine has been running.

Configuring the Call Director SIP Service

Viewing system information

- **Calls processed** — The number of telephone calls served by the Call Director SIP Service (since the last restart of the Call Director SIP Service server machine).

3.4.2 Viewing the security status

You can view a summary of the key security-related information.

To view the security status:

- In the left pane, expand **Monitoring**, and then click **Security**.



This screen shows:

- **Selected SIP Transport Type** — the protocol chosen for SIP messages (UDP, TCP, or TLS). See [Section 3.3.4, “Configuring the communication platform settings”](#), on page 25
- **Public Certificate Installed** — Whether a public certificate has been installed for TLS security. See [Section 3.3.9, “Configuring security credentials”](#), on page 42/
- **Private Key Installed** — Whether a private key has been installed for TLS security. See [Section 3.3.9, “Configuring security credentials”](#), on page 42
- **Root CA Certificate Installed** — Whether a certificate has been installed to verify keys from the OpenScape Voice server. See [Section 3.3.9, “Configuring security credentials”](#), on page 42.

- **TLS Connection Status** — Whether a TLS connection has been established and the server has been verified.

A padlock icon will be visible if TLS (Transport Layer Security) is enabled. (See Section 3.3.4, “Configuring the communication platform settings”, on page 25.)



- If the padlock is closed, this means that TLS security is fully operational.
- If the padlock is open, as show above, this means that something is preventing TLS security from being established.

Clicking the padlock shows the security monitoring page where you can see more details of the security status.

3.4.3 Viewing the port status

You can view the status of the various ports. A port corresponds to an extension in the communication platform and an extension configured in OpenScape Contact Center Call Director

Configuring the Call Director SIP Service

Viewing system information

To view the port status:

- In the left pane, expand **Monitoring**, and then click **Port Status**.



This screen shows:

- **Port** — The port number.
- **Status** — The current status of the port. This may be:
 - **uninitialized** — The default startup state.
 - **initializing** — The port is trying to register with the SIP registrar.
 - **failed** — The port could not register with the SIP registrar.
 - **idle** — The port has registered and is now waiting to do some work.
 - **picked_up** — The port has been picked up.
 - **ringing** — The port is ringing.
 - **connected** — A call is in progress.
 - **not registered** — The port has not been successfully registered with the communication platform.
- **Calls Processed** — The number of calls on the port (since the Call Director SIP Service server machine was last rebooted).

To configure the ports, see [Section 3.3.6, “Configuring the ports”](#), on page 29.

3.4.4 Viewing the logs

You can view the Call Director SIP Service log files and control what level of detail is written to the log files.

To view the logs:

- In the left pane, expand **Monitoring**, expand **Logging**, and then click **Current Log**.

The screenshot shows the 'Call Director SIP Service - Internet Explorer' window. The left navigation pane has 'Monitoring' expanded, showing 'System and Statistics', 'Port Status', 'Security', 'Logging', and 'Archived Logs'. 'Logging' is selected. The main content area is titled 'Logging' and shows a table of log entries. Below the table are 'Log View Filtering Options' with 'View Level' and 'Level' both set to 'Debug', and buttons for 'Clear Logs' and 'Download Logs'.

Date	Log-Level	Log-Source	Error String
2014-05-14 20:46:16 385096	DEBUG	APP	cConfigMonitor::handleMessage() msgType: 9
2014-05-14 20:46:16 385354	DEBUG	APP	cConfigMonitor::handleMessage() msgSubType
2014-05-14 20:46:16 385368	DEBUG	APP	cConfigMonitor::handleMessage() LOGGING_CC

To change the level of detail shown on the screen:

- In the **View Level** list, select the level and click **Apply**.

To choose the level of detail to be logged from now on:

- In the **Level** list, select the level, and then click **Apply**. **Debug** is the most detailed level, and **Emergency** is the least.

Configuring the Call Director SIP Service

Viewing system information

- **Emergency** — shows only the most important messages.
- **Alert** — shows the above plus important alerts.
- **Critical** — shows the above plus critical items that require attention.
- **Error** — shows the above plus all error messages.
- **Warning** — shows the above plus all warnings.
- **Notice** — shows the above plus notices of major software operations.
- **Information** — shows the above plus detailed information about the software operations.
- **Debug** — shows the above plus trace information about all the software operations.

NOTE: Setting the log level to a very detailed level may affect performance.

To delete all log entries:

- Click **Clear Logs**.

To save the log file to disk:

- Click **Download Logs**.

This saves the logs to your local machine via the Web browser (not to the Call Director SIP Service server machine).

NOTE: If the log file is larger than 10 MB it will not be displayed and can only be downloaded.

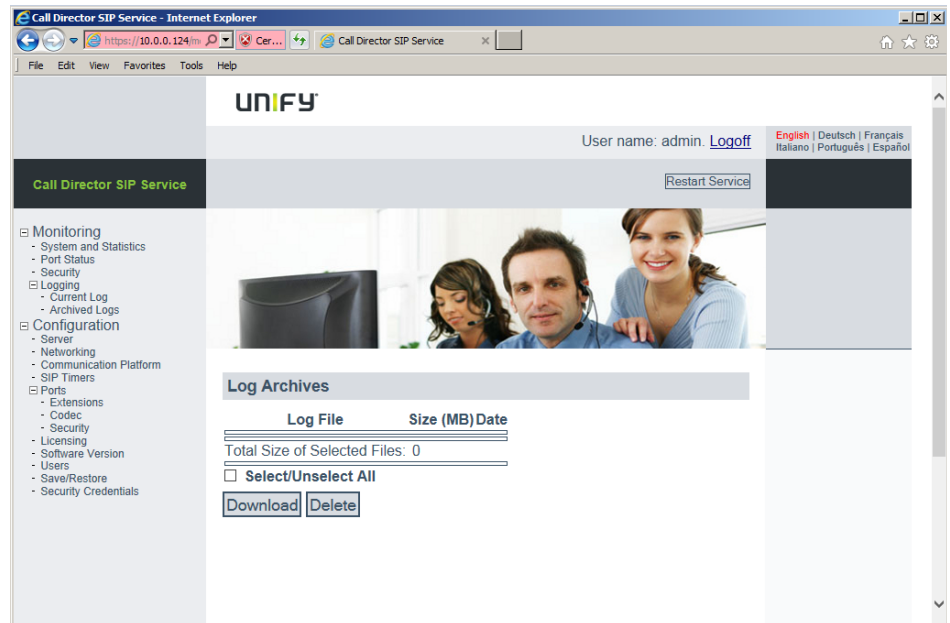
Archived Logs

Periodically, the Call Director SIP Service archives old logs.

- Every hour, if the log is 1 GB or larger, the log is archived.
- The last 50 archived logs are kept and labelled sequentially. The file labelled `cdss.log.0.gz` is always the latest.
- All logs older than 365 days are deleted automatically.

To download archived logs:

1. In the left pane, expand **Monitoring**, expand **Logging**, and then click **Archived Logs**.



2. To download one or more logs, select them and click **Download**.
All selected logs are downloaded in one file: `cdss_archived_logs.tar`.
3. To delete one or more logs, select them and click **Delete**.

Configuring the Call Director SIP Service

Viewing system information