

Spectralink IP-DECT Server 200/400/6500

Interoperability Guide

Microsoft Lync/Skype for Business Server

Copyright Notice

© 2013 - 2018 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Warranty

The Product Warranty and Software License and Warranty and other support documents are available at <http://support.spectralink.com/>.

Contact Information

US Location
+ 1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

UK Location
+44 (0) 20 3769 9800

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com

Denmark Location
+45 75602850

Spectralink Europe ApS
Bygholm Søpark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

Contents

About This Guide	5
Infrastructure Version Information	5
Available Licenses	5
Related Documentation	6
Feature List	7
Introduction	9
Manual User Entry on Spectralink IP-DECT Server 200/400/6500	9
Trusted Server	10
Handset Login	11
About Certificates	12
Microsoft Lync/Skype for Business Server	13
System Access	13
Creating a DNS Entry on the DNS Server	13
Downloading and Exporting a Root CA Certificate	14
Creating a Host Certificate for Trusted Server (Optional - But Recommended)	15
<i>To Request a Security Certificate for the Spectralink IP-DECT Server using IIS Manager</i>	15
Adding a Spectralink IP-DECT Server as Trusted Application Server	17
<i>Configuration Powershell Example Lync/Skype for Business Server</i>	17
Enabling PIN Authentication	18
Assigning PIN to User	18
Configuring Handset Login	18
<i>Enable Handset Login on Spectralink IP-DECT Server</i>	18
<i>Enable Handset Login on Spectralink DECT Handset</i>	19
Spectralink IP-DECT Server	20
To Order a License	20
To Load the License from the Web Based Administration Page	20
Importing Certificates	21
<i>Host Certificates</i>	21
<i>CA Certificates</i>	21
Configuring the Spectralink IP-DECT Server	22
<i>General Settings</i>	22
<i>Lync/Skype for Business Server Settings</i>	22
<i>SIP Settings</i>	22
Adding Users and Handsets	25
<i>To Add Users to the Spectralink IP-DECT Server from the Web Based Administration Page</i>	25

Presence Description	27
Presence Feature in Handset Menu	28
Presence on Lync/SfB Client when Handset is Idle	28
Presence on Lync/SfB Client when Handset is in a Call	29
Overview of Presence Status in the Lync/SfB Client	30
Example of XML Configuration File	31

About This Guide

This guide describes how to configure a Spectralink IP-DECT Server for connecting to a Lync/Skype for Business Server (SfB Server).

This guide is intended for qualified technicians and the reader is assumed to have a basic knowledge about the Spectralink IP-DECT Server and the Lync/Skype for Business Server. It is also assumed, that you have an installed and functioning Lync/Skype for Business Server and Spectralink IP-DECT Server.

The guide is divided into two parts:

- Lync/Skype for Business Server part
- Spectralink IP-DECT Server part

Each part describes the general configuration and the user administration.

Infrastructure Version Information

- To support the configuration described in this guide, the Spectralink IP-DECT Server must have firmware version (200 PCS18B or 400/6500 PCS17Ba) or newer.
- Spectralink DECT Handsets 7522/7532, 7622/7642 and 7722/7742 must have firmware PCS17Ha.

Spectralink DECT Handset 7502 must have firmware PCS18C.

Spectralink DECT Handset 7202/7212 and Spectralink Butterfly only have basic functionality.



Note:

The examples in this guide are made with IP-DECT Server firmware PCS17Ba.

Available Licenses

- Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 200 (part no 1407 5511)
- Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 400 (part no. 1407 5510)
- Lync/SfB + Security (TLS, SRTP) | IP-DECT Server 6000/6500 (part no. 1407 5270)

Related Documentation

All Spectralink documents are available at <http://support.spectralink.com/>.

Subject	Documentation
Lync/Skype for Business Server and Lync/Skype for Business Client	Navigate to the Microsoft documentation site for the latest Microsoft documentation.
Spectralink DECT Handsets	For more information about the handset, refer to the user guide available online at http://support.spectralink.com/products .
Site Survey Function in Handset	For more information about the site survey function in handset, refer to the guide available online at http://support.spectralink.com/products .
Synchronization and Deployment	For more information about synchronization and deployment, refer to the guide available online at http://support.spectralink.com/products .
Spectralink IP-DECT/DECT Server	For more information about the server, refer to the guide available online at http://support.spectralink.com/products .
Provisioning	For more information about provisioning, refer to the guide available online at http://support.spectralink.com/products .
Spectralink Technical Bulletins	Available online at http://support.spectralink.com/products .
Release Notes	Document that describes software changes, bug fixes, outstanding issues, and hardware compatibility considerations for new software releases. Available online at http://support.spectralink.com/products .
Spectralink DECT Training material	<p>In order to gain access to the Spectralink training material, you must attend training and become Spectralink Certified Specialist.</p> <p>Please visit http://partneraccess.spectralink.com/training/classroom-training for more information and registration.</p>

Feature List

The following features are supported:

	Supported features
Telephony	<ul style="list-style-type: none"> • Basic Calling • Call Hold • Call Transfer • Call Waiting • Call Forward • Message Waiting • Music on Hold (MOH) • Call Completed Elsewhere • E911 (75xx, 76xx, 77xx only) • Private Line (72xx, 75xx, 76xx, 77xx only) • Conference (Join)
User experience	<ul style="list-style-type: none"> • Federation • Presence (7522/7532, 76xx, 77xx only) • Centralized phone book via Active Directory and LDAP • SIP URI Support Phone Book (75xx, 76xx, 77xx only)
Security	<ul style="list-style-type: none"> • TLS • SSRTP/ SRTP/ RTP • STUN/TURN/ICE
Management/Administration	<ul style="list-style-type: none"> • Call Admission Control • Client Inventory • Resiliency • QoE
Voice Quality	<ul style="list-style-type: none"> • Codecs: G.726 (default), G.711 • Media Bypass
Value added Spectralink features	<ul style="list-style-type: none"> • Rich APIs for third-party solutions integration • Multi-language (on handsets) • Centralized management and provisioning via DECT server management capability • Plug and play DECT is easy to use and fast to deploy • Real Time Location Services (RTLTS)



Note:

Internal messaging is not possible when using Lync/SfB on a Spectralink IP-DECT Server because the handsets only have SIP URIs and no extension number.

The Spectralink IP-DECT Server use the extension field (web based Administration Page > **Users** > **List Users**), to match the number that you want to send a message to (handsets to handset). Since this is not a number, but a name, internal messaging is not possible.

Introduction

Setting up a Spectralink IP-DECT Server for usage in a Lync/Skype for Business environment requires a number of configuration steps to be performed on the Spectralink IP-DECT Server and in some cases also on the Lync/Skype for Business Server.

In order to enable the Lync/Skype for Business support, a Lync/SfB + Security (TLS, SRTP) License must be installed on the Spectralink IP-DECT Server.

The connection to the Lync/Skype for Business Server is secured by the TLS protocol which requires that a CA certificate used to sign the certificate of the Lync/Skype for Business Server must be installed on the Spectralink IP-DECT Server. When the Spectralink IP-DECT Server is added to the Lync topology as trusted server, it also requires that a host certificate is installed in order for the Lync/Skype for Business Server to authenticate the connection. Other configurations do not require a host certificate installed, but it is strongly recommended as it also allows a secure and authenticated connection to the Spectralink IP-DECT Server's web based Administration Page. For more information, see "[About Certificates](#)" on page 12.

The Spectralink IP-DECT Server supports three different methods of user administration, each with a number of configuration requirements and supported features:

- [Manual User Entry](#) on Spectralink IP-DECT Server
- [Trusted Server](#) (optional - but recommended)
- [Handset Login](#)

Manual User Entry on Spectralink IP-DECT Server 200/400/6500

In Manual Entry mode, all user data and credentials (including passwords) must be entered and maintained by the Spectralink IP-DECT Server administrator and the handsets can be used without any further setup. Authentication towards the Lync/Skype for Business Server is done using TLS-DSK with fallback to NTLM. No additional configuration is needed on the Lync/Skype for Business Server.

To use manual user entry on the Spectralink IP-DECT Server 200/400/6500, the following steps are necessary:

1. Install Lync/SfB + Security (TLS, SRTP) License on Spectralink IP-DECT Server
2. Configure Spectralink IP-DECT Server
3. Install CA certificate on Spectralink IP-DECT Server
4. Install Host certificate on Spectralink IP-DECT Server (optional)
5. Create users on Spectralink IP-DECT Server

Trusted Server

In Trusted Server mode, the Spectralink IP-DECT Server is added to the Lync/Skype for Business topology as a trusted server. Running as a trusted server causes the Spectralink IP-DECT Server to authenticate using a Host certificate with a MTLS connection toward the Lync/Skype for Business Server, removing the need for entering user password into the Spectralink IP-DECT Server. All other user information must still be entered into the Spectralink IP-DECT Server.



Note:

Trusted server is only supported when connecting directly to the Lync/Skype for Business Server frontend, not when connecting through an edge server.



Note:

E911 support is not available in trusted server configuration.

To use trusted server, the following steps are necessary:

1. Install Lync/SfB + Security (TLS, SRTP) License on Spectralink IP-DECT Server
2. Configure Spectralink IP-DECT Server
3. Install CA certificate on Spectralink IP-DECT Server
4. Install Host certificate on Spectralink IP-DECT Server
5. Create Spectralink IP-DECT Server DNS entry
6. Add Spectralink IP-DECT Server as trusted server in Lync topology
7. Create users on Spectralink IP-DECT Server

Handset Login

In Handset Login mode, no user data is required to be entered into the server by the Spectralink IP-DECT Server administrator, but is rather entered directly on the handset by the user. Authentication towards the Lync/Skype for Business Server is done using TLS-DSK with fallback to NTLM. No additional configuration is needed on the Lync/Skype for Business Server. When using handset login, the user can authenticate either using username and password or, if PIN authentication is enabled on the Lync/Skype for Business Server, with phone extension and PIN.



Note:

Handset login requires handset firmware PCS17H (7522/7532, 7622/7642, 7722/7742) or PCS18C (7502). Older or third-party handsets must be manually entered into the Spectralink IP-DECT Server.



Note:

PIN authentication is available if enabled on the Lync/Skype for Business Server and requires no settings on the Spectralink IP-DECT Server.

To use handset login, the following steps are necessary:

1. Install Lync/SfB + Security (TLS, SRTP) License on Spectralink IP-DECT Server
2. Configure Spectralink IP-DECT Server
3. Install CA certificate on Spectralink IP-DECT Server
4. Install Host certificate on Spectralink IP-DECT Server (optional)
5. Enable Handset Login on Spectralink IP-DECT Server

For more information, see "[Configuring Handset Login](#)" on page 18.

About Certificates

To interoperate with the Lync/Skype for Business Server, the Spectralink IP-DECT Server support TLS as transport protocol for SIP signaling. This requires a root Certification Authority (CA) certificate on the Spectralink IP-DECT Server.

The Spectralink IP-DECT Server is delivered with a CA certificate bundle with common public CA certificate. This means that the Spectralink IP-DECT Server will accept certificates, for example, issued by VeriSign out-of-the-box.

In addition to the CA bundle, the web based Administration Page allows installation of a local CA certificate bundle. If the certificate is generated by a local authority (such as a service provider or the local IT department), you can import a certificate bundle in PEM-format (also known as base 64).

Furthermore, the Spectralink IP-DECT Server supports installing a host certificate that authenticates the identity of the Spectralink IP-DECT Server when configured as trusted server and also when a browser accesses the web based Administration Page.



Note:

It is important that the Common Name and a Subject Alternative Name (SAN) values in the certificate matches both the hostname configured in the Spectralink IP-DECT Server and the DNS entry created for the Spectralink IP-DECT Server.

The host certificate can be in either a PKCS#12 format file (.pfx file extension) containing both certificate and private key or as two individually PEM formatted files. Both formats can optionally have password protection on the private key.

Microsoft Lync/Skype for Business Server

Below is a description of how to create a DNS entry for the Spectralink IP-DECT Server, how to download a CA certificate, how to create a Host certificate for Trusted Server, how to add the Spectralink IP-DECT Server as trusted application server, how to assign a PIN to a user, and how to configure Handset Login.

System Access

To configure the Spectralink IP-DECT Server you may need access to the following systems:

- Lync/Skype for Business Server
- Domain Name Service (DNS) Server
- Certificate Authority (CA)
- Internet Information Services (IIS) to request a Server Certificate

Creating a DNS Entry on the DNS Server



Note:

A DNS Entry is required for trusted server and generally recommended for ease of use and security.

In the following example a Windows 2012 Server is used.

1. Create a hostname for the Spectralink IP-DECT Server and Domain DNS Server.
2. Add the **Spectralink IP-DECT Server** as New Host. The FQDN name will be used in the configuration later. For more information, see "[General Settings](#)" on page 22.
3. Click **Add Host**.

Downloading and Exporting a Root CA Certificate

If not using the public CA certificates provided with the Spectralink IP-DECT Server it is necessary to download and export a local CA certificate.

The following describes how to export the CA certificate from a Microsoft Certificate Authority (MCA). If not using MCA, please refer to the vendor documentation.



Note:

The Spectralink IP-DECT Server accept a Base64 Encoded x.509 CA certificate that uses a .cer extension.

1. Open Microsoft Certificate Authority directly in your web browser. <IP address>/certsrv.
For example, <http://172.29.193.33/certsrv/>
2. Select **Download a CA certificate**.



Note:

Download of CA certificate is not required if the server certificate is signed by a public CA.

3. Under **Encoding method**, select the current CA certificate. Set the encoding method to **Base 64** (.CER)
4. Click **Download CA certificate**.
5. The CA certificate is downloaded to your browser and will be used later in the configuration of the Spectralink IP-DECT Server.

Creating a Host Certificate for Trusted Server (Optional - But Recommended)

Host certificates can be imported as PKCS#12 (.PFX,.P12) or PKI X.509 format + a key file. The creation may be performed on Internet Information Server (IIS).

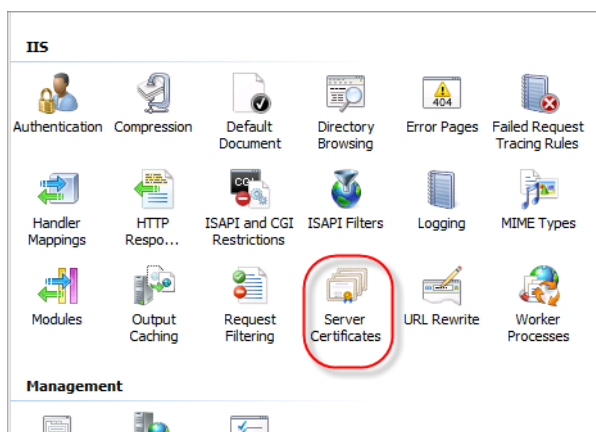


Note:

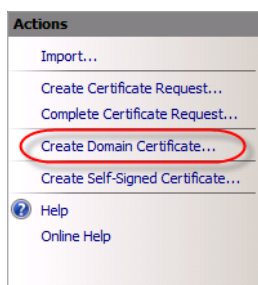
In the example below on how to create and export a host certificate for trusted server, we have used the Internet Information Server (IIS) in our test environment to create the certificate. Using the IIS is not necessary, if you have another way of creating the host/server certificate, this can be used as well.

To Request a Security Certificate for the Spectralink IP-DECT Server using IIS Manager

1. On the Lync/Skype for Business Server, select **Administrative Tools > Internet Information Services (IIS) Manager** to open IIS.
2. Under Connections, double-click the server name.
3. Under IIS, in the **Features View**, double-click **Server Certificates**.



4. Under **Actions** (far right), click **Create Domain Certificate**.



The **Create Certificate** wizard appears.

- In the **Distinguished Name Properties** panel, enter the required information in all fields, and then click **Next**.

**Note:**

Do not leave any fields empty under **Distinguished Name Properties**. All fields must be completed to finalize the configuration.

Create Certificate

Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: IP-DECT6500.EWSLynctest.com

Organization: Spectralink

Organizational unit: Service

City/locality: Horsens

State/province: Jylland

Country/region: DK

Previous Next Finish Cancel

- In the **Common name** field, enter the FQDN of the Spectralink IP-DECT Server that you created in the previous step, and then click **Next**.
- In the **Online Certification Authority** panel, click the relevant Certificate Authority from the list, and enter a relevant name in the field from the pop-up box.
- Click **Finish**. Your certificate has been created.
- Double-click on the certificate just created, and select details and copy to file.
- Click **Next**, and then select the **Yes, export the private key** check box.
- Click **Next**, select **Cryptographic Message Syntax Standard – PKCS** and remember to select the Include all certificates in the certification path if possible check box. Click **Next**.
- Enter a name for the certificate.
- Select the certificate you just created, and then, in the Actions pane (far right), select **Export**.
- Choose the file export path, and specify a password for the certificate.

The password is used when importing into the Spectralink IP-DECT Server. For more information, see "[Configuring the Spectralink IP-DECT Server](#)" on page 22.

Adding a Spectralink IP-DECT Server as Trusted Application Server

Open Lync Management Shell and enter the 3 commands below. The text marked in bold should be replaced with values from your Lync/SfB typology. If any database errors are displayed when you enter the information, run the Lync Server Management Shell as Administrator.

1. Enter:

```
New-CsTrustedApplicationPool -Identity <FQDN of IP-DECT Srv> -Site <SiteID> -
RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true -Registrar
<FQDN of SBA/Lync frontend pool>
```

2. A warning is displayed. Click **Y** for Yes.

3. Enter:

```
New-CsTrustedApplication -ApplicationId dect -Port 5061 – TrustedApplicationPoolFqdn
<FQDN of IP-DECT Srv>
```

4. Enter:

```
Enable-CsTopology
```

The following Powershell commands help you obtain the information for the commands above:

- To obtain Site ID, enter: Get-CsSite
- To obtain FQDN, enter: Get-CsPool



Note:

All servers in the Lync domain have to be online.

Configuration Powershell Example Lync/Skype for Business Server

1)

```
New-CsTrustedApplicationPool -Identity IP-DECT6500.example.org -Site 1
-RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true -
Registrar.example.org
```

2)

```
New-CsTrustedApplication -ApplicationId dect -Port 5061 -TrustedApplicationPoolFqdn
IP-DECT6500.example.org
```

3)

```
Enable-CsTopology
```

Enabling PIN Authentication

To provide PIN authentication to users, the Spectralink IP-DECT Server must be able to locate the web service on the Lync/SfB frontend that provisions user certificates. The URL for this web service should be provided to the Spectralink IP-DECT Server from the DHCP server in the vendor specific option 43, for the vendor class "MS-UC-Client".

Please refer to the Microsoft document "Setting Up DHCP for Devices" for further details on configuring the correct DHCP options.

Assigning PIN to User

When using PIN authentication the administrator must assign a PIN to the user.



Note:

It is not necessary to assign a PIN to a user if using Trusted Server or if using user name and password for authentication .

1. Open Skype for Business Server Management Shell.
2. Enter the following command:

```
Set-CsClientPin -Identity john.doe@example.org -Pin 123456
```

Configuring Handset Login

Enable Handset Login on Spectralink IP-DECT Server

1. Ensure that Lync is enabled (**Configuration > Lync**)
2. Click **Configuration**, and then click **Wireless Server**.
3. Enter the required information:

Field	Setting
Handsets	
Handset sharing	Enable
Handset login	Enable

Handsets	
Handset sharing	<input checked="" type="checkbox"/>
Handset login	<input checked="" type="checkbox"/>

Enable Handset Login on Spectralink DECT Handset

The Handset Login feature can be invoked in two ways:

- By utilizing MSF function number 9, either from the handset main menu or by long-pressing the '9' key (not supported by Handset 7502). Long-press must be enabled in the **Settings > Advanced > Long Key** menu. For more information, see Handset User Guides.
- Through the shortcut menu using the Sign in/out shortcut. For more information, see Handset User Guides.

When invoking the Handset Login feature, a menu is presented allowing the user to select signing in with either extension and PIN (if configured) or with user name and password. Entering the required credentials will allow the Spectralink IP-DECT Server to connect the user to the Lync/Skype for Business Server and the handset will be ready for use.

How to Sign In

When accessing the Sign in menu, you can choose between **PIN Sign in** or **Sign in** (**PIN Sign in** is only visible if PIN authentication is available). This is configured on the Lync/Skype for Business Server).

1. When in idle mode, access the Sign in menu by using either Sign in/out shortcut or long-press key 9.
2. If selecting **PIN Sign in**:
 - Enter number and click **OK**.
 - Enter PIN, and click **OK**.
3. If selecting **Sign in**:
 - Enter user and click **OK**.
 - Enter password, and click **OK**.
4. The handset is now ready for use.

How to Sign Out

1. When in idle mode, sign out by using either Sign in/out shortcut or long-press key 9.
2. Select **Sign out** and click **OK**.

Spectralink IP-DECT Server

Below is a description of how to order and load the Lync/SfB + Security (TLS, SRTP) License, import certificates, configure the Spectralink IP-DECT Server and how to add users and handsets to the system.

To Order a License

The Spectralink IP-DECT/DECT Server requires a Lync/Skype for Business License to connect to a Lync/Skype for Business Server. The license can be ordered through normal Spectralink channels.

1. Send your Purchase Order (PO) including the software part number and the number of licenses needed to Spectralink Order Management via (EMEA and APAC) emeaom@spectralink.com or (NALA) nalaom@spectralink.com.
2. When your order is processed, Order Management will send you an email including an Authentication Product Key for your software license.
3. To activate your software license, use the License Key Generator available at <http://support.spectralink.com/keycode>.



Note:

Please note that once a software license is generated this is locked to the specified ARI code, and cannot be changed.

To Load the License from the Web Based Administration Page

1. If using Spectralink IP-DECT , click **Administration**, and then click **License**.

Licenses	
Load license	
License **	<input type="text" value="3a1970e88f442a0fe055672efcf3ab184c877830000000041000000000000"/> <input type="button" value="Load"/>

2. Copy the provided license key from your email, paste it in the **License** field, and then click **Load**.
3. Reboot the server to activate the license.

Importing Certificates

It is necessary to import following certificates into the Spectralink IP-DECT/DECT Server:

- [Host certificate](#)
- [CA certificate](#)

For more information about certificates, see "[About Certificates](#)" on page 12.

Host Certificates

If using a Trusted Server it is necessary to import a Host Certificate into the Spectralink IP-DECT Server. The Host Certificate can be created and exported from the Lync/Skype for Business Server. For more information, see "[Creating a Host Certificate for Trusted Server \(Optional - But Recommended\)](#)" on page 15.

1. Click **Configuration**, and then click **Certificates**.
2. Under **Host certificate chain**, click **Browse** to find the relevant host certificate file.
3. In the **Password** field, enter the password.
4. Select **PKCS#12**.
5. Click **Import Certificate**.

CA Certificates



Note:

If the certificate of the Lync/Skype for Business Server is signed by a public CA certificate, it is not required to import and install a local CA certificate bundle.

Before you can import the local CA Certificate, it must be exported from a Microsoft Certificated Authority. For more information, see "[Downloading and Exporting a Root CA Certificate](#)" on page 14.

1. Click **Configuration**, and then click **Certificates**.
2. Under **CA certificates**, click **Browse** to find the relevant CA certificate file (*.pem file).
3. Click **Import List**.
4. Reboot the server.

Configuring the Spectralink IP-DECT Server

General Settings

1. Click **Configuration**, the **General Configuration** page displays.
2. Under **DNS**, enter the hostname/FQDN in the **Hostname (FQDN)** field. For information about creating the hostname, see "[Creating a DNS Entry on the DNS Server](#)" on page 13.
3. Click **Save**.

Lync/Skype for Business Server Settings

It is necessary to enable Lync/Skype for Business Server support.

1. Click **Configuration**, and then click **Lync**.
2. Enable Lync support.
3. Enable Trusted Server, if using this.
4. Click **Save**, and then reboot the system.

SIP Settings

The Spectralink IP-DECT Server requires a few SIP settings to be adjusted in order to connect properly to the Lync/Skype for Business Server.



Note:

SIP settings not mentioned below should be left at their default values.

To modify the SIP settings from the web based Administration Page:

1. Click **Configuration**, and then click **SIP**.
2. Modify the settings below.

Field	Setting
SIP Configuration - General	
Transport	TLS
DNS method	Select DNS SRV .
Default domain	Enter the SIP domain name of the Lync/Skype for Business Server. E.g. John.Doe@example.org should be "example.org" . Note: SIP domain name refers to the Lync/Skype for Business Server - SIP domain name, not the AD domain name, if they are different.

Field	Setting
Register each endpoint on separate port	Enable if Spectralink IP-DECT Server is located on the external side of the edge server.
GRUU	Enable
Use SIPS URI	Check that this setting is NOT enabled.
SIP Configuration - Media	
Ignore SDP version	Enable
Enable media encryption (SRTP)	Enable SRTP (encrypted RTP) support towards external SIP endpoints.
Require media encryption (SRTP)	Enable Note: This setting must match the setting in the Lync/Skype for Business Server.
Include lifetime in SDES offers	Enable
Include MKI in SDES offers	Enable

Example of SIP configuration:

SIP Configuration	
General	
Local port * **	5060
Transport * **	TLS ▼
DNS method * **	DNS SRV ▼
Default domain * **	example.org
Register each endpoint on separate port **	<input type="checkbox"/>
Send all messages to current registrar **	<input type="checkbox"/>
Registration expire(sec) *	3600
Handset power off action	Ignore ▼
Max forwards *	70
Client transaction timeout(msec) *	16000
SIP type of service (TOS/Diffserv) * **	96
SIP 802.1p Class-of-Service *	3
GRUU	<input checked="" type="checkbox"/>
Use SIPS URI	<input type="checkbox"/>
TLS allow insecure **	<input type="checkbox"/>
TCP ephemeral port in contact address **	<input type="checkbox"/>
Media	
Packet duration(msec) *	20 ▼
Media type of service (TOS/Diffserv) *	184
Media 802.1p Class-of-Service *	5
Port range start * **	58000
Codec priority *	1: AAL2-G726-32/8000 ▼
	2: PCMU/8000 ▼
	3: PCMA/8000 ▼
	4: None ▼
	5: None ▼
	6: None ▼
SDP answer with preferred codec	<input type="checkbox"/>
SDP answer with a single codec	<input type="checkbox"/>
Ignore SDP version	<input checked="" type="checkbox"/>
Enable media encryption (SRTP) **	<input checked="" type="checkbox"/>
Require media encryption (SRTP)	<input checked="" type="checkbox"/>
Include lifetime in SDES offers	<input checked="" type="checkbox"/>
Include MKI in SDES offers	<input checked="" type="checkbox"/>

3. Click **Save**, and then reboot the system.

For an example of the configuration XML file from your Spectralink IP-DECT Server, see ["Example of XML Configuration File"](#) on page 31.

Adding Users and Handsets

Each individual DECT handset/user must be added to the Spectralink IP-DECT Server and also on to the Lync/Skype for Business Server. This section describes how to add the handsets to the Spectralink IP-DECT Server.



Note:

It is not necessary to add users and handsets if using Handset Login.

To Add Users to the Spectralink IP-DECT Server from the Web Based Administration Page

1. If using Spectralink IP-DECT 400/6500, click **Users**, click **List Users**, and then click **New**.
2. Enter the required information:

Field	Setting
DECT device	
IPEI (optional)	If a specific handset is being subscribed for this extension, enter the IPEI number of the actual handset. The IPEI number is readable from the label on the product. If this is not the case this field can be left empty and it will auto-fill when the handsets subscribe. Note: A SIP REGISTER will not be sent before there is an IPEI number present.
Access code (optional)	Admins can define a system wide or individual access code as extra wireless security during the subscription process.
User	
Standby text (optional)	A standby text is a fixed label shown in the top left part of the screen on the DECT handset when in idle state. Note: This feature is only available if Spectralink DECT handsets are being used. If third party DECT handsets are being subscribed, this feature is not supported.
SIP	
Username/Extensions	Enter SIP username. E.g. Jane.Doe

Field	Setting
Display name (optional)	The name of the user can be entered here.
Authentication user	Enter the user ID of the Lync/SfB end user. E.g. Jane.Doe
Authentication password	Enter the digest credential of the Lync/SfB end user. Note: A password is not necessary when using Trusted server.

User

DECT device

Model

Software part number

Firmware

IPEI

User

PIN code

Standby text

Disabled

SIP

Username / Extension *

Domain

Displayname

Authentication user

Authentication password

Features

Call forward unconditional

*) Required field

3. Click **Save**.
4. When the users have been added to the Spectralink IP-DECT Server, the handsets must be DECT subscribed in order to be able to communicate with the Spectralink IP-DECT Server. For more information, see Handset User Guides.

Presence Description

Presence is the ability to detect another user's availability. Using Skype for Business, users can display their Presence status, e.g. **Available**, **Away**, **Do Not Disturb**, or **Offline** - to let others know their availability.


The availability can be set in the Skype for Business Client and by using the Presence feature in the Spectralink DECT Handset. Also, the Presence status is displayed in both the client and the handset display. When in a call, the status **In a call** is displayed in the client, when ending the call, this status changes to e.g. **Available**. Other users availability are visible in the Skype for Business but not in the Spectralink DECT Handset, here only the handset user's availability is displayed.



Note:

Skype for Business makes it possible to define a Private Line and assign private numbers to a user at which the user can be reached directly independent of which Presence status is used. Normal incoming calls do not come through if presence is set to **Do Not Disturb**, incoming private line calls do come through. Private line calls do not follow **Do Not Disturb** settings. The private line numbers do not appear in the phone book directories.

 appears when incoming private line call arrives.

 appears when in a private line call.

Normal handset functionality, such as e.g. **Call Forward**, does not work when receiving a private line call.

Contact your system administrator for more information.



Note:

The Presence feature is not available on Spectralink Handset 72xx, Spectralink Handset 7502 and Spectralink Handset Butterfly.

Presence Feature in Handset Menu

From the Presence menu, you can set the following status about your presence:

- Available
- Busy
- Do Not Disturb
- Be Right Back
- Appear Away

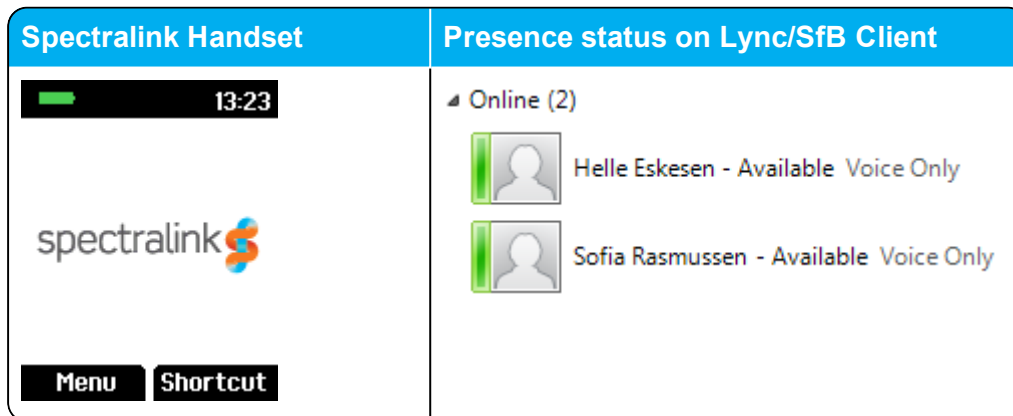


The selected status is shown with an icon in the handset display.

The same Presence status is shown in the Lync/Skype for Business Client.

Presence on Lync/SfB Client when Handset is Idle

The images below show how the Presence status is indicated on a Lync/Skype for Business Client, when a Spectralink DECT Handsets is idle.

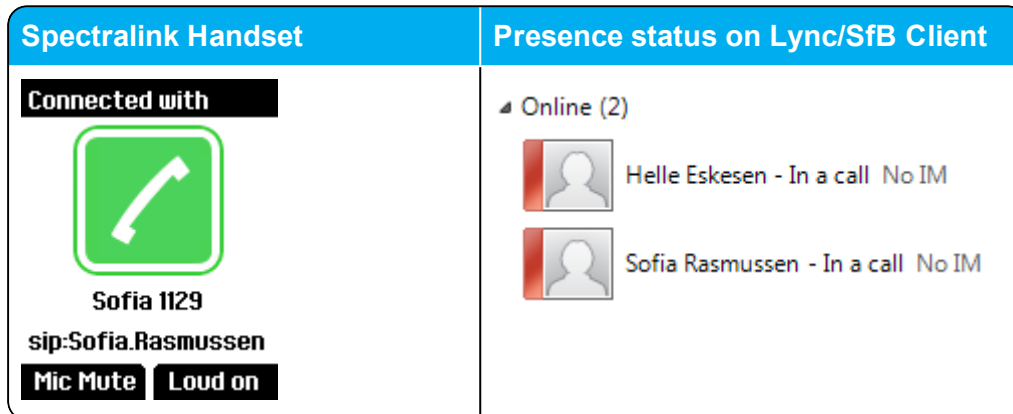


Note:

The users in this example only have a Spectralink DECT Handset and are not logged on with a Lync/Skype for Business Client. Therefore, **Voice Only** is displayed.

Presence on Lync/SfB Client when Handset is in a Call

The images below show how the Presence status is indicated on a Lync/Skype for Business Client, when a Spectralink DECT Handset is in a call.



Note:

The users in the example only have a Spectralink DECT Handset and are not logged on with a Lync/Skype for Business Client. Because the Spectralink DECT Handset does not accept Instant Messages from the Lync/Skype for Business Client, **No IM** appears.

Overview of Presence Status in the Lync/SfB Client

The handset's presence status is set to **Available** for 5 minutes after it has been used.

▲ Online (2)



Helle Eskesen - Available Voice Only



Sofia Rasmussen - Available Voice Only

After 5 minutes, the handset status changes to **Inactive** if the handset is not used.



Helle Eskesen - Inactive 5 mins - Voice Only

After 10 minutes, the handset status changes to **Away** if the handset is not used.



Bo Suurballe - Away 35 mins - No IM

When a Spectralink DECT Handset is in use the presence status is **In a call**.

▲ Online (2)



Helle Eskesen - In a call No IM



Sofia Rasmussen - In a call No IM

Example of XML Configuration File

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<config>
<application>
  <enable_rpc>true</enable_rpc>
  <internal_messaging>true</internal_messaging>
</application>
<dect>
  <auth_call>true</auth_call>
  <handset_login>true</handset_login>
  <handset_sharing>true</handset_sharing>
  <send_date_time>true</send_date_time>
  <subscription_allowed>true</subscription_allowed>
</dect>
<feature_codes>
  <call_forward>
    <voicemail>
      <enable>*21*</enable>
    </voicemail>
  </call_forward>
</feature_codes>
<language>en</language>
<log>
  <syslog>
    <facility>16</facility>
    <level>info</level>
    <port>514</port>
    <scope_of_settings>all</scope_of_settings>
  </syslog>
</log>
<network>
  <bootproto>static</bootproto>
  <dns1>172.29.129.54</dns1>
  <dns2>172.29.129.47</dns2>
  <domain>example.org</domain>
  <gateway>172.29.192.1</gateway>
  <hostname>ip-dect.example.org</hostname>
  <ipaddr>172.29.198.6</ipaddr>
  <ipv6>
    <method>disabled</method>
  </ipv6>
  <netmask>255.255.240.0</netmask>
  <ntp>172.29.129.47</ntp>
  <timezone>CET-1CEST-2,M3.5.0/02:00:00,M10.5.0/03:00:00</timezone>
</network>
<rfp>
  <media>
    <port>57000</port>
  </media>
  <ptp>
    <tos>184</tos>
    <transport>12</transport>
  </ptp>
</rfp>

```

```

<security>
  <allow_http>>false</allow_http>
  <allow_new_media_resource>>true</allow_new_media_resource>
  <allow_new_rfp>>true</allow_new_rfp>
  <password_timestamp>1496219863</password_timestamp>
  <username>admin</username>
</security>
<sip>
  <callwaiting>>true</callwaiting>
  <client_transaction_timeout>16000</client_transaction_timeout>
  <dect_detach_action>deregister</dect_detach_action>
  <defaultdomain>example.org</defaultdomain>
  <dnsmethod>dnssrv</dnsmethod>
  <dtmf>
    <duration>270</duration>
    <info>>false</info>
    <rtp>>true</rtp>
    <rtp_payload_type>96</rtp_payload_type>
  </dtmf>
  <gruu>>true</gruu>
  <handset_login>>true</handset_login>
  <localport>5060</localport>
  <lync>
    <enable>>true</enable>
    <trusted>>false</trusted>
  </lync>
  <maxforwards>70</maxforwards>
  <media>
    <codecs>64,1,2,0,0,0</codecs>
    <port>58000</port>
    <ptime>20</ptime>
    <sdp_answer_single>>false</sdp_answer_single>
    <sdp_answer_with_preferred>>false</sdp_answer_with_preferred>
    <sdp_ignore_version>>true</sdp_ignore_version>
    <srtp>
      <enable>>true</enable>
      <lifetime>>true</lifetime>
      <mki>>true</mki>
      <required>>true</required>
    </srtp>
    <tos>184</tos>
    <vlan_cos>5</vlan_cos>
  </media>
  <music_on_hold>>true</music_on_hold>
  <mwi>
    <enable>>true</enable>
    <expire>3600</expire>
    <subscribe>>false</subscribe>
  </mwi>
  <onholdtone>>false</onholdtone>
  <pound_dials_overlap>>false</pound_dials_overlap>
  <proxy>
    <port>0</port>
    <port2>0</port2>
    <port3>0</port3>
    <port4>0</port4>
    <priority>1</priority>

```



```
<priority2>2</priority2>
<priority3>3</priority3>
<priority4>4</priority4>
<weight>100</weight>
<weight2>100</weight2>
<weight3>100</weight3>
<weight4>100</weight4>
</proxy>
<registration_expire>3600</registration_expire>
<send_to_current_registrar>false</send_to_current_registrar>
<separate_endpoint_ports>false</separate_endpoint_ports>
<showstatustext>true</showstatustext>
<tcp_contact_ephemeral_port>false</tcp_contact_ephemeral_port>
<tls_allow_insecure>false</tls_allow_insecure>
<tos>104</tos>
<transport>tls</transport>
<use_sips_uri>false</use_sips_uri>
<vlan_cos>3</vlan_cos>
</sip>
<snmp>
  <community>public</community>
  <enable>false</enable>
</snmp>
<upnp>
  <broadcast>false</broadcast>
  <enable>true</enable>
</upnp>
</config>
```