

Spectralink IP-DECT Server 400 and 6500

Spectralink IP-DECT Server 400 and 6500 and Microsoft® Lync™ Server Configuration Guide

Using a Spectralink IP-DECT Server 400 or Spectralink IP-DECT Server 6500 in a Microsoft Lync Server 2013 or Microsoft Lync Server 2010 Setup

Copyright Notice

© 2013 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.

Indhold

Chapter 1: Introduction	4
Overview.....	4
Firmware Compatibility	4
Transport Protocol.....	4
Chapter 2: Supported Features	5
SIP Authentication	6
Chapter 3: Configuration.....	7
Configuration Requirements.....	7
Chapter 4: Overview of Lync Server 2013 and 2010 Settings	8
Configuring the Microsoft Lync Server 2013 and 2010 Setup	8
Chapter 5: Required Settings for Spectralink IP-DECT Server....	12
Chapter 6: Spectralink IP-DECT Server Configuration.....	13
Configuring the IP-DECT Server for MS Lync Server 2013 or 2010 Support	13
Configure SIP Settings	14
Adding Users to Spectralink IP-DECT Server	16
Chapter 7: Known Limitations	18
Chapter 8: Third party endpoints	20
Chapter 9: Presence Description.....	21
NTLM:	22
TLS/MTLS:.....	23

Chapter 1: Introduction

This configuration guide describes how to setup a Spectralink IP-DECT Server 400 or 6500 in a Microsoft® Lync™ Server 2013 or 2010 installation.

Overview

The configuration guide includes the following information:

- Transport Protocol
- Supported Features
- SIP User Authentication
- Settings required for Lync Server 2013 and 2010
- Settings required for Spectralink IP-DECT Server
- Adding users to the Spectralink IP-DECT Server

Firmware Compatibility

The Spectralink IP-DECT Server interoperate with Lync Server 2013 and 2010 from firmware version PCS12_. The Spectralink Microsoft Lync Interoperability is backward compatible with Microsoft® Office Communications Server 2007 R2.

The communication protocol between Spectralink IP-DECT Server, Spectralink Media Resources, and Spectralink IP-DECT Base Stations is not backward compatible. This means that Spectralink Media Resources with firmware versions older than PCS08B_ and Spectralink IP-DECT Base Stations with firmware versions older than PCS08__ will not be able to connect to a Spectralink IP-DECT Server running firmware PCS08B_ or newer.

To minimize downtime, you need to update Spectralink Media Resources and Spectralink IP-DECT Server to firmware PCS012_ or newer and Spectralink IP-DECT Base Stations to firmware PCS12A_ or newer before rebooting any of these.

Transport Protocol

To interoperate with the Lync Server 2013 or 2010, the Spectralink IP-DECT Server support TLS as transport protocol for SIP signaling. This requires a Certificate Authority (CA) on the Spectralink IP-DECT Server.

The Spectralink IP-DECT Server are delivered with a Certificate Authority bundle with common Certificate Authorities. 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 GUI 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, there is support for server certificate. Trusted Server PFX 12 certificate is required if you are using local CA authority. This is also known as PKCS#12 file with password protection

Chapter 2: Supported Features

- SIP User Authentication via Trusted Server or NTLM
- Telephony features:
 - Call hold
 - Call transfer
 - Call forward
 - Call waiting
 - Message Waiting Indication (MWI)
 - Redial from Call log
 - Call logs (missed/received/placed calls)
 - Call completed elsewhere
 - Ad hoc conferencing - enables users to participate in conference calls
- Centralized phone book via Active Directory and LDAP
- Supported codecs: G.711
- SBA - Survival Branch Appliance - enables users to register through the SBA
- CAC - Call admission control - protects the network against oversubscription
- ICE - Interactive Connectivity Establishment
- Media Bypass
- Supports federation with users on Microsoft® Office Communication Server 2007 R2 devices
- Basic Presence. In the Microsoft® Lync™ 2013 or 2010 client the presence status of each subscribed Spectralink Handset is displayed as either “Available”, “Inactive”, “Away” or “In a call”.



Note

An initial log-in to a Lync client with each DECT user is required to activate the presence functionality of the handset. Alternatively, you can use the Presence bootstrapping tool for Lync Server 2013 or 2010. For more information, see <http://support.microsoft.com/kb/2737277>.

SIP Authentication

In a Lync Server setup, SIP users are authenticated against an Active Directory server. The following two authentication methods are supported:

System Authentication: Trusted Server

This is the recommended authentication method.

A CA and a Server (Host) Certificate is installed on the Spectralink IP-DECT Server 400 and 6500. TLS and MTLS are used to create a network of trusted servers and to ensure that all communications over the network are encrypted. All SIP communications between servers occur over MTLS. SIP communications from client to server occurs over TLS. Server-to-server connections rely on mutual TLS (MTLS) for mutual authentication. On a MTLS connection, the server that sends a message and the server that receives it exchange certificates from a mutually trusted CA. The certificates prove the identity of each server to the other.

User Authentication: NTLM

This authentication method is not recommended

Enter the credentials for each SIP user into the Spectralink IP-DECT Server 400 or 6500 either by using the web GUI or provisioning. It is not possible to change the Authentication Username or Password directly from the Spectralink DECT Handsets. It can only be changed via the Spectralink IP-DECT Server 400 or 6500.

Chapter 3: Configuration

Configuration Requirements

Several key systems need to be accessed and some settings need to be changed before the systems can integrate together.

Windows Lync Server 2013 or 2010 environment:

- Access to Microsoft Lync Server 2013 or 2010
- Access to Domain Name Service (DNS) Server
- Access to Microsoft Active Directory (AD), configuration, and administration
- Access to Certificate Authority (CA)
- Access to Internet Information Services (IIS) to create a Server Certificate

Spectralink IP-DECT Server 400 or 6500:

- Admin access to the Spectralink IP-DECT Server
- Spectralink Microsoft Lync Interop License (part no. 14075270) for Spectralink IP-DECT Server 6500
- Spectralink Microsoft Lync Interop License (part no. 14075510) for Spectralink IP-DECT Server 400
- External Syslog Server (recommended)



Note

To troubleshoot the system integration properly and to obtain errors from the Spectralink IP-DECT Server 400 or 6500, it is recommended that you use a Syslog Server to ensure that no critical errors from the Spectralink IP-DECT Server 400 or 6500 are left unresolved. You specify the Syslog settings in the Spectralink IP-DECT Server under General configuration -> Remote syslog. As a minimum, choose Error or Warning setting.

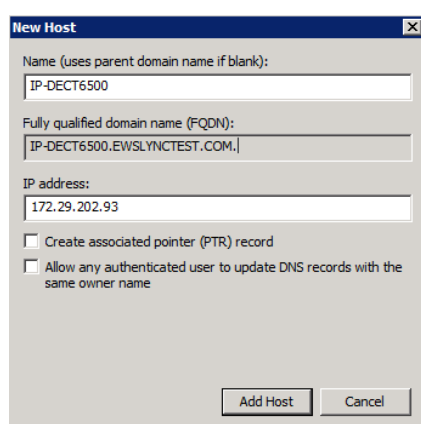
Chapter 4: Overview of Lync Server 2013 and 2010 Settings

- DNS entry for Spectralink IP-DECT Server
- CA certificate from Domain
- Host certificate for Trusted Server
- Adding the Spectralink IP-DECT Server as Trusted application server

Configuring the Microsoft Lync Server 2013 and 2010 Setup

Step 1: Create a DNS Entry on the DNS Server

- 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 later in the configuration later. See page [10](#).
- 3 Click the **Add Host** button.



Step 2: Download a CA Certificate

This step describes how to export the CA certificate from a Microsoft Certificated Authority. 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.

Microsoft Active Directory Certificate Services – EWSLYNCTEST-HORLYNCTEST01-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install](#)

To download a CA certificate, certificate chain, or CRL, select

CA certificate:

Current [EWSLYNCTEST-HORLYNCTEST01-CA]

Encoding method:

DER
 Base 64

[Install CA certificate](#)

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

3 Select the current CA certificate. Set the encoding method to **Base-64** (.CER)

4 Select **Download CA Certificate**

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

5 The Certificate is downloaded to your browser and will be used later in the configuration of the Spectralink IP-DECT Server 400 or 6500. See page [15](#)



Note

Step 2 is not required if the Lync Server 2010 certificate is signed by a public CA

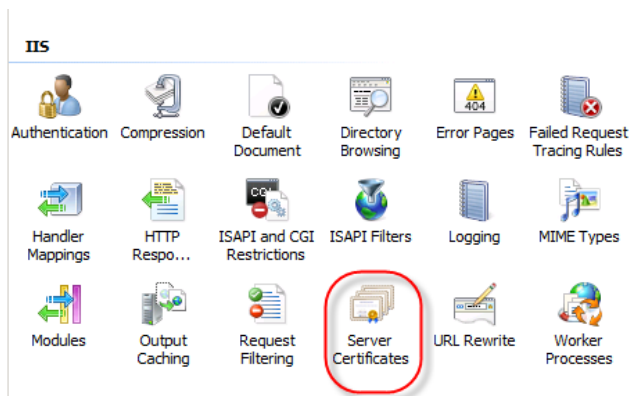
Step 3: Create a Host Certificate for Trusted Server

Host Chain certificates can be imported as PKCS#12 (.PFX,.P12) or PKI X-509 format + a key file. 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, this is not necessary, if you have another way of creating the Host/server certificate, this can be used as well, but the below is a guideline, on how this can be done using the IIS.

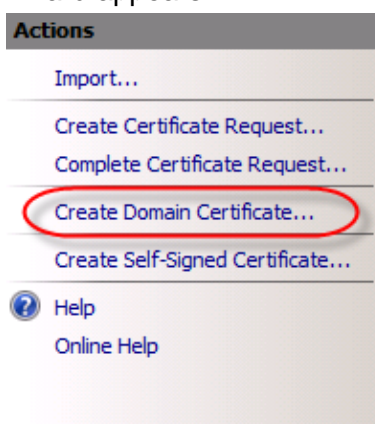
This action is performed on Internet Information Server (IIS) Cert SRV.

To request a security certificate for the Spectralink IP-DECT Server using IIS Manager 7, do the following.

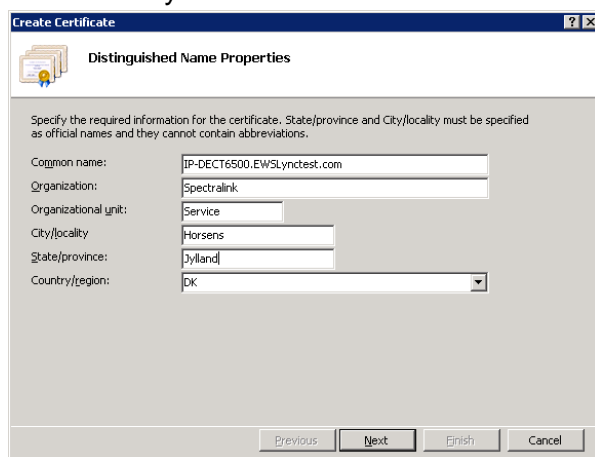
- 1 On the Lync Server, select Start > All Programs > Administrative Tools > Internet Information Services (IIS) Manager (7.0) to open IIS 7.
- 2 Under **Connections**, double-click the server name.
- 3 In the **Features View**, double-click **Server Certificates under IIS**.



- 4 In the **Actions** pane (far right), select **Create Domain Certificate**. The **Create Certificate** wizard appears.



- 5 In the **Distinguished Name Properties** panel, enter the required information in all fields. Do not leave any fields blank. All fields must be completed to finalize the configuration.



- 6 In the **Common name** field, enter the FQDN of the Spectralink IP-DECT Server that you created in step 1 above, and then click **Next**.
- 7 In the **Online Certification Authority** panel, select a Certificate Authority from the list, and enter a friendly name in the field from the pop-up box.
- 8 Click **Finish**. Your certificate has been created.
- 9 Select the certificate you just created, and then, in the **Actions** pane (far right), select **Export**.

- 10** Choose the file export path, and specify a password for the certificate. The password is used when importing on Spectralink IP-DECT Server. See page 16.

Step 4: Add 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 your Lync Server 2013 or 2010 Powershell commands. 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 example

1)

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

2)

```
New-CsTrustedApplication -ApplicationId dect -Port 5061 -
TrustedApplicationPoolFqdn
IP-DECT6500.ewslynctest.com
```

3)

```
Enable-CsTopology
```

Chapter 5: Required Settings for Spectralink IP-DECT Server

When you configure a Spectralink IP-DECT Server for Lync Server 2013 or 2010, you need to configure the following settings:

- The Spectralink Microsoft Lync Interop License needs to be installed on the Spectralink IP-DECT Server.
- Lync Server 2013 or 2010 support needs to be enabled.
- Trusted Server needs to be enabled (not if NTLM authentication is used).
- DNS Hostname needs to be entered.
- The Lync Server 2013 or 2010 domain needs to be configured.
- The Lync Server 2013 or 2010 Front End Pool(s) and SBA(s) needs to be configured.
- SRTP needs to be enabled (The Require Setting is optional and depends on your Lync setup).
- If NTLM is used, credentials have to be configured for each user.



Note

The Spectralink Microsoft Lync Interop License (part no. 14075270 or part no. 14075510) must be installed on the Spectralink IP-DECT Server 400 or 6500. The Lync Interop License includes the Spectralink Software Security Package (HTTPS, TLS, and SRTP), which is needed for the RTP encryption (SRTP) towards the Lync Server 2013 or 2010.

Chapter 6: Spectralink IP-DECT Server Configuration

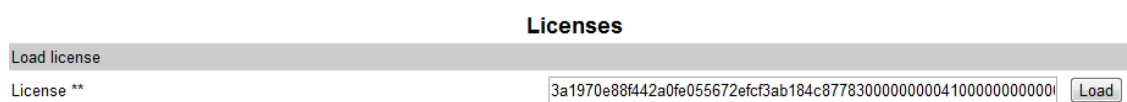
The following configuration settings must be entered in the Spectralink IP-DECT Server.

Log in to the system via your browser, and enter the IP address of the system as well as the User Name and Password (default: admin/ip6000). If the IP address of the system is not known, the server can be discovered via UpnP and the server will be discovered with the serial number (S/N) written on the label at the back of the server. Otherwise, if a handset is subscribed to the server you can use the command (**999*00 + Off Hook). This gives you the IP address of the system the handset is registered to.

Configuring the IP-DECT Server for MS Lync Server 2013 or 2010 Support

Add a Lync license to the Spectralink IP-DECT Server

- 1 Click **Administration** and then click **License**.
- 2 In the **License** field, enter the License code.



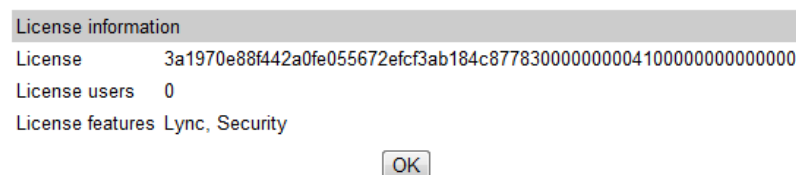
Licenses

Load license

License ** 3a1970e88f442a0fe055672efcf3ab184c8778300000000041000000000000 Load

License successfully loaded

Please reboot to activate the new license



License information

License 3a1970e88f442a0fe055672efcf3ab184c8778300000000041000000000000

License users 0

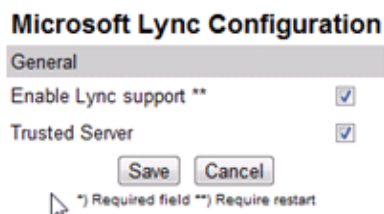
License features Lync, Security

OK

- 3 Click the **Load** button. The license is loaded and new window states that Lync license has been loaded.
- 4 Reboot the Spectralink IP-DECT Server when prompted

Enable Lync support

- 1 Click **Configuration** and then click **Lync**.
- 2 Select **Enable Lync support**.
- 3 Select **Trusted Server**.



Configure SIP Settings

- 1 Click **Configuration**, and then click **SIP**.
- 2 Set **Transport** to TLS.
- 3 Set **DNS method** to A records.
- 4 Set **Default domain** to the SIP domain name of the Lync Server 2013 or 2010. For example, Jim.kander@ewslynctest.com should be “ewslynctest.com” entered in default domain.



Note

SIP domain name refers to the Lync Server 2013 or 2010 - SIP domain name, not the AD domain name, if they are different.

- 5 Select **GRUU**.
- 6 Deselect **Use SIPs URI**.

SIP Configuration	
General	
Local port * **	5060
Transport * **	TLS
DNS method * **	A records
Default domain * **	ewslynctest.com
Register each endpoint on separate port **	<input type="checkbox"/>
Send all messages to current registrar **	<input type="checkbox"/>
Registration expire(sec) *	3600
Max forwards *	70
Client transaction timeout(msec) *	4000
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"/>

Proxies			
	Priority	Weight	URI
Proxy 1 **	1	100	sip.horlynctest02.ewsynctest.com
Proxy 2 **	2	100	
Proxy 3 **	3	100	
Proxy 4 **	4	100	

7 Set the proxies to the prioritized list of **FQDN(s) the Front End Pool(s) and the SBA.**



Note

If SBA is being used, use the SBA as primary proxy and front end as secondary proxy.

8 Select Ignore SDP version.

9 Select Enable RTP encryption.

10 Select Require RTP encryption. This setting is optional, depending on your Lync Server 2013 or 2010 setting.

11 Select Include lifetime in SDES offers.

12 Select Include MKI in SDES offers.

- SDP answer with preferred codec
- SDP answer with a single codec
- Ignore SDP version
- Enable media encryption (SRTP) **
- Require media encryption (SRTP)
- Include lifetime in SDES offers
- Include MKI in SDES offers



Note

When Require SRTP is set on the IP-DECT server, you must be sure that your LYNC setup support the feature on all attached devices, we have seen some Gateways that do not support "require SRTP" and therefore calls will fail, when routed to or from these gateways. if require is not set, the server will enable the feature if necessary and this will be mentioned in the logs of the IP-DECT server. SRTP require is default setting in LYNC environment.

CA Certificates

<input type="button" value="Clear List"/> <input type="button" value="Restore Default List"/> <input type="button" value="Browse..."/> <input type="button" value="Import List"/> <input type="button" value="Export List"/>		
Common Name	Organization	SHA1 fingerprint
EWSLYNCTEST-HORLYNCTEST01-CA	<Not Part Of Certificate>	24:3d:08:cf:20:22:56:8a:4c:89:f5:ec:3f:fd:b4:d4:dc:98:e7:ad

13 In the **Certificates Configuration tab** (Configuration -> Certificates), import the CA certificate exported above.



Note

Step 13 is not required if the certificate of the Lync Server 2013 or 2010 is signed by a public CA.

14 In the **Certificates Configuration** tab, import the Host Certificate exported above. Choose PKCS#12, enter the password, and then select **Import certificate**.

Host certificate chain

Certificate file: Der er ikke valgt nogen fil Key file: Der er ikke valgt nogen fil Password: Type: X.509 PKCS#12

Subject	Validity	SHA1 fingerprint	Issuer
IP-DECT6500.ewslynctest.com, Spectralink	29-10-2013 - 29-10-2015	a4:1e:43:19:3f:39:41:0b:25:99:b4:4f:a8:9b:6a:a2:7c:88:67:a4	EWSLYNCTEST-HORLYNCTEST01-CA

15 Enter the DNS **Hostname**. Use the DNS Hostname created above.

DNS	
Hostname **	<input type="text" value="IP-DECT6500.ewslynctest.com"/>
Domain **	<input type="text" value="ewslynctest.com"/>

DNS	
Hostname **	<input type="text" value="pmkws6000.ewslynctest.com"/>
Domain	<input type="text" value="ewslynctest.com"/>

Adding Users to Spectralink IP-DECT Server

The authentication method determines which information you need to enter when you add a user.

System Authentication (Trusted Server)

If System Authentication is used for authentication, the following information is required:

- Username/Extension field: SIP username (without domain)

The **Display name** and **Standby text** are optional, but recommended.

User

DECT	
IPEI	05003 0070387
Access code	
Standby text	Jim Kander
SIP	
Username / Extension *	jim.kander
Domain	
Displayname	Jim Kander
Authentication user	
Authentication password	
Disabled	<input type="checkbox"/>
Features	
Call forward unconditional	

*) Required field

User Authentication (NTLM)

If User Authentication is used for authentication, the following information is required:

- Username/Extension field: SIP username (without domain)
- Authentication Username: AD login name
- Authentication Password: AD login password

The authentication username must be the same username as specified in the Active Directory without the domain. The password must be the same password as specified in the Active Directory.

The **Display name** and **Standby text** are optional, but recommended.

Chapter 7: Known Limitations

Presence

The presence information changes when a Spectralink DECT user is in a call or in idle state.

By default the Spectralink DECT Handset is set to “Away” because the user is on a DECT phone and away from the Lync Client. The different presence settings for the Spectralink DECT Handsets are:

- **Available** - green icon (lasts for 5 minutes after a call has been completed)
- **Inactive** - yellow icon (is set automatically after 5 minutes of inactivity from “Available” state)
- **Away** - yellow icon (is set automatically after 5 minutes of inactivity from “Inactive” state)
- **In a Call** - red icon

The presence information option “Offline” is not available for Lync users that use a Spectralink DECT Handset.



Note

An initial log-in to a Lync client with each DECT user is required to activate the presence functionality of the handset. Alternatively you can use the Presence bootstrapping tool for Lync Server 2013 or 2010. For more information, see: <http://support.microsoft.com/kb/2737277>.

Characters in Spectralink DECT Handsets

The following describes the SIP limitations of the Spectralink DECT and how the Spectralink DECT Handsets handles them:

- **Incoming call number SIP-URI** - In SIP-URI the Spectralink DECT Handset can handle up to 64 characters in incoming calls and call logs. The “sip:” at the beginning of a possible SIP address is included in the 64 characters. A SIP URI of more than 64 characters is not saved in the handset call log. Only the call party name will be saved. However, it is not possible to redial this because the number is not present.
- **Call party name** - When the SIP URI is over 64 characters, the handset truncates the call party name to a maximum of 24 characters, and only the first 24 characters of the name are displayed.

Microsoft Lync 2013 or 2010 Attendant

During Beta test, a number of issues regarding blind transfer of external calls from the Lync Attendant were reported. This information is taken into consideration for future development.

Lync response groups and delegates

Spectralink DECT Handsets can receive calls to a response group and/or delegated persons, but due to limited display capacity the designated response group or delegated persons cannot be displayed. The call will be displayed as a normal call and only the caller will be identified.

When a DECT handset is a member of a response group, calls will NOT arrive at the DECT handset if the handset is idle for more than 10 minutes. This is due to the automatic presence status functionality built into the handset. After 5 minutes you change status to "Inactive". After another 5 minutes you change status to "Away". Users in response groups will not receive calls when their presence is set to Away. This is only if the users are not using the DECT handsets or if they are not using a Lync client, as the presence on the Lync client, overtakes the presence from the handset, when the client is online, until again the user is away from the Lync client, or changes presence manually on the Lync client. This information is taken into consideration for future development of the DECT Handset.

E911

This feature is not supported because in a campus environment the location cannot be determined exactly, since the Spectralink DECT Handset is a portable device.

Chapter 8: Third party endpoints

If you experience problems with interoperability with other Lync Certified endpoints, please contact Spectralink support at technicalsupport@spectralink.com.

Chapter 9: Presence Description

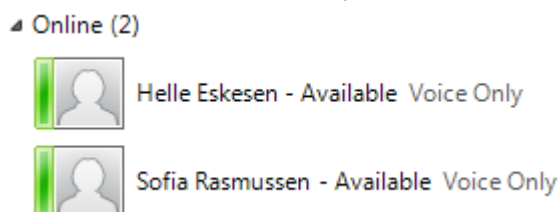
The following screenshots show how presence is indicated on a Lync Client, when a Spectralink DECT Handset is idle or in use.

Idle Spectralink DECT Handset

Spectralink Handset status:



Status in Microsoft Lync client:



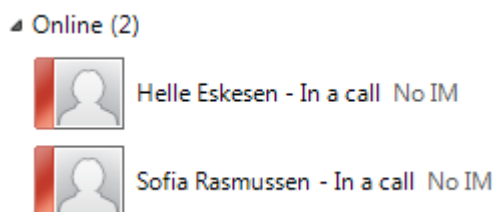
The users in this example only have a Spectralink DECT Handset and are not logged on with a Lync Client. That is why **Voice Only** is displayed.

Spectralink DECT Handset in conversation

Spectralink handset status (active call)



Status in Microsoft Lync client:



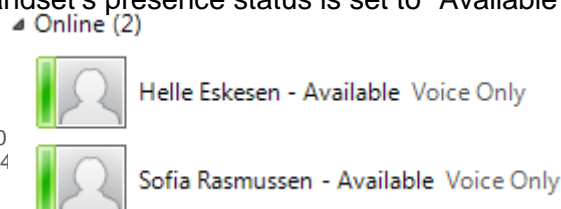
The users in the example only have a Spectralink DECT handset and are not logged on with a Lync client. Because the Spectralink DECT handset does not accept Instant Messages from the Lync client, **No IM** appears.

To activate the presence functionality of the handset, an initial log-in to a Lync client with each DECT user is required.

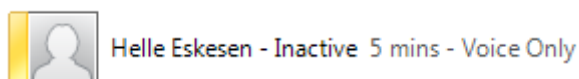
Alternatively, you can use the Presence bootstrapping tool for Lync Server 2010. For more information, see: <http://support.microsoft.com/kb/2737277>.

Overview of presence statuses in the Lync client

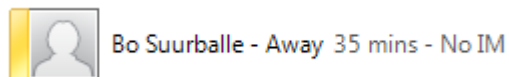
The handset's presence status is set to "Available" for 5 minutes after it has been used.



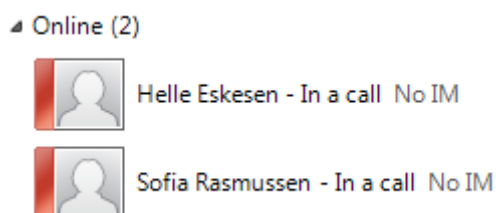
After 5 minutes, the handset status changes to “Inactive” if the handset is not used.



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



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



NTLM:

Windows Challenge/Response (NTLM) is the authentication protocol used on networks that include systems running the Windows operating system and on stand-alone systems. NTLM credentials are based on data obtained during the interactive logon process and consist of a domain name, a user name, and a one-way hash of the user's password. NTLM uses an encrypted challenge/response protocol to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials.

TLS/MTLS:

TLS and MTLS protocols provide encrypted communications and endpoint authentication on the Internet. Microsoft Lync Server 2010 uses these two protocols to create the network of trusted servers and to ensure that all communications over that network are encrypted. All SIP communications between servers occur over MTLS. SIP communications from client to server occur over TLS.

TLS enables users, through their client software, to authenticate the Lync Server 2010 servers to which they connect. On a TLS connection, the client requests a valid certificate from the server. To be valid, the certificate must have been issued by a CA that is also trusted by the client and the DNS name of the server must match the DNS name on the certificate. If the certificate is valid, the client uses the public key in the certificate to encrypt the symmetric encryption keys to be used for the communication, so only the original owner of the certificate can use its private key to decrypt the contents of the communication. The resulting connection is trusted and from that point is not challenged by other trusted servers or clients. Within this context, Secure Sockets Layer (SSL) as used with Web services can be associated as TLS-based.

Server-to-server connections rely on mutual TLS (MTLS) for mutual authentication. On an MTLS connection, the server originating a message and the server receiving it exchange certificates from a mutually trusted CA. The certificates prove the identity of each server to the other. In Lync Server 2010 deployments, certificates issued by the enterprise CA that are during their validity period and not revoked by the issuing CA are automatically considered valid by all internal clients and servers because all members of an Active Directory domain trust the Enterprise CA in that domain. In federated scenarios, the issuing CA must be trusted by both federated partners. Each partner can use a different CA, if desired, so long as that CA is also trusted by the other partner. This trust is most easily accomplished by the Edge Servers having the partner's root CA certificate in their trusted root CAs, or by use of a third-party CA that is trusted by both parties.

TLS and MTLS help prevent both eavesdropping and man-in-the middle attacks. In a man-in-the-middle attack, the attacker reroutes communications between two network entities through the attacker's computer without the knowledge of either party. TLS and Lync Server 2010 specification of trusted servers (only those specified in Topology Builder) mitigate the risk of a man-in-the middle attack partially on the application layer by using end-to-end encryption coordinated using the Public Key cryptography between the two endpoints, and an attacker would have to have a valid and trusted certificate with the corresponding private key and issued to the name of the service to which the client is communicating to decrypt the communication. Ultimately, however, you must follow best security practices with your networking infrastructure (in this case corporate DNS). Lync Server 2010 assumes that the DNS server is trusted in the same way that domain controllers and global catalogs are trusted, but DNS does provide a level of safeguard against DNS hijack attacks by preventing an attacker's server from responding successfully to a request to the spoofed name.

(Source: <http://technet.microsoft.com/en-us/library/gg195752.aspx>)

Specifications subject to change without notice.

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

Spectralink Europe ApS
Langmarksvej 34
DK-8700 Horsens

www.spectralink.com