Using a Polycom® KIRK® Wireless Server 6000 Solution in a Microsoft® Lync™ Server 2010 Setup

Configuration Guide

Version 9.0 | May 2012 | 14207900

Table of Contents

Introduction

This configuration guide describes how to setup a KIRK Wireless Server 6000 in a Microsoft® Lync™ Server 2010 installation.

Overview

The configuration guide includes the following information:

- Transport Protocol
- Supported Features
- SIP User Authentication
- Settings required for Lync Server 2010
- Settings required for KIRK Wireless Server 6000
- Adding users to the KIRK Wireless Server 6000

Firmware Compatibility

The KIRK Wireless Server 6000 interoperates with Lync Server 2010 from firmware version PCS12_. The KIRK Microsoft Lync Interoperability is backward compatible with Microsoft® Office Communications Server 2007 R2.

The communication protocol between KIRK Wireless Server 6000, KIRK Media Resources, and KIRK IP Base Stations is not backward compatible. This means that KIRK Media Resources with firmware versions older than PCS08B_ and KIRK IP Base Stations with firmware versions older than PCS08__will not be able to connect to a KIRK Wireless Server running firmware PCS08B_ or newer.

To minimize downtime, you need to update KIRK Media Resources and KIRK Wireless Server 6000 to firmware PCS012_or newer and KIRK IP Base Stations to firmware PCS12A_or newer before rebooting any of these.

Transport Protocol

To interoperate with the Lync Server 2010, the KIRK Wireless Server 6000 supports TLS as transport protocol for SIP signaling. This requires a Certificate Authority (CA) on the KIRK Wireless Server 6000.

The KIRK Wireless Server 6000 is delivered with a Certificate Authority bundle with common Certificate Authorities. This means that the KIRK Wireless Server 6000 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.

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, G.726, and G.729AB (codec module required)
- 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 ™ 2010 client the presence status of each subscribed KIRK 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.

SIP User 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 KIRK Wireless Server 6000. 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

You enter the credentials for each SIP user into the KIRK Wireless Server 6000 either by using the web GUI or provisioning. It is not possible to change the Authentication Username or Password directly from the KIRK DECT Handsets. It can only be changed via the KIRK Wireless Server 6000.

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 2010 environment:

- Access to Microsoft Lync Server 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

KIRK Wireless server 6000:

- Admin access to the KIRK Wireless Server
- KIRK Microsoft Lync Interop License (part no. 14075270)
- External Syslog Server (recommended)

Note: To troubleshoot the system integration properly and to obtain errors from the KIRK Wireless Server 6000, it is recommended that you use a Syslog Server to ensure that no critical errors from the KIRK Wireless Server 6000 are left unresolved. You specify the Syslog settings in the KIRK Wireless Server under General configuration -> Remote syslog. As a minimum, choose **Error** or **Warning** setting.

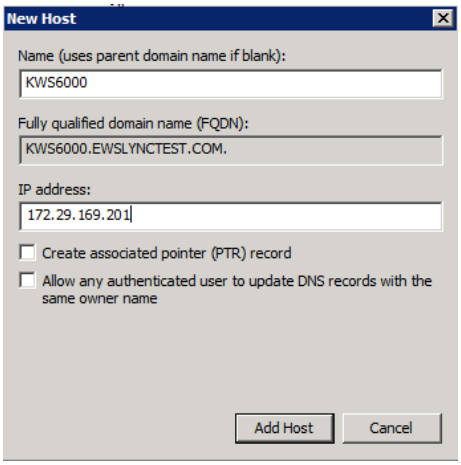
Settings Overview for Lync Server 2010

- DNS entry for KIRK Wireless Server 6000
- CA certificate from Domain
- Host certificate for Trusted Server
- Adding the KIRK Server as Trusted application server

Configuring the Microsoft Lync Server 2010 Setup

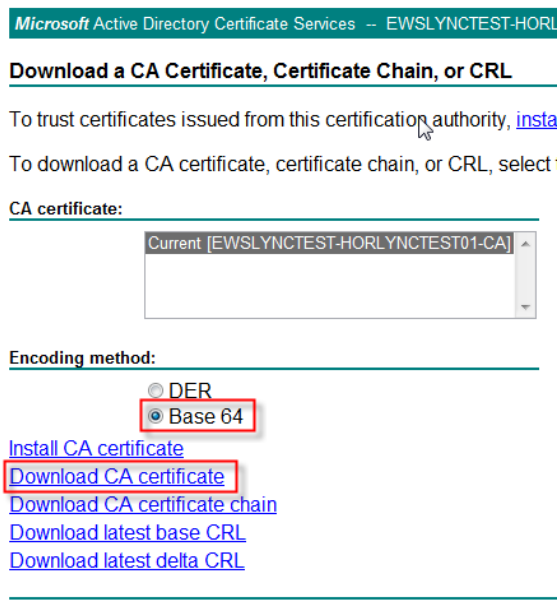
Step 1: Create a DNS Entry on the DNS Server

1. Create a hostname for the KIRK Wireless Server 6000 and Domain DNS Server.
2. Add the KIRK Wireless Server 6000 as New Host. The FQDN name will be used later in the configuration later. See page 7.
3. Click the **Add Host** button.

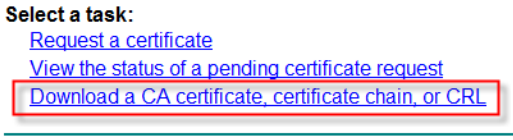


Step 2: Download a CA Certificate

1. Open Microsoft **Certificate Authority** directly in your web browser. <IP address>/certsrv.
2. Select **Download a CA certificate.**
3. Select the current CA certificate.
4. Set the encoding method to **Base-64** (.CER)



5. Select **Download CA Certificate**



6. The Certificate is downloaded to your browser and will be used later in the configuration of the KIRK Wireless Server 6000. See page below12

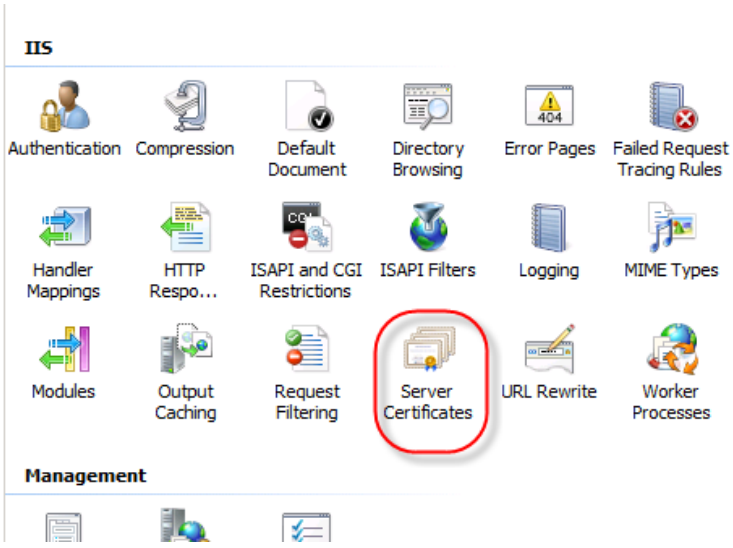
Note: Step 2 is not required if the Lync Server 2010 certificate is signed by a public CA. This guide describes how to export the CA certificate from a Microsoft Certificated Authority. If a different CA authority technology is deployed, please refer to the vendor documentation.

Step 3: Create a Host Certificate for Trusted Server

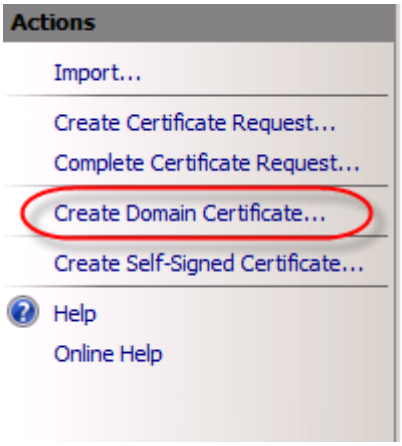
This action is performed on Internet Information Server (IIS) Cert SRV.

To request a security certificate for the Polycom KIRK Wireless Server 6000 using IIS Manager 7, do the following.

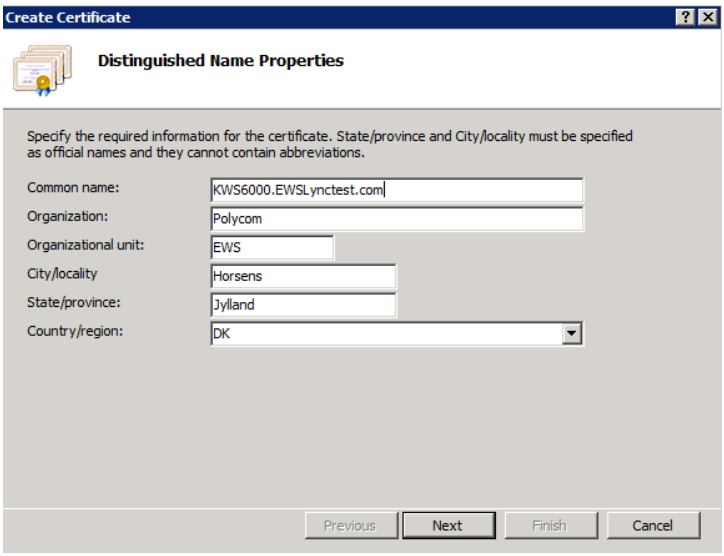
1. On the Lync Server, select **Start** > **All Programs** > **Administrative Tools** > **Internet Information Services (IIS) Manager** (7.0) to open IIS 7.
2. Under **Connections**, double-click the server name.
3. In the **Features View**, double-click **Server Certificates under IIS**.



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 DNS FQDN of the KIRK Wireless Server 6000, 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 **file export path**, and set a password for the certificate. The password is used when importing on KIRK Wireless Server 6000. See page 12.

Step 4: Add a KIRK Server as Trusted Application Server

Open Lync Management Shell and enter the 3 commands below. The text marked as bold should be replaced with your Lync Server 2010 configuration names. If any database errors are displayed when you enter the information, run the **LYNC Server Management Shell** as Administrator.

1. `New-CsTrustedApplicationPool -Identity` **`<FQDN of KWS6000>`** `-Site` **`<SiteID>`** `-RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true -Registrar` **`<FQDN of Lync frontend pool>`**

Note: After completing this step a warning is displayed. Confirm with Y – Yes.

2. `New-CsTrustedApplication -ApplicationId dect -Port 5061 -TrustedApplicationPoolFqdn` **`<FQDN of KWS6000>`**
3. `Enable-CsTopology`

The following 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` **`kws6000.ewslynctest.com`** `-Site 1 -RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated $true -Registrar` **`ewslynctest.com`**
2. `New-CsTrustedApplication -ApplicationId dect -Port 5061 -TrustedApplicationPoolFqdn` **`kws6000.ewslynctest.com`**
3. `Enable-CsTopology`

Settings Required for KIRK Wireless Server 6000

When you configure a KIRK Wireless Server 6000 for Lync Server 2010, you need to configure the following settings:

- The KIRK Microsoft Lync Interop License needs to be installed on the KIRK Wireless Server 6000.
- Lync Server 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 2010 domain needs to be configured.
- The Lync Server 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 KIRK Microsoft Lync Interop License (part no. 14075270) must be installed on the KIRK Wireless Server 6000. The Lync Interop License includes the KIRK Software Security Package (HTTPS, TLS, and SRTP), which is needed for the RTP encryption (SRTP) towards the Lync Server 2010.

KIRK Wireless Server 6000 Settings Summary

The following server settings are specifically relevant in a Lync Server 2010 setup:

Configuration key	Description	Lync Setting
sip.lync.enable	Enables Lync Server 2010 support Values: true, false. Default: false	True
sip.lync.trusted	Enables Trusted Server support Values: true, false. Default: false	True (recommended)
sip.media.sdp_ignore_version	Specifies whether to ignore the version information in incoming SDP received from remote endpoints. Values: true/false. Default: false.	True
sip.transport	Specifies the transport mechanism used for SIP requests. Values: UDP, TCP, TLS. Default: UDP.	TLS
sip.dnsmethod	Specifies the dns method used for SIP requests. Values: arecord, dnssrv. Default: arecord.	Arecord (A Record)
sip.gruu	Specifies the use of Globally Routable UA URI (GRUU) which is an URI which routes to a specific UA instance. If enabled a GRUU will be obtained from a server and communicated to a peer within a SIP dialog. Values: true/false	True

	Default: true.	
sip.use_sips_uri	Normally SIP communication on a TLS connection uses the SIPS: URI scheme. Disabling this option causes the KIRK Wireless Server 6000 to use the SIP: URI scheme with a transport=tls parameter for TLS connections. Values: true/false Default: true.	False
sip.default_domain	The SIP domain of the Lync Server 2010.	
sip.proxy.domain **sip.proxy.domain[2-4]**	The FQDN of the Lync Front End Pool(s) and SBA(s).	
sip.media.srtp.enable	Enables SRTP between the KIRK Wireless Server 6000 and other endpoints. Not encrypted RTP is still allowed. Values: true, false. Default: false	True
sip.media.srtp.lifetime	Controls if SRTP lifetime key parameter is included in SDP security descriptors. Values: true, false. Default: false	True
sip.media.srtp.mki	Controls if SRTP MKI key parameter is included in SDP security descriptors. Values: true, false. Default: false	True
sip.media.srtp.required	Controls if SRTP is required for calls. If enabled calls will fail if the other end does not support SRTP. Values: true, false. Default: false.	True

KIRK Wireless Server 6000 Configuration

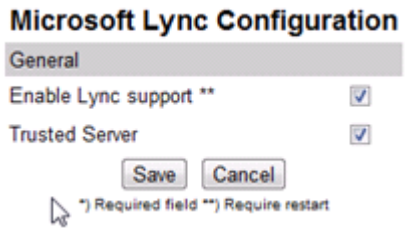
The following configuration settings must be entered in the KIRK Wireless Server 6000.

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.

Step 1: Configuring KIRK Wireless Server 6000 for Lync Server 2010 Support

In the Lync Configuration menu:

1. Select **Enable Lync support**.
2. Select **Trusted Server**.



Step 2: Configure SIP Settings for Lync Server 2010

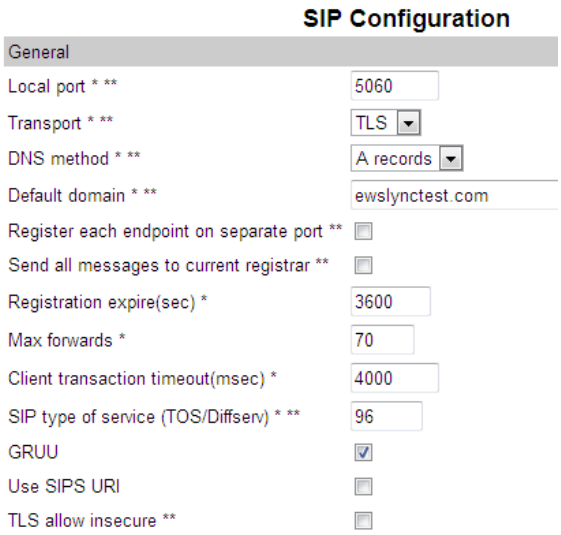
In the SIP Configuration menu:

1. Set **Transport** to TLS.
2. Set **DNS method** to A records.
3. Set **Default domain** to the SIP domain name of the Lync Server 2010.

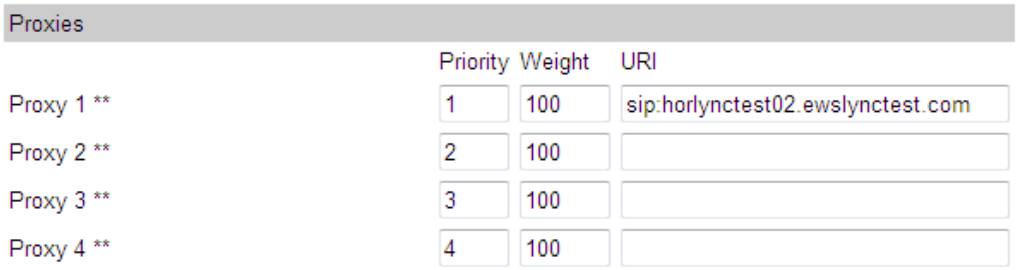
   For example, Jim.kander@ewslynctest.com should be “ewslynctest.com” entered in default domain.

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

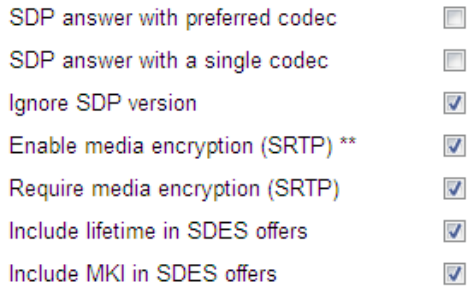
4. Select **GRUU**.
5. Deselect **Use SIPS URI**.



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



7. Select **Ignore SDP version**.
8. Select **Enable RTP encryption**.
9. Select **Require RTP encryption**. This setting is optional, depending on your Lync Server 2010 setting.
10. Select **Include lifetime in SDES offers**.
11. Select **Include MKI in SDES offers**.

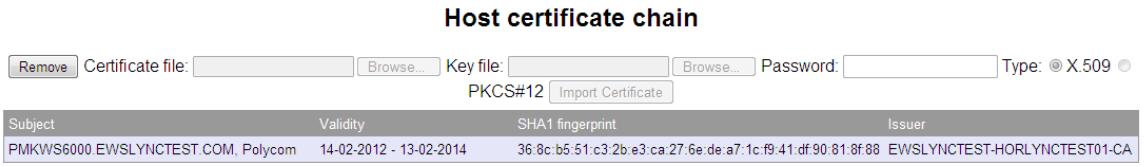


Note: When SRTP is enabled between the KIRK Wireless Server 6000 and the Lync Server 2010, the number of voice channels will be reduced from 32 to 16 voice channels (with G.729 codec card from 24 to 16 channels). For maximum security, it is possible to enable SRTP between the KIRK Wireless Server 6000 and the KIRK IP Base Stations. Please note that this will reduce the number of voice channels on each of the KIRK IP Base Stations from 11 to 6.

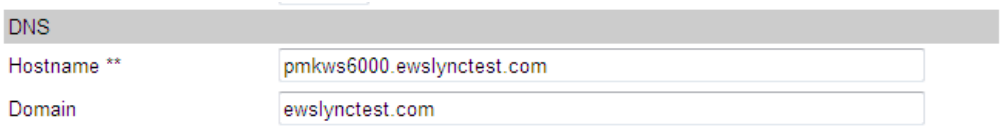
12. In the **Certificates Configuration tab**, import the CA certificate exported above.

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

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



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



Adding Users to KIRK Wireless Server 6000

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.

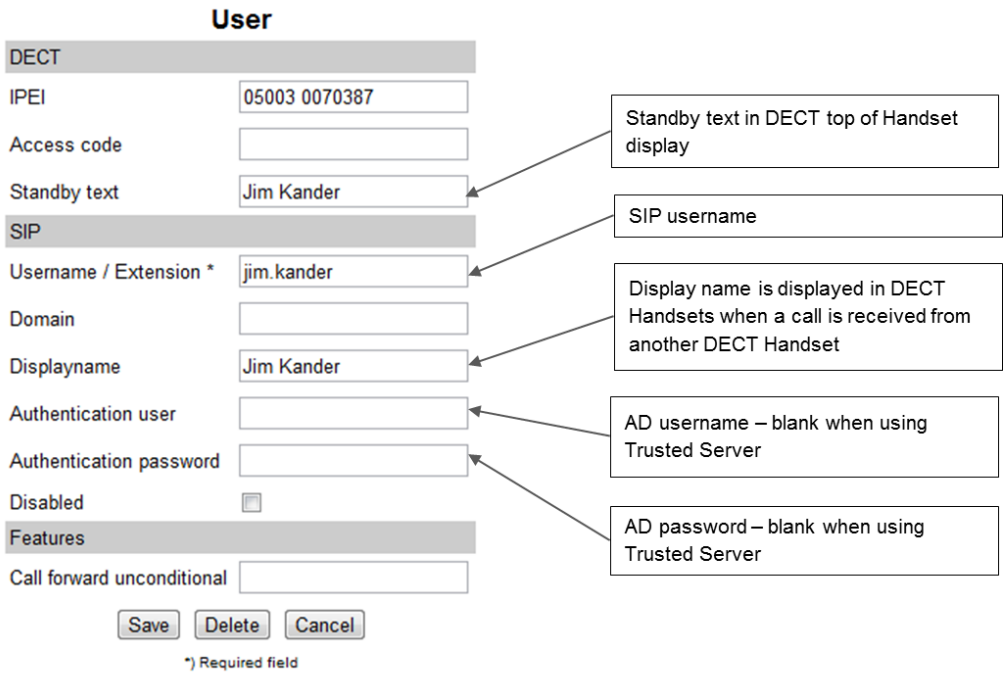
User Authentication (NTLM)

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.



Known Issues

The following issues have been identified on software version PCS 12A.

- **RFC3489-Biz02**: System administrators can enable support for this protocol by using a special command. This command enables the support for RFC3489 on the KIRK Wireless Server 6000. The default setting is False (not supported). The following line enables the feature: **(http://<host>/config/set?sip.media.rfc3489=true)**
- **Third party endpoints:** If you experience problems with interoperability with other Lync Certified endpoints, please contact Polycom support at the following email address: emeadksupport@polycom.com

Known Limitations

Call forward

When you enable Call forward (CFU) on Lync Server 2010, the KIRK DECT Handsets have the following limitations:

- When you enable CFU on a Lync device, you can normally disable the feature on other Lync enabled devices. This is not possible with the KIRK DECT Handsets.
- When you enable CFU ***21*$#** on a KIRK DECT Handset, you have to use the same handset when you want to disable the feature. You cannot disable the CFU feature from other Lync enabled devices. ($ should be replaced by the number)
- When you enable CFU on other Lync devices, you cannot disable CFU from a KIRK DECT Handset.

Presence

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

By default the KIRK 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 KIRK 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 KIRK DECT Handset.

Characters in KIRK DECT Handsets

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

- **Incoming call number SIP-URI** - In SIP-URI the KIRK DECT Handset can handle up to 36 characters in incoming calls and call logs. The “**sip:**” at the beginning of a possible SIP address is included in the 36 characters. A number above 36 characters will not be saved in the handset call log. Only the call party name will be saved. However, it is not possible to redial this call because the number is not present.
- **Call party name** - The handset will truncate the call party name to a maximum of 24 characters and only the first 24 characters of the name will be shown.

Microsoft Lync 2010 Attendant

Beta testers mentioned in the reports and test setup a number of issues they encountered regarding blind transfer of external calls from the Lync Attendant. This information is taken into consideration, but since the Microsoft Lync 2010 Attendant is a discontinued application this issue will not be fixed.

Lync response groups and delegates

KIRK 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.

E911

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

Invite to an ad-hoc conference call (App invite)

When a conference call is initiated from Lync, an invitation is sent to all devices of the invitees to allow both Video and Audio participation. The KIRK Wireless Server 6000 only makes an audio response in order to receive this type of call. If the user has a Lync video enabled device in addition to a KIRK DECT Handset, the conference will only be received by the video enabled device.

Appendix:

Presence description:

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

IDLE KIRK DECT Handset

KIRK Handset status:

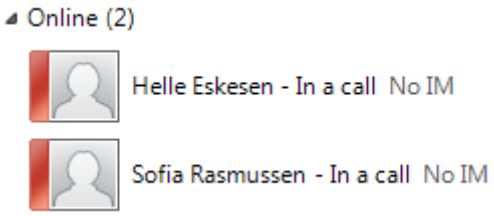
Status in Microsoft Lync client:

Note: these users only have a KIRK DECT Handset and are not logged on with a Lync Client. This is why “Voice only” appears.

KIRK DECT Handset in conversation

Kirk handset status (active call)

Status in Microsoft Lync client:

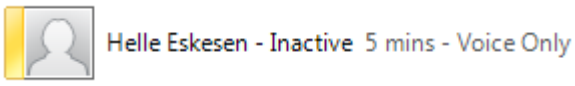


Note: these users only have a KIRK DECT Handset and are not logged on with a Lync Client. “No IM” appears as the KIRK DECT Handsets do not accept Instant Messages from the Lync Client.

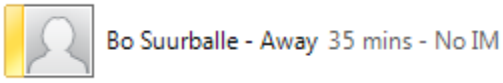
Overview of presence statuses in the Lync client

The handset’s presence status is set to “Available” for 5 minutes after it has been used.

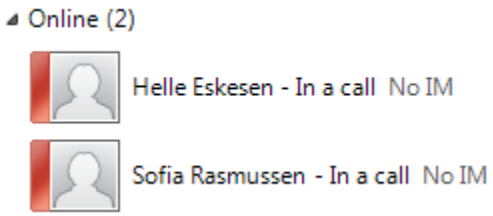
After 5 minutes, the handset status changes to “Inactive” if the handset is not used.



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



When a KIRK 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)

CAC (Call Admission Control) Administrators have the option to set limits the amount of Lync Server 2010 voice and video traffic carried on constrained network links, and specify the action taken if an offered session exceeds the limit. The action may include routing the session via an alternate path or refusing the session. Separate routes for voice and video allow administrators to prioritize these media types differently and specify preferred and alternate routes for various media types. Lync Server 2010 Call Admission Control is network-agnostic and does not require any vendor-specific networking equipment or setup.

(Source: http://technet.microsoft.com/en-us/library/gg398529.aspx)