

Implementation notes on Integration of Avaya Aura® Application Enablement Services with Microsoft® Lync® 2010 Server.

Introduction

The Avaya Aura ® Application Enablement Services Integration for Microsoft® Lync® 2010 Server is an application that provides click-to-call, and telephony presence. It enables users to operate more efficiently by launching phone calls from the Microsoft Lync client. As a result, people, teams, and organizations are able to communicate simply and effectively while working with Avaya and Microsoft applications. The AE Services Integration for Microsoft Lync is for customers who want a click-to-call solution that takes advantage of their existing Avaya Aura ® Communication Manager.

These implementation notes are intended for those responsible for architecting, designing, and/or deploying the Avaya Aura ® Application Enablement Services (AE Services) Integration for Microsoft Lync Server. Considerations and recommendations for deploying AE Services with a Microsoft Lync Standard Server environment will be outlined.

For more detailed information regarding Application Enablement Services integration with Microsoft Lync, it is strongly recommended that the following documents be reviewed:

Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007

Avaya Aura™ Application Enablement Services Administration and Maintenance Guide

These documents can be downloaded from <http://support.avaya.com>

Documentation for Microsoft Lync 2010 Server:

The following list is not the complete list of Microsoft Lync 2010 documents, but it includes documents that are strongly recommended for integrating AE Services with Microsoft Lync Server. The documents *Deploying Remote Call Control* and *Microsoft Lync Server 2010 (Release Candidate) Lab Deployment Guide* are particularly useful for integrating AE Services in a Microsoft Lync Server environment.

Planning for Microsoft Lync Server 2010

Preparing Active Directory Domain Services for Lync Server 2010

Microsoft Lync Server 2010 Active Directory Guide

Deploying Lync Server 2010 Standard Edition

Deploying Lync Server 2010 Enterprise Edition

Deploying Edge Servers

Deploying Remote Call Control

Microsoft Lync Server 2010 (Release Candidate) Lab Deployment Guide

Microsoft Lync Server 2010 Client and Device Deployment Guide

Microsoft Lync Server 2010 Active Directory Guide

Microsoft Lync Server 2010 Capacity Calculator

These documents can be downloaded from the Microsoft Download Center at the following Web address: <http://www.microsoft.com/downloads>

Document scope

This document will strictly focus on configuration tasks necessary to integrate AE Services into an existing Microsoft Lync Infrastructure. This document is not intended to be a comprehensive configuration guide and focuses only on the steps required to integrate AE Services with the Microsoft Lync Server. Most other related subjects not covered by these notes can be found in *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007* or the documents listed above. Keep in mind these notes are general guidelines, in many cases deviation may be required to maintain a functional environment. To be successful in these tasks you should have a good understanding of Avaya AE Services and Microsoft Lync Server environments.

Features of the AE Services implementation for Microsoft Lync Server

With the AE Services and Microsoft Lync Server integration you have the simplicity and convenience of instant messaging (IM) combined with the power of the enterprise telephone network. The following features provide you with a rich set of communications capabilities:

Easily locate and contact people using corporate directories, Microsoft Outlook contacts, or your buddy list

Click-to-call - With click-to-call you can communicate seamlessly with others in different locations or time zones, using voice or instant messaging.

You can easily escalate an instant message to a call.

Your presence is shared.

Your phone and Microsoft Lync stay synchronized together.

You have access to call control features such as Hold, Transfer, Call forwarding, and so on.

View rich information about your contacts' availability - details about their schedule, or even their 'out of office' message - through integration with Microsoft Office Outlook and Microsoft Exchange Server.

You can perform nearly all the same operations with Microsoft Lync that you could with OCS 2007 R2, however the interface has changed. More details on this will be provided in a future document release.

A Brief Summary of Microsoft Lync

The Microsoft Lync Client

The Lync client provides users with access to the features and capabilities of the Microsoft Lync environment. AE Services supports the current Microsoft Lync Client.

Microsoft Lync Standard or Enterprise Server

Microsoft Lync 2010 is Microsoft's next generation feature rich Unified Communication Server. Microsoft Lync 2010, like Microsoft Live Communications Server 2005 and Microsoft Office Communications Server 2007, enable instant messaging (IM), live collaboration, SIP telephony, and integration with telephony systems. Lync provides an enhanced topology builder feature, a central management store and many other changes, features and improvements over previous communications server offerings. Microsoft Lync 2010 is offered in a standard and an enterprise edition that both run only on 64 bit Windows 2008 R2 Server.

Architectural Summary

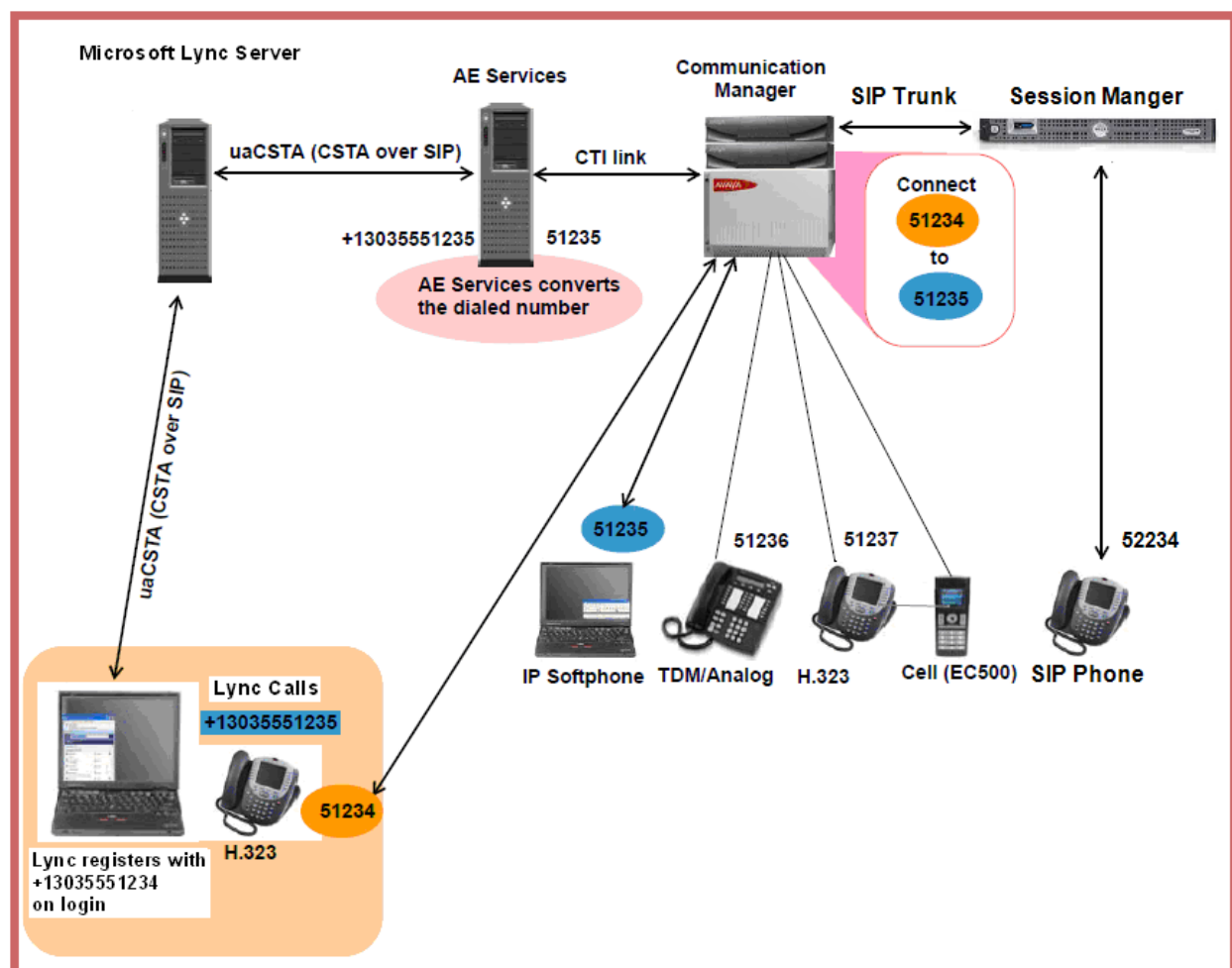
The AE Services Integration with Microsoft Lync makes use of AE Services DMCC over TR/87 Application support. TR/87 refers to the ECMA Technical Report, ECMA TR/87, which describes how Computer Supported Telecommunications Applications (CSTA) can be used to provide CSTA call control functionality for SIP user agents. TR/87 is the means by which AE Services Communicates with the Microsoft Lync Server for 3rd Party Call Control of Communication Manager PBX Stations. AE Services Acts as a SIP to CSTA III Gateway. AE Services exchanges control and status messages with Avaya Aura® Communication Manager over a Telephony Server Application Programming Interface (TSAPI) Link.

Making a simple phone call

The following figure illustrates a simple call path (using MakeCall) from Lync to an H.323 endpoint. While Lync is shown in this diagram as controlling an H.323 telephone, it is also capable of controlling IP Softphone, a digital phone or an analog phone. Lync can also control Specific Avaya SIP endpoints. For more information see page 21 of Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007 Release 6.1, February 2011 Issue 1

Note:

Analog phones require special usage instructions; see Usage instructions for analog phones on page 106 of *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007*



Integrating Avaya Aura™ Application Enablement Services with Microsoft Lync Server

The following steps should be completed prior to configuring certificates and other tasks directly related to integrating AE Services with Microsoft Lync Server. For more details on completing these prerequisite tasks refer to *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007*

- Administer a switch connection from AE Services to Communication Manager.
- Check the status of the switch connection (from AE Services to Communication Manager).
- Administer a TSAPI Link.
- Enable the TR/87 Port in the AE Services Management Console.
- Administer the Dial Plan

Installing the trusted certificate on Microsoft Lync Server

The Document “*Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007*” provides a detailed discussion on Certificates and Trust Management. Review this document for more background information on implementing certificates with AE Services and Microsoft Servers.

If you have not already installed certificates on the Microsoft Lync 2010 Server as part of the Microsoft Lync deployment you can use the following procedure to create a custom template that includes the attributes required by AE Services and then specify this template during the Certificate Assignment phase of the Lync Server deployment.

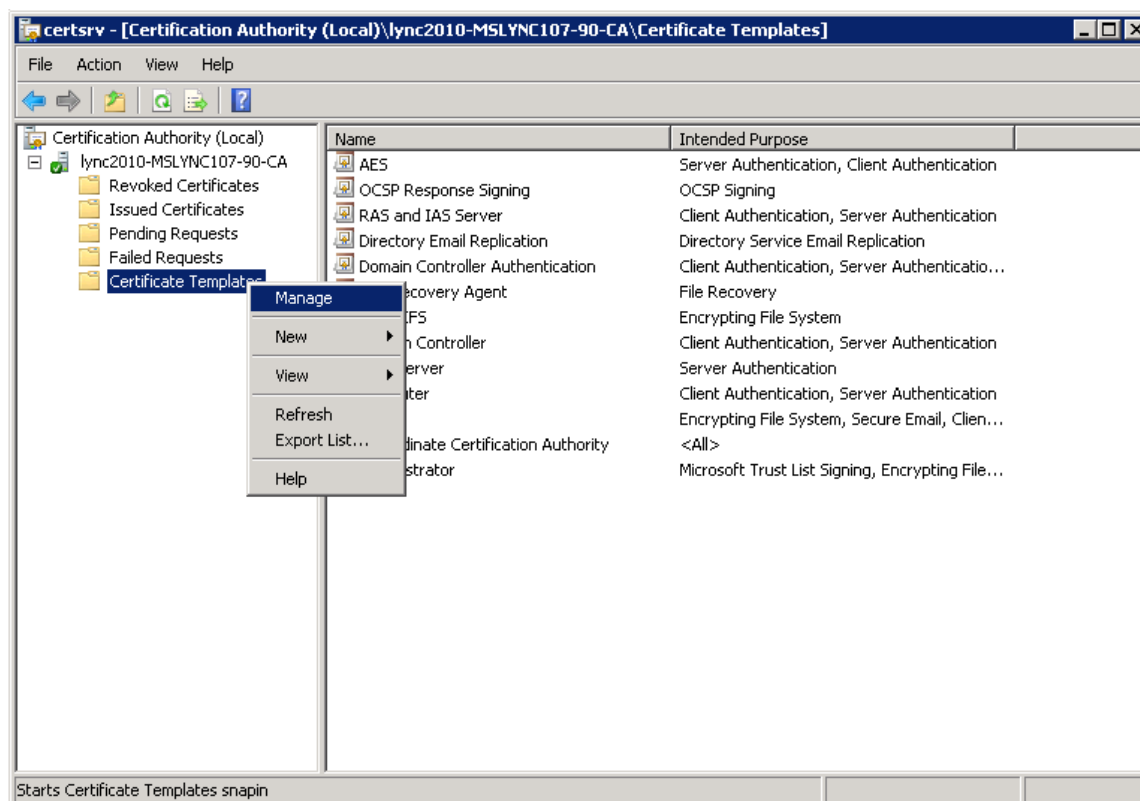
If the Microsoft Lync Server deployment has been previously completed, use this procedure to re-run Step 3 of the Microsoft Lync 2010 Deployment Wizard so the Lync Server will have a certificate that includes the Application Policies required by AE Services. Care must be taken to insure the template used and the issuing server satisfies all trust management needs of the Microsoft Lync Environment.

When installing the trusted certificate, note that Microsoft Lync Server and AE Services must use either the same CA or an issuer in the same certificate chain.

Creating a custom Certificate Template

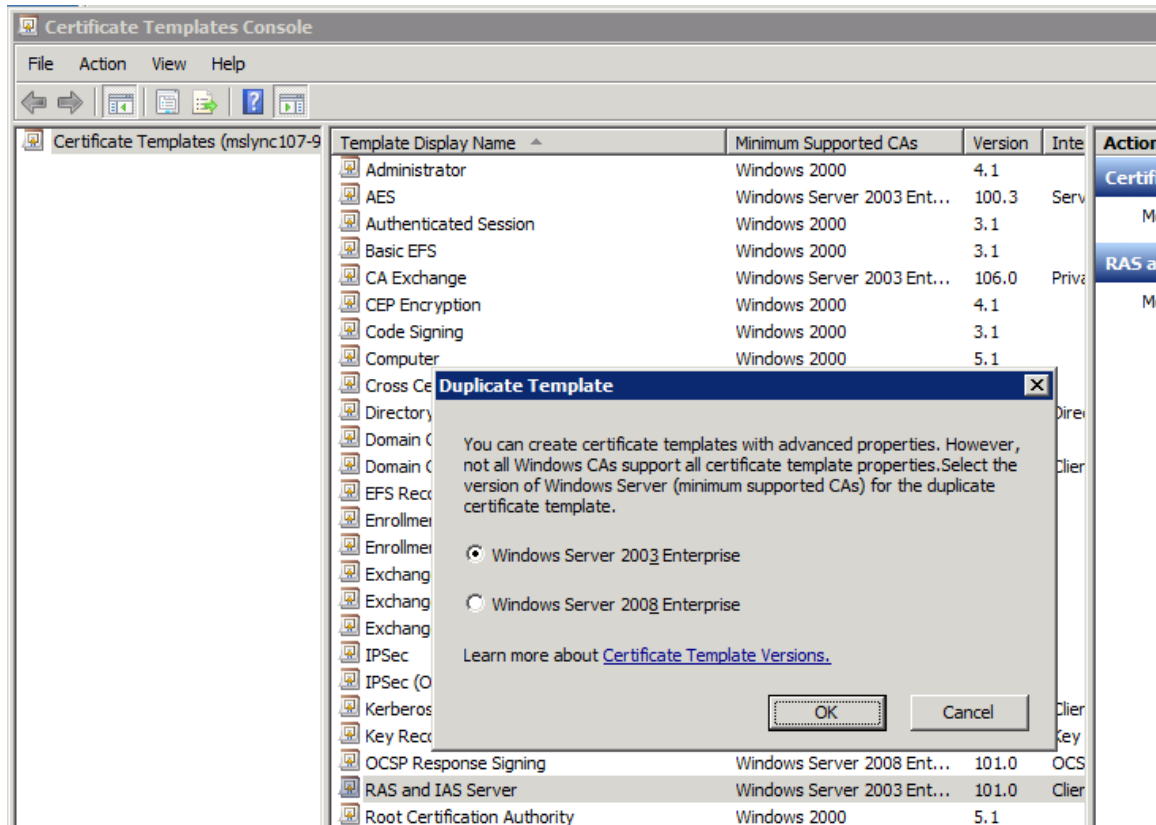
This procedure assumes the use of a Microsoft 2008 Certificate Authority (CA) Server. If you are using another vendors CA, use this as a general guide and consult the documentation for the CA Server.

Access the Windows 2008 CA Server Console, run the CA MMC snap-in or access **Start > Administrative Tools > Certificate Authority**. Expand the CA Server in the left pain, and then right click on the **Certificate Templates** folder in the left pain. Select **Manage**.

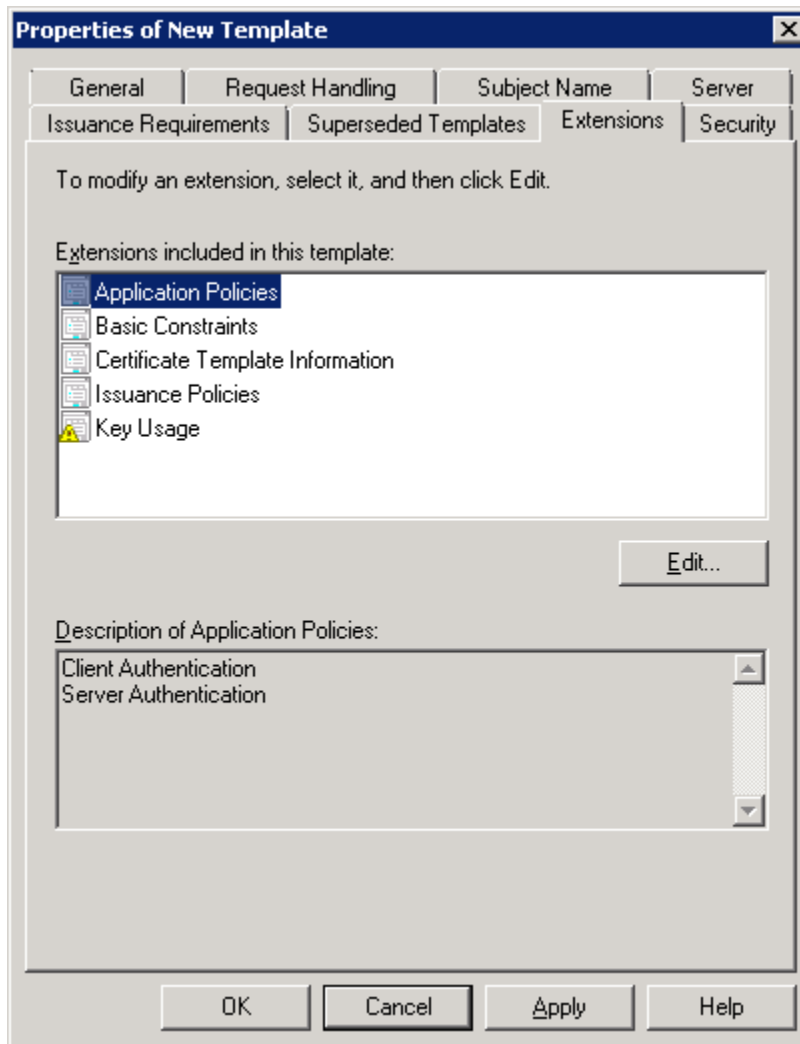


Right click **RAS and IAS Server**, then in the popup window select **duplicate template**.

Note: RAS and IAS template was chosen for this example because it includes Client and Server Authentication Application Policies required by Avaya AE Services. You should select a template that meets the needs of your environment which also satisfies Avaya AE Services requirements. For more information on certificates refer to the Microsoft and Avaya Documentation on pages 1 and 2 of this guide.



The screen shot below shows the Extensions tab when this template is duplicated. On the General tab, give the template a unique name like “**AES**” and then select **Apply** and **Okay**.



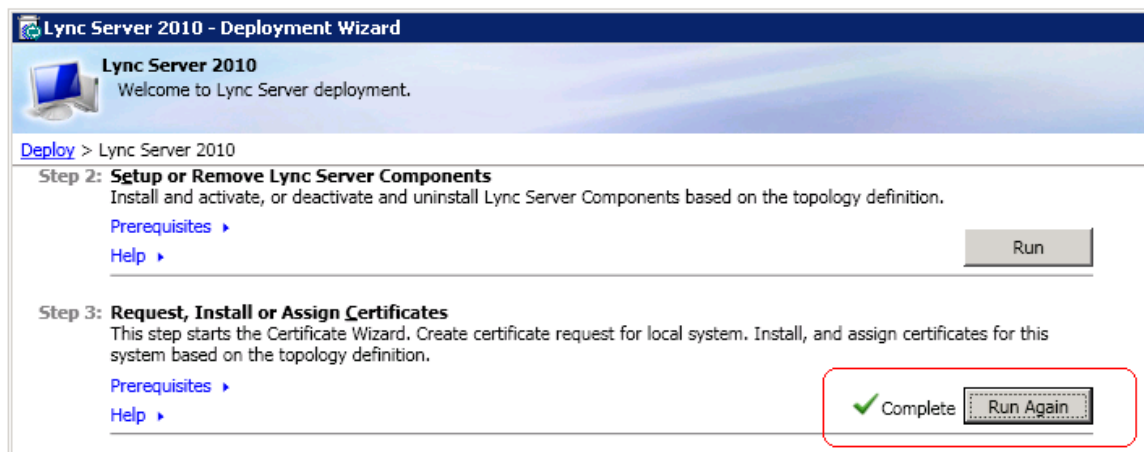
This procedure successfully creates a template that can be used when assigning certificates to the Microsoft Lync Server. It contains the Client and Server Authentication Policies required by AE Services.

Installing or re-installing certificates on the Microsoft Lync Server

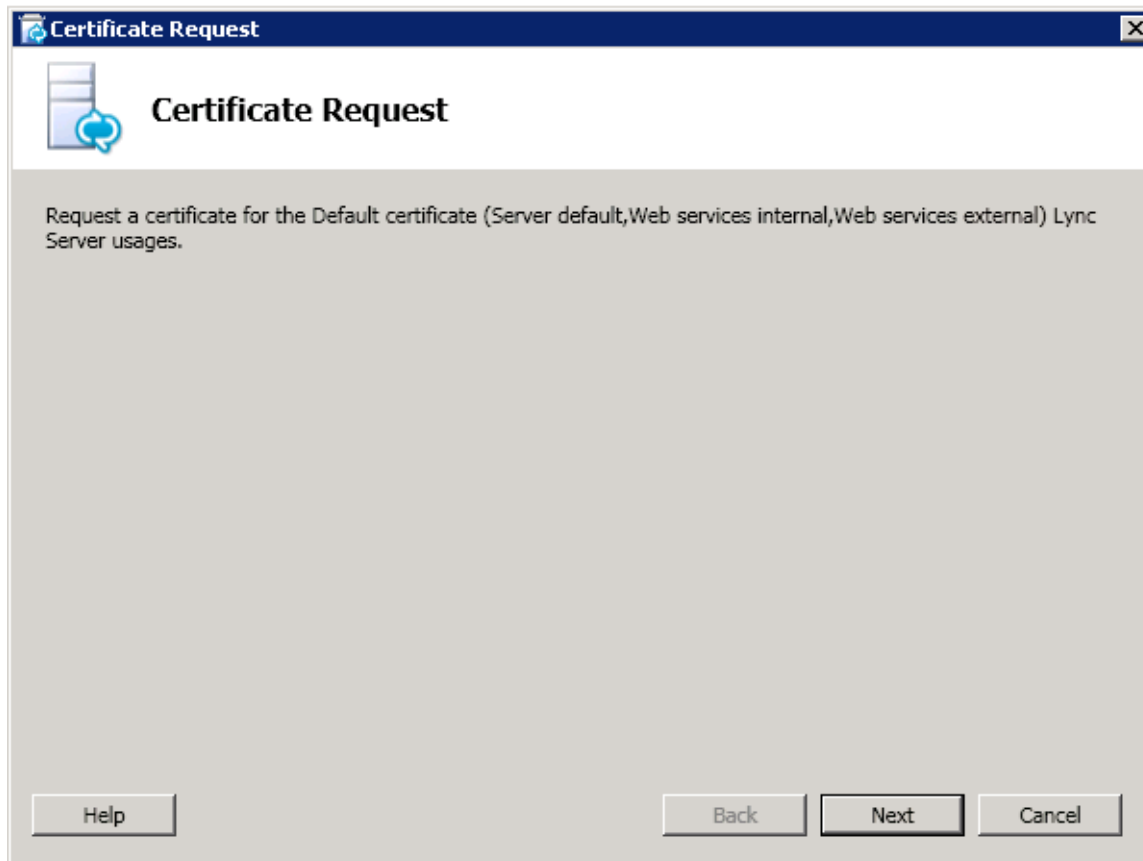
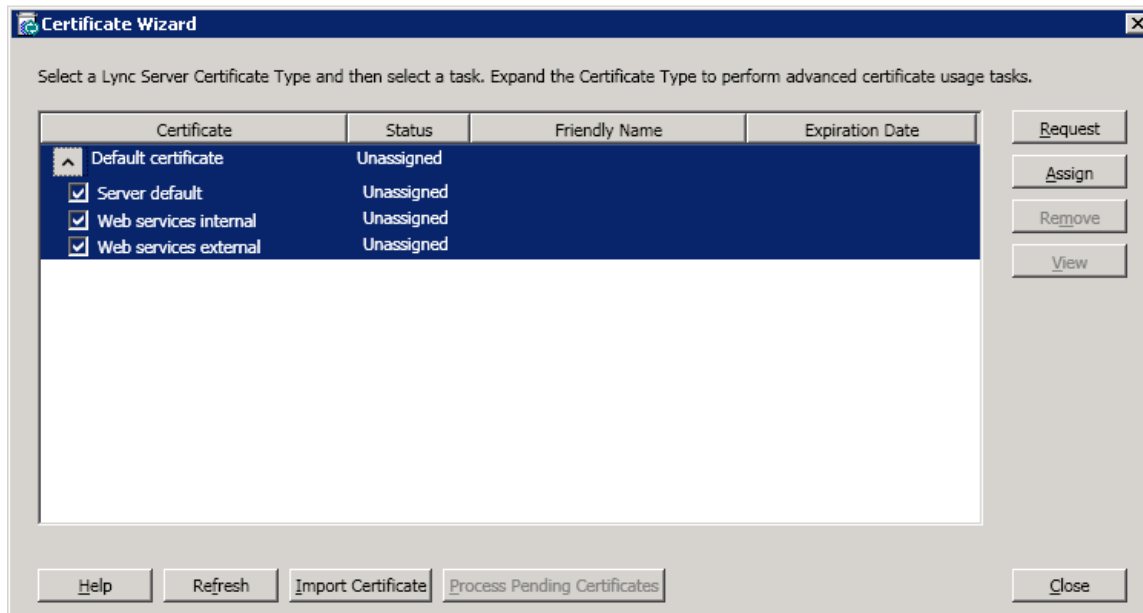
Step 3 of the Lync Server Deployment Wizard requests installs and assigns certificates required by the Microsoft Lync Server. For integration with AE Services you will need to specify the template you created in the previous step which contains the client and server authentication application policy required by AE Services. During this process the Certificate Wizard allows for specifying the template you created.

If you have not already done so start the Lync Server Deployment Wizard. From the start menu, open the Lync Server Deployment Wizard. From the Lync Server system Console, select *Start > All Programs > Microsoft Lync Server 2010 > Lync Server Deployment Wizard*. Select “*Install or Update Lync Server System*”. The Lync Server Deployment Wizard launches.

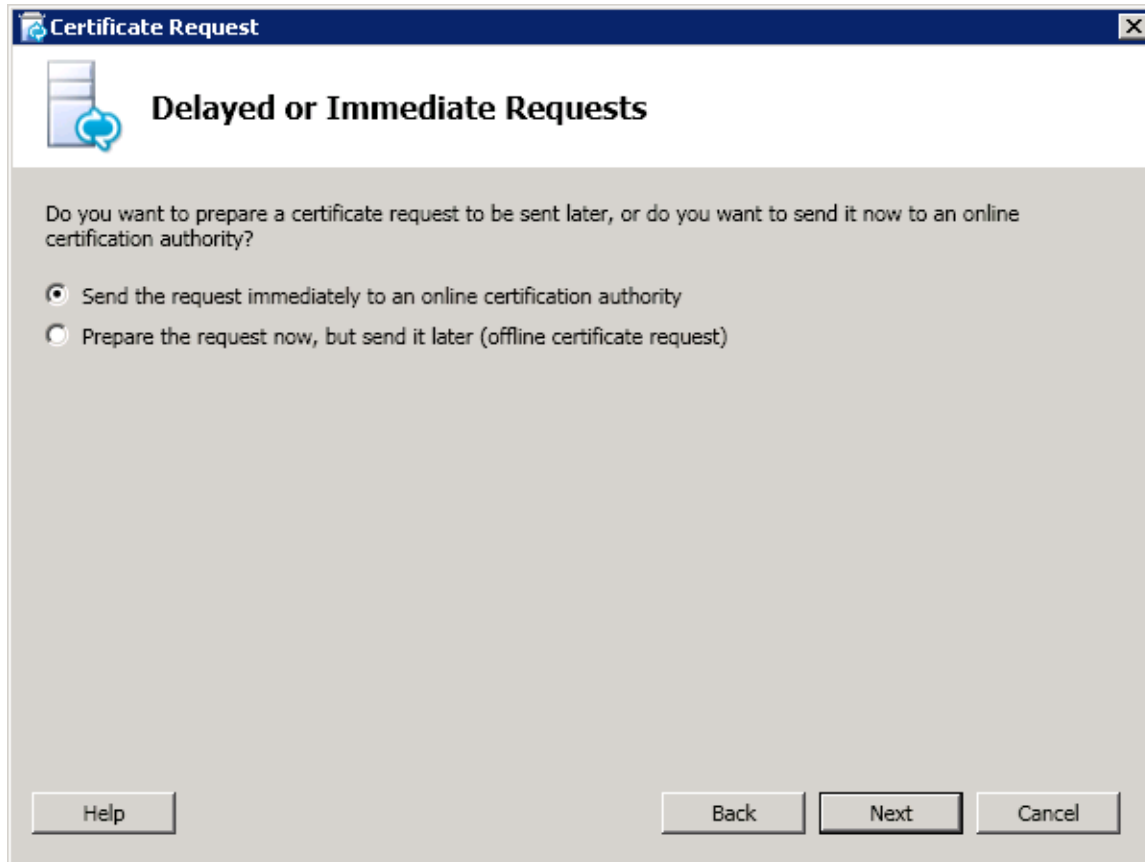
For step 3 of the wizard, “Request, Install or Assign Certificates” select ***Run or Run Again***.



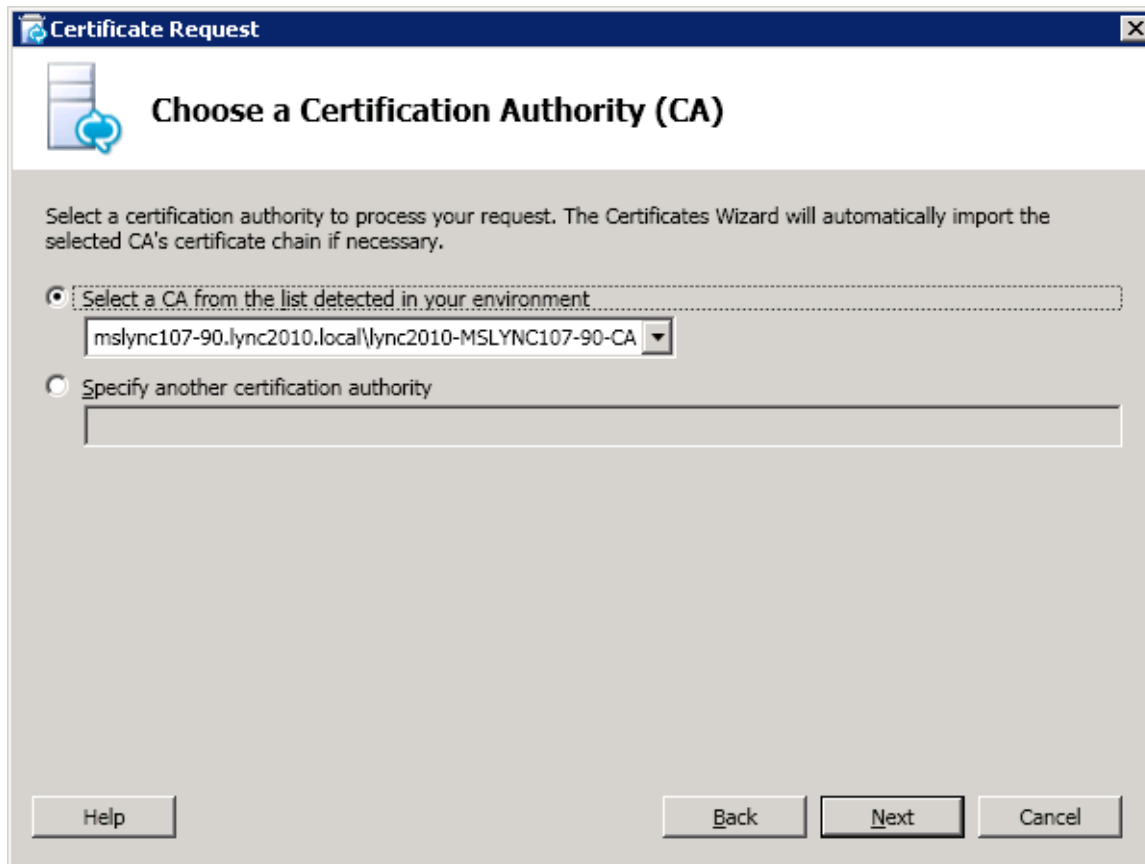
This launches the Certificate Wizard. Select Request which launches the certificate request screen, then select **Next** on the certificate request screen.



On the Delayed or Immediate Requests screen select “Send the request immediately to the certificate authority”. Then Select **Next**.



On the Choose a certificate Authority (CA) screen, select the radio button for “*Select a CA from the list detected in your environment*”. In the dropdown select CA Server, then Select **Next**.



The image shows a Windows-style dialog box titled "Certificate Request". Inside, there is a section titled "Choose a Certification Authority (CA)" with a sub-icon of a server and a circular arrow. Below this, a text box explains: "Select a certification authority to process your request. The Certificates Wizard will automatically import the selected CA's certificate chain if necessary." There are two radio buttons. The first is selected and labeled "Select a CA from the list detected in your environment". Below it is a dropdown menu showing "mslync107-90.lync2010.local\lync2010-MSLYNC107-90-CA". The second radio button is labeled "Specify another certification authority" and has an empty text box below it. At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".

Certificate Request

Choose a Certification Authority (CA)

Select a certification authority to process your request. The Certificates Wizard will automatically import the selected CA's certificate chain if necessary.

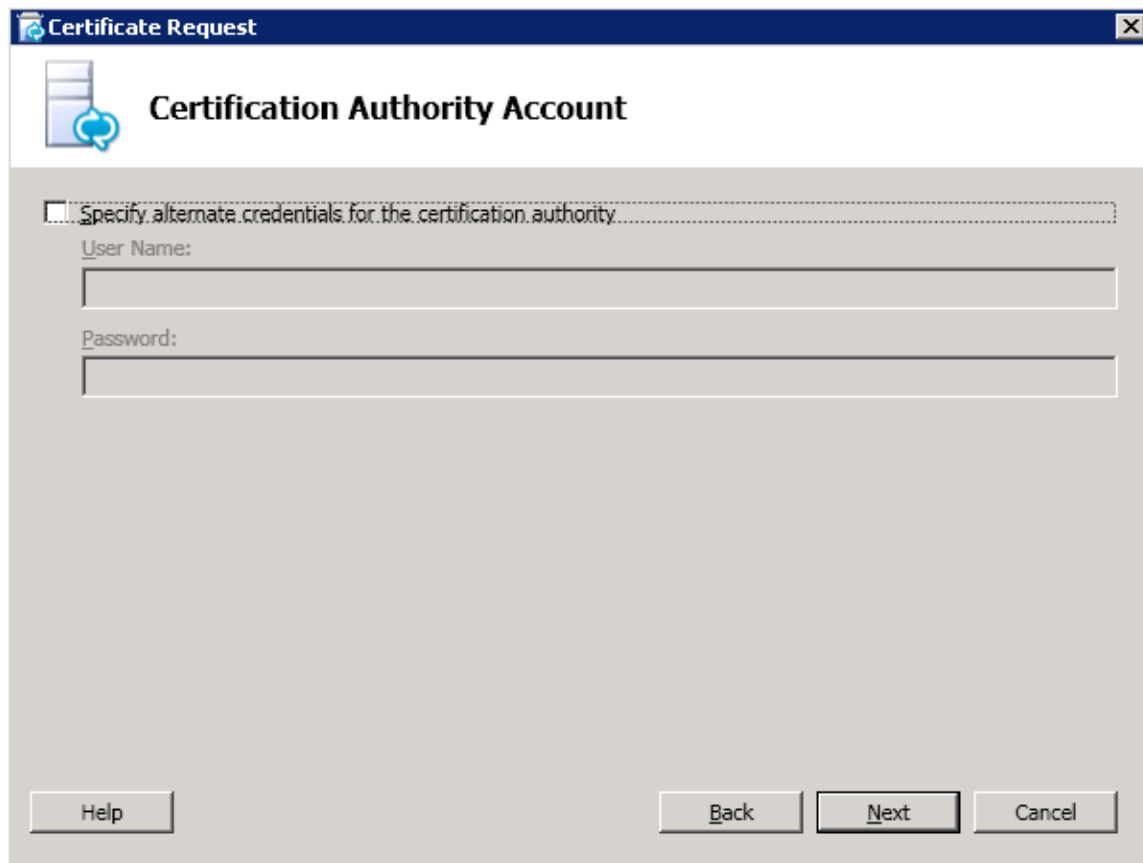
☒ Select a CA from the list detected in your environment

mslync107-90.lync2010.local\lync2010-MSLYNC107-90-CA ▼

☐ Specify another certification authority

Help Back Next Cancel

On the Certificate Authority Account Screen, select **Next**.



The image shows a Windows-style dialog box titled "Certificate Request" with a standard icon and a close button. The main heading is "Certification Authority Account" next to a server icon. Below this is a checkbox labeled "Specify alternate credentials for the certification authority...". Under the checkbox are two text input fields: "User Name:" and "Password:". At the bottom, there are three buttons: "Help", "Back", and "Next" (which is highlighted with a thick border), and a "Cancel" button.

Certificate Request

Certification Authority Account

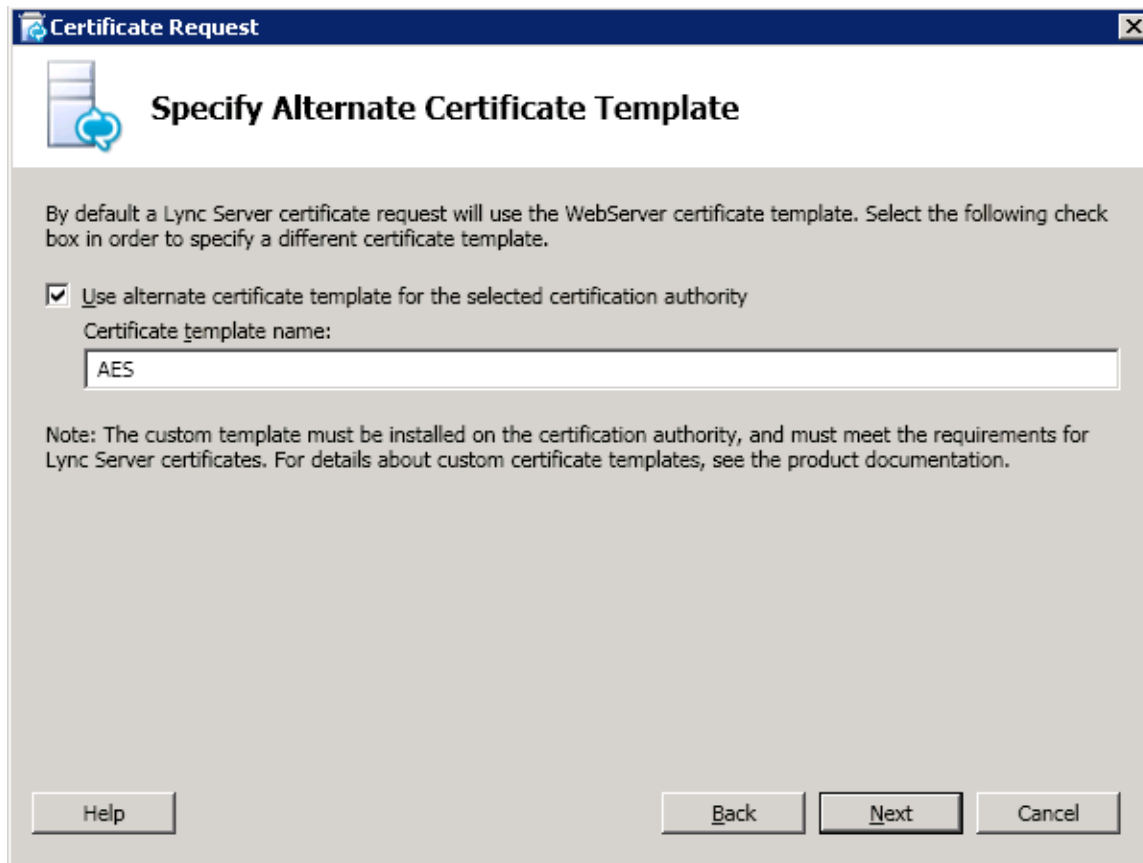
☐ Specify alternate credentials for the certification authority...

User Name:

Password:

Help Back **Next** Cancel

On the Specify Alternate Certificate Template screen, select the check box for *Use alternate certificate template for the selected certification authority*. Specify the name of the template you created earlier. Then select **Next**.



The screenshot shows a Windows-style dialog box titled "Certificate Request" with a sub-header "Specify Alternate Certificate Template". The dialog contains a checkbox labeled "Use alternate certificate template for the selected certification authority" which is checked. Below this is a text field labeled "Certificate template name:" containing the text "AES". A note at the bottom states: "Note: The custom template must be installed on the certification authority, and must meet the requirements for Lync Server certificates. For details about custom certificate templates, see the product documentation." At the bottom of the dialog are four buttons: "Help", "Back", "Next", and "Cancel".

Certificate Request

Specify Alternate Certificate Template

By default a Lync Server certificate request will use the WebServer certificate template. Select the following check box in order to specify a different certificate template.

☒ Use alternate certificate template for the selected certification authority

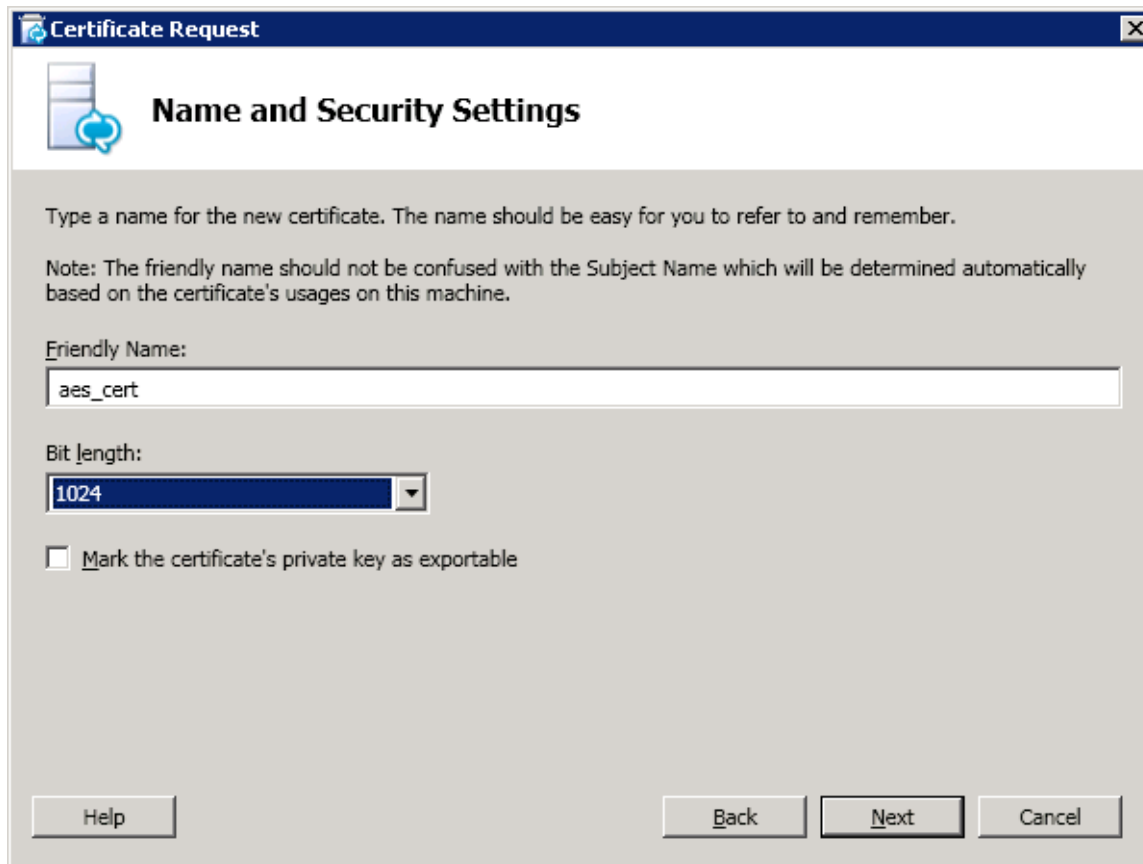
Certificate template name:

AES

Note: The custom template must be installed on the certification authority, and must meet the requirements for Lync Server certificates. For details about custom certificate templates, see the product documentation.

Help Back Next Cancel

On the Name and Security Settings screen, enter a friendly name and change the bit length by selecting **1024** in the dropdown. Select **Next**.



The image shows a Windows-style dialog box titled "Certificate Request". Inside, there is a section titled "Name and Security Settings" with a small icon of a document and a circular arrow. Below this, there is instructional text: "Type a name for the new certificate. The name should be easy for you to refer to and remember." followed by a note: "Note: The friendly name should not be confused with the Subject Name which will be determined automatically based on the certificate's usages on this machine." There are two input fields: "Friendly Name:" with the text "aes_cert" entered, and "Bit length:" with a dropdown menu showing "1024". Below these is a checkbox labeled "Mark the certificate's private key as exportable" which is currently unchecked. At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".

Certificate Request

Name and Security Settings

Type a name for the new certificate. The name should be easy for you to refer to and remember.

Note: The friendly name should not be confused with the Subject Name which will be determined automatically based on the certificate's usages on this machine.

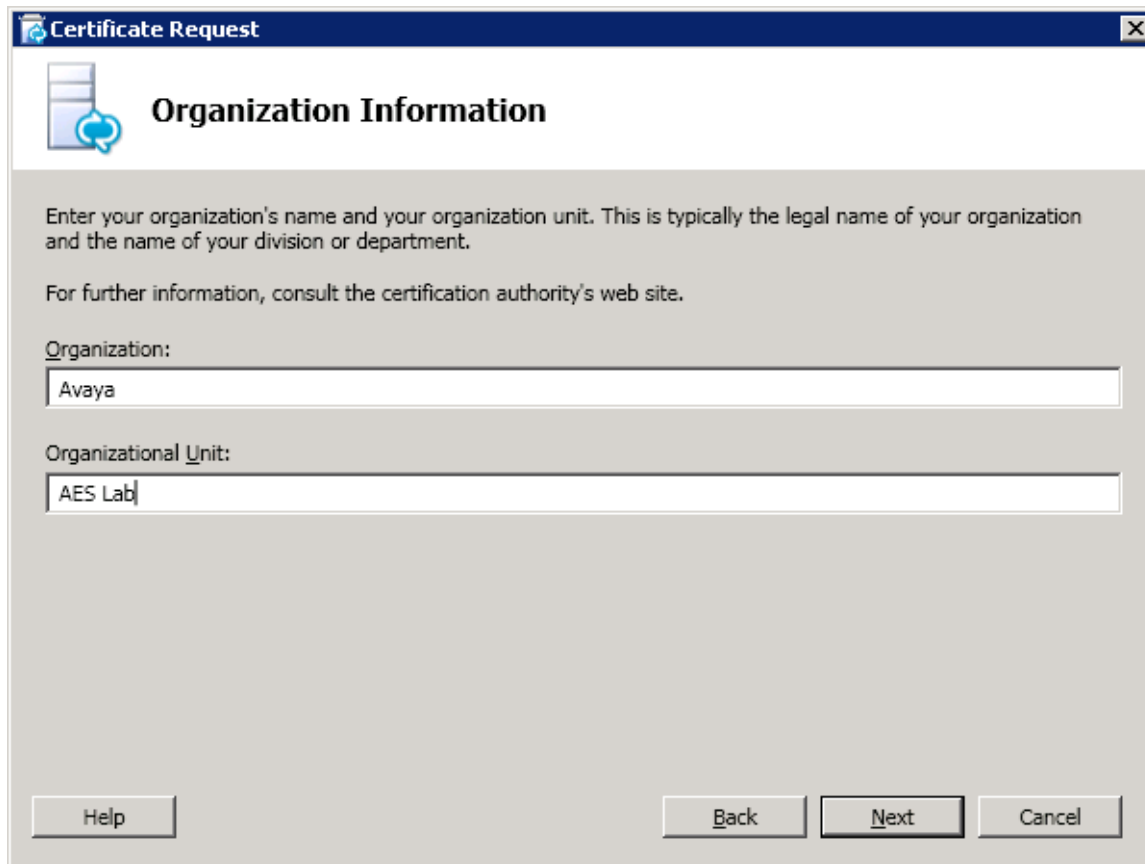
Friendly Name:
aes_cert

Bit length:
1024

☐ Mark the certificate's private key as exportable

Help Back Next Cancel

On the Organization Information screen provide your organizational information as prompted, then select **Next**.



The image shows a Windows-style dialog box titled "Certificate Request" with a close button in the top right corner. The main heading is "Organization Information" next to a server icon. The text inside the dialog reads: "Enter your organization's name and your organization unit. This is typically the legal name of your organization and the name of your division or department." followed by "For further information, consult the certification authority's web site." There are two text input fields: the first is labeled "Organization:" and contains the text "Avaya"; the second is labeled "Organizational Unit:" and contains the text "AES Lab". At the bottom of the dialog, there are four buttons: "Help", "Back", "Next", and "Cancel". The "Next" button is highlighted with a darker border.

Certificate Request

Organization Information

Enter your organization's name and your organization unit. This is typically the legal name of your organization and the name of your division or department.

For further information, consult the certification authority's web site.

Organization:

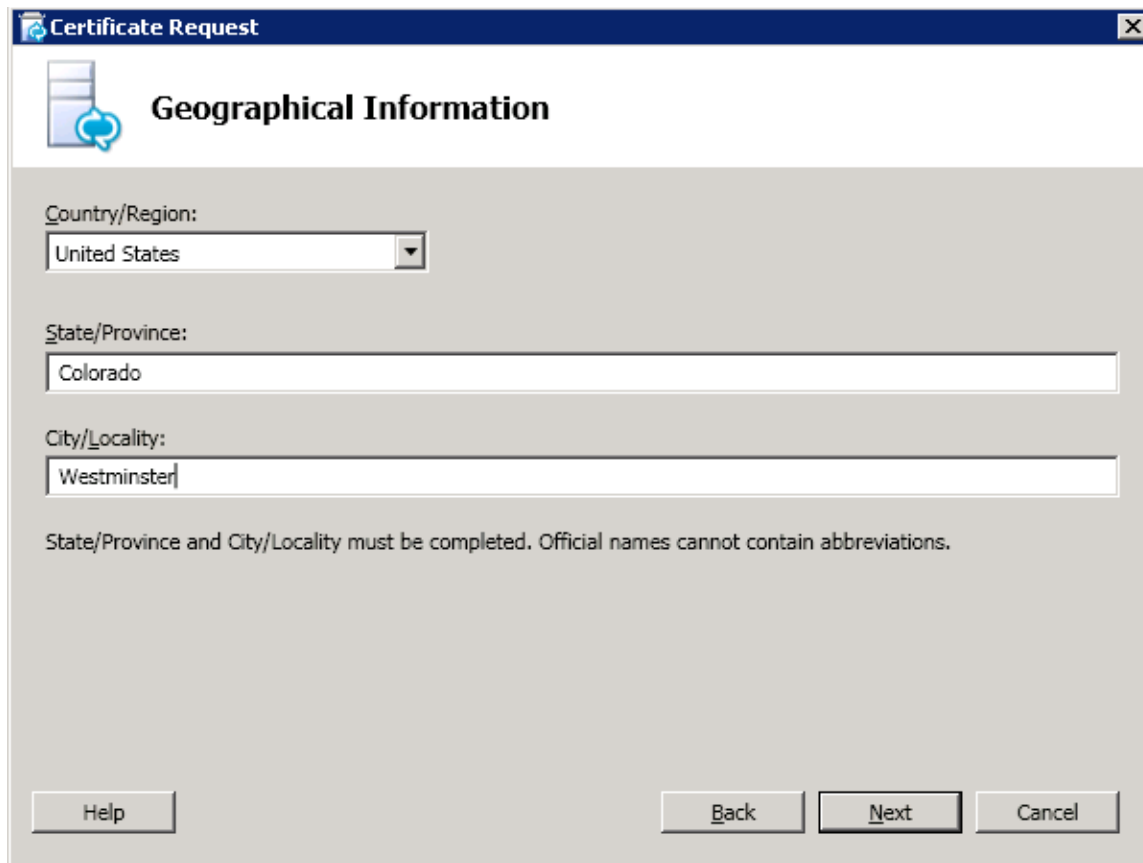
Avaya

Organizational Unit:

AES Lab

Help Back Next Cancel

On the Geographical Information screen provide your geographical information and select **Next**.



The image shows a Windows-style dialog box titled "Certificate Request" with a close button in the top right corner. The main heading is "Geographical Information" next to a small icon of a server with a circular arrow. Below this, there are three input fields: "Country/Region:" with a dropdown menu showing "United States", "State/Province:" with a text box containing "Colorado", and "City/Locality:" with a text box containing "Westminster". A note below these fields states: "State/Province and City/Locality must be completed. Official names cannot contain abbreviations." At the bottom, there are three buttons: "Help", "Back", and "Next" (which is highlighted with a black border), and a "Cancel" button.

Certificate Request

Geographical Information

Country/Region:
United States

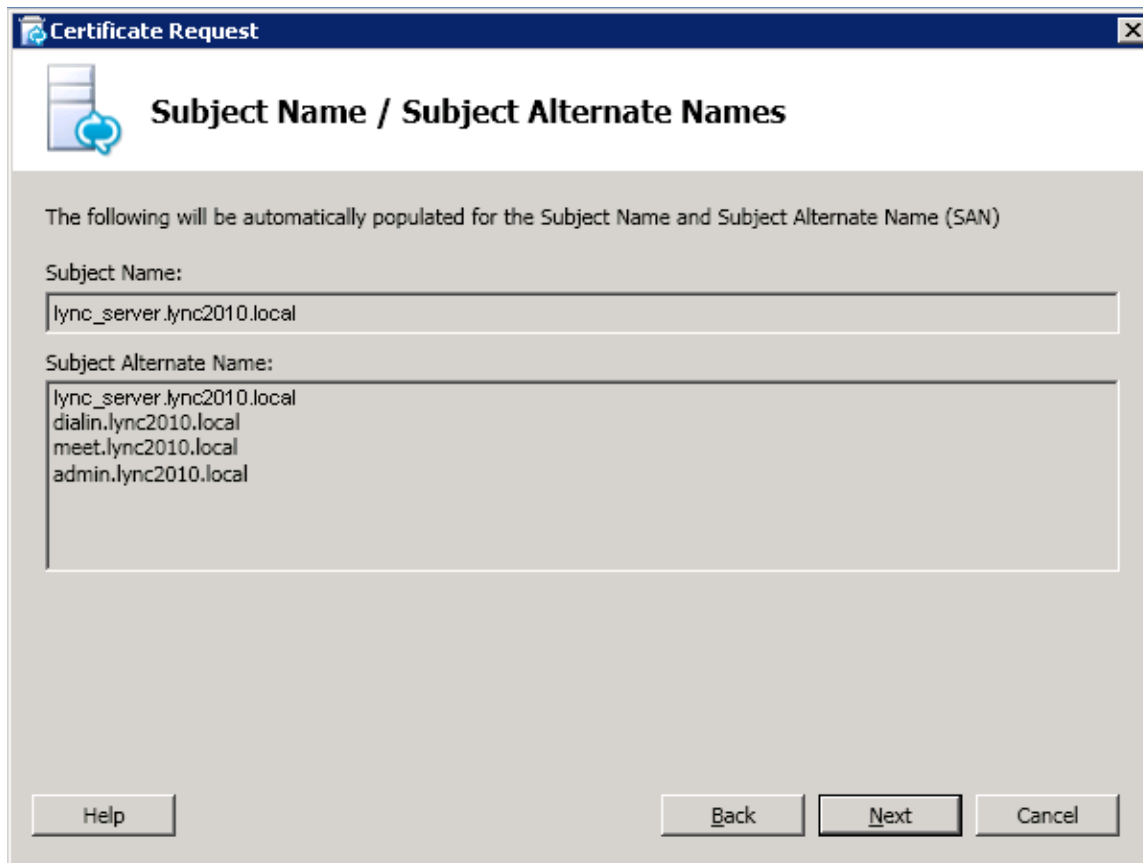
State/Province:
Colorado

City/Locality:
Westminster

State/Province and City/Locality must be completed. Official names cannot contain abbreviations.

Help Back **Next** Cancel

On the Subject Name / Subject Alternate Names screen select **Next**.



The image shows a Windows-style dialog box titled "Certificate Request". Inside the dialog, there is a sub-header "Subject Name / Subject Alternate Names" with a small icon of a document and a circular arrow. Below this, a message states: "The following will be automatically populated for the Subject Name and Subject Alternate Name (SAN)". There are two input fields. The first, labeled "Subject Name:", contains the text "lync_server.lync2010.local". The second, labeled "Subject Alternate Name:", contains a list of four entries: "lync_server.lync2010.local", "dialin.lync2010.local", "meet.lync2010.local", and "admin.lync2010.local". At the bottom of the dialog, there are four buttons: "Help", "Back", "Next", and "Cancel". The "Next" button is highlighted with a thick border.

Certificate Request

Subject Name / Subject Alternate Names

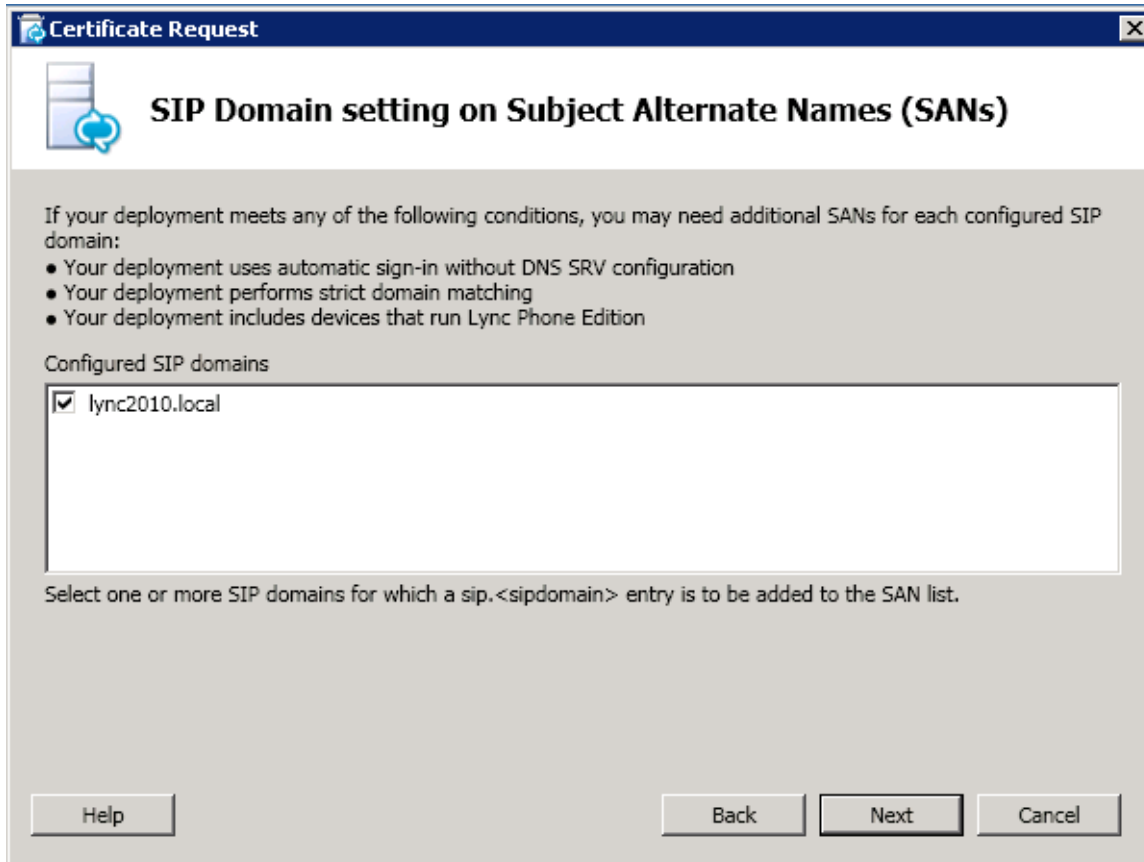
The following will be automatically populated for the Subject Name and Subject Alternate Name (SAN)

Subject Name:
lync_server.lync2010.local

Subject Alternate Name:
lync_server.lync2010.local
dialin.lync2010.local
meet.lync2010.local
admin.lync2010.local

Help Back Next Cancel

On the SIP Domain setting on Subject Alternate Names (SANs) screen select the SIP Domain(s) that were configured as part of the Lync Deployment and then select **Next**.



The image shows a Windows-style dialog box titled "Certificate Request". Inside, there is a sub-header "SIP Domain setting on Subject Alternate Names (SANs)" with a small icon of a server and a circular arrow. Below this, a paragraph explains that additional SANs may be needed based on deployment conditions. A list of three conditions is provided: automatic sign-in without DNS SRV, strict domain matching, and Lync Phone Edition devices. A section titled "Configured SIP domains" contains a list box with one entry, "lync2010.local", which is selected with a checkmark. Below the list box, a note states: "Select one or more SIP domains for which a sip.<sipdomain> entry is to be added to the SAN list." At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".

Certificate Request

SIP Domain setting on Subject Alternate Names (SANs)

If your deployment meets any of the following conditions, you may need additional SANs for each configured SIP domain:

- Your deployment uses automatic sign-in without DNS SRV configuration
- Your deployment performs strict domain matching
- Your deployment includes devices that run Lync Phone Edition

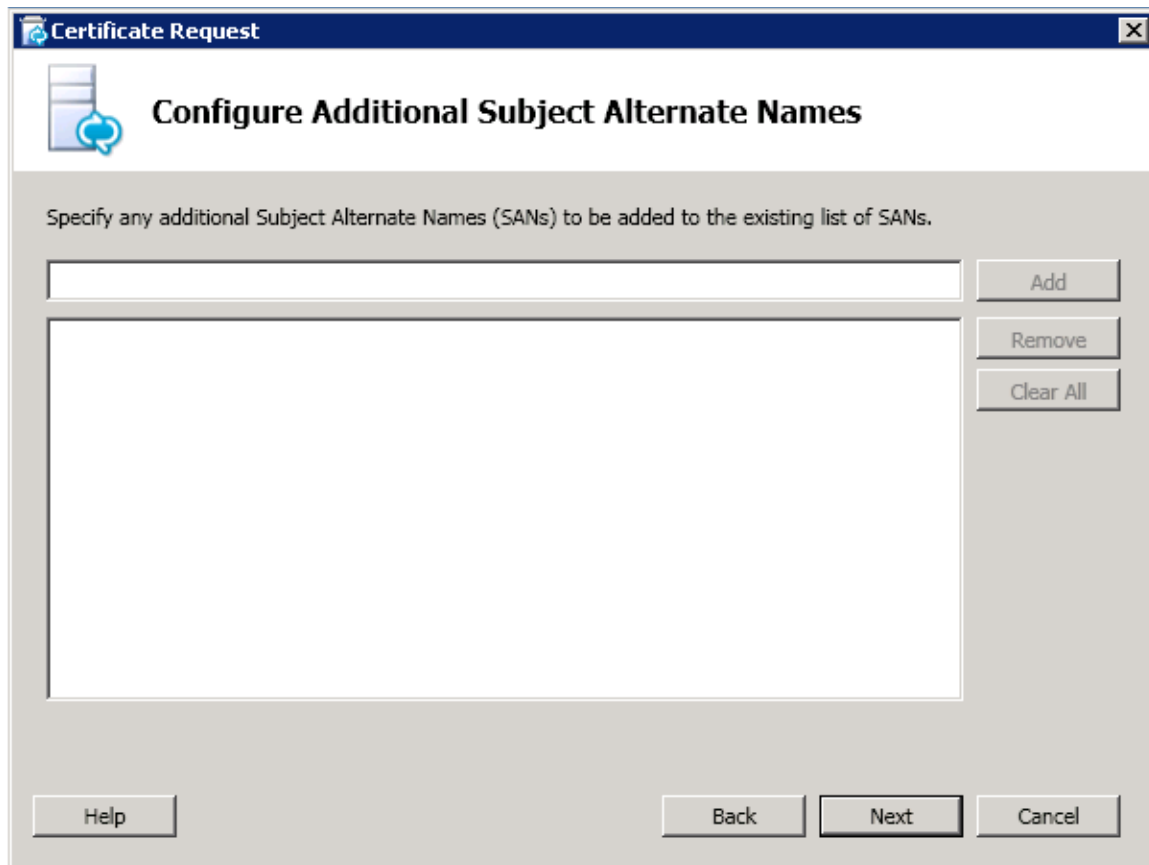
Configured SIP domains

☒ lync2010.local

Select one or more SIP domains for which a sip.<sipdomain> entry is to be added to the SAN list.

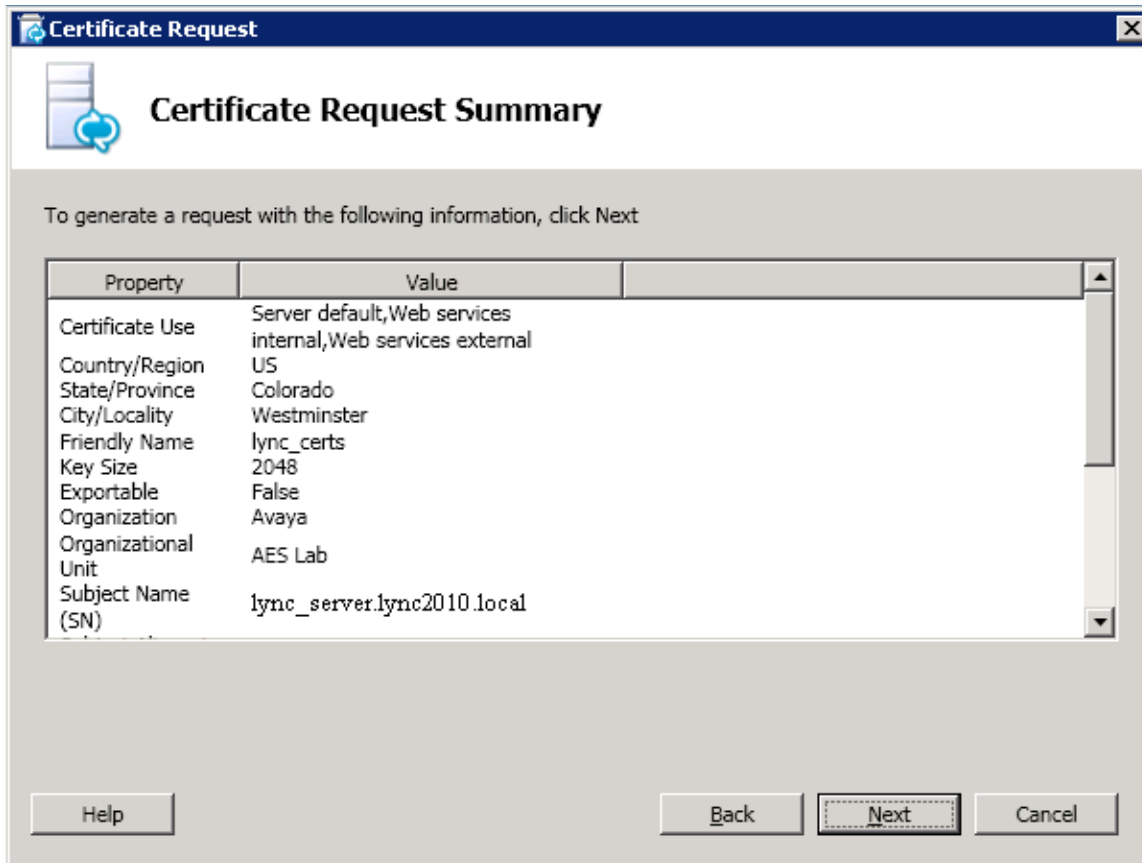
Help Back Next Cancel

On the Configured Additional Subject Alternate Names screen select **Next**.



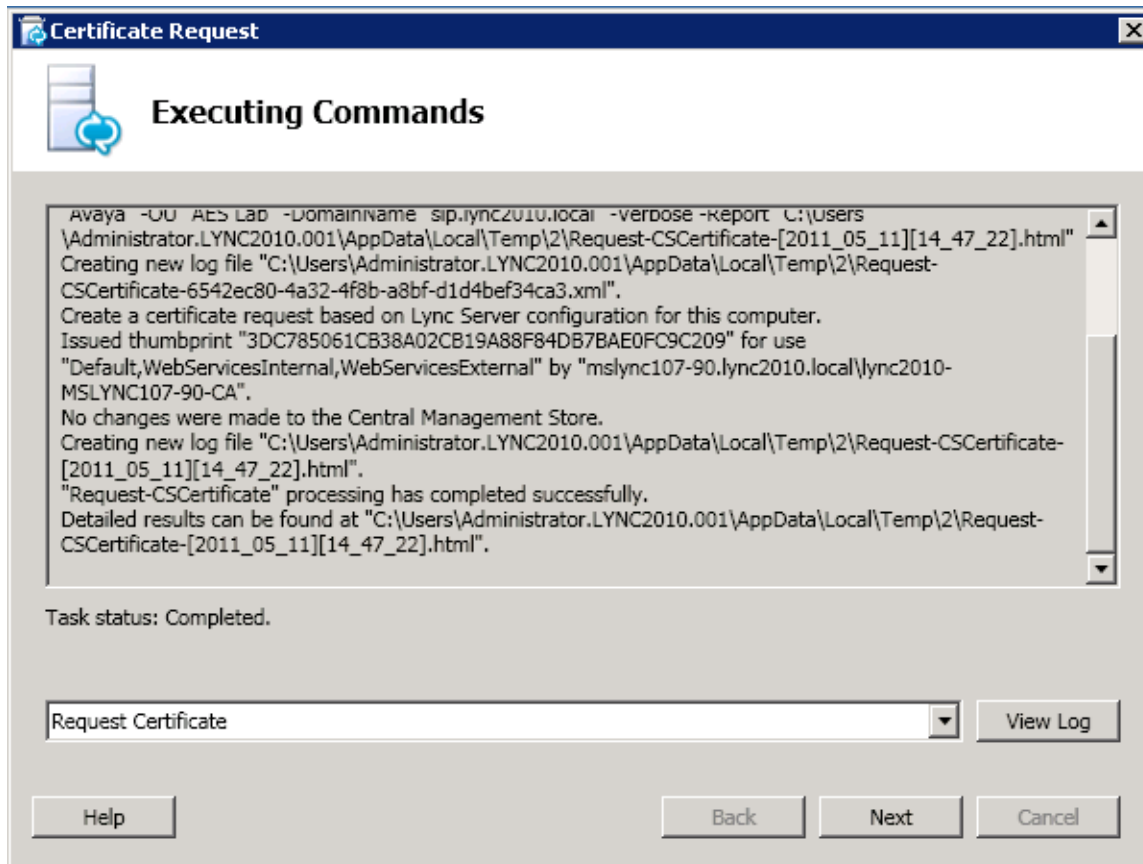
The screenshot shows a Windows-style dialog box titled "Certificate Request" with a close button in the top right corner. The main title bar is dark blue. Below the title bar, there is a light blue header area with a server icon and the text "Configure Additional Subject Alternate Names". The main content area is light gray and contains the instruction: "Specify any additional Subject Alternate Names (SANs) to be added to the existing list of SANs." Below this text is a large white rectangular input field. To the right of the input field are three buttons: "Add", "Remove", and "Clear All". At the bottom of the dialog, there are four buttons: "Help", "Back", "Next", and "Cancel". The "Next" button is highlighted with a black border.

On the Certificate Request Summary screen select **Next**.

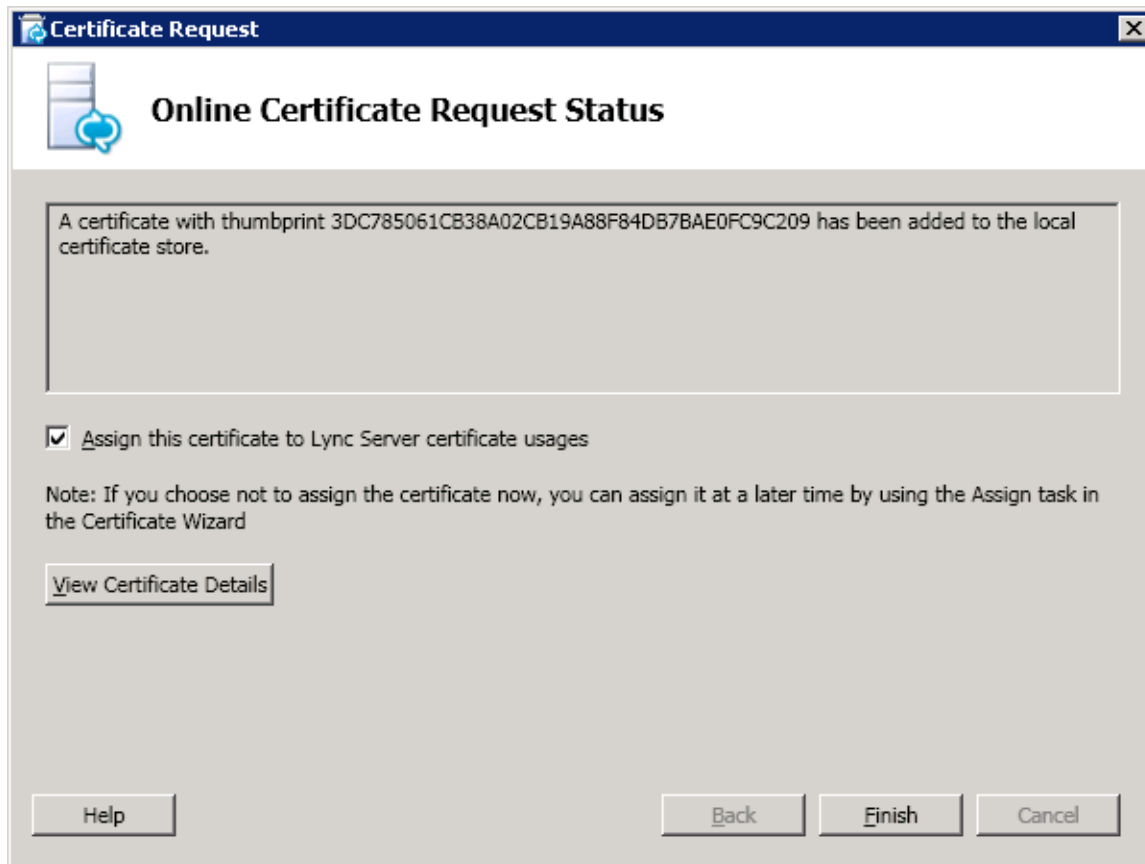
A screenshot of a Windows-style dialog box titled "Certificate Request". The main heading is "Certificate Request Summary". Below the heading is a message: "To generate a request with the following information, click Next". This message is followed by a table with two columns: "Property" and "Value". The table contains the following entries: Certificate Use (Server default, Web services internal, Web services external), Country/Region (US), State/Province (Colorado), City/Locality (Westminster), Friendly Name (lync_certs), Key Size (2048), Exportable (False), Organization (Avaya), Organizational Unit (AES Lab), and Subject Name (SN) (lync_server.lync2010.local). At the bottom of the dialog are four buttons: "Help", "Back", "Next" (which is highlighted with a dashed border), and "Cancel".

Property	Value
Certificate Use	Server default, Web services internal, Web services external
Country/Region	US
State/Province	Colorado
City/Locality	Westminster
Friendly Name	lync_certs
Key Size	2048
Exportable	False
Organization	Avaya
Organizational Unit	AES Lab
Subject Name (SN)	lync_server.lync2010.local

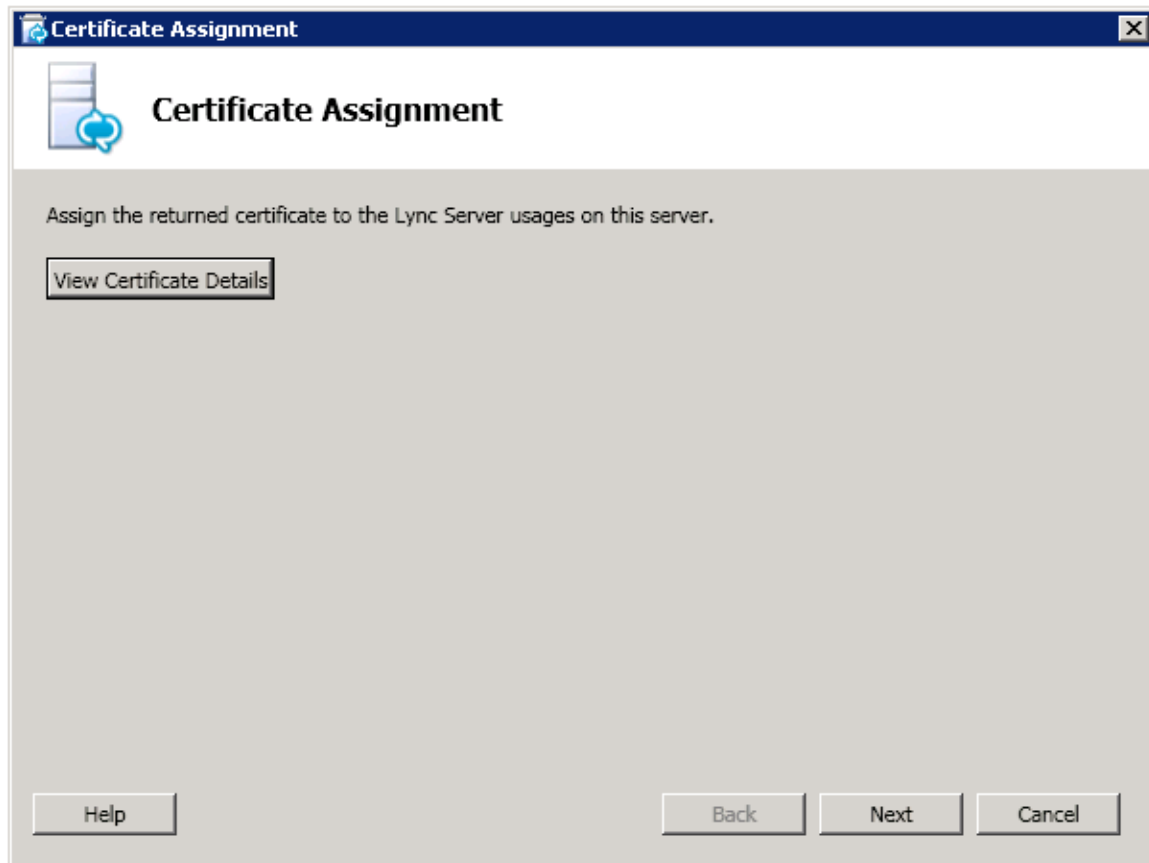
On the Executing Commands screen you will see a summary of commands executed. Select **Next**.



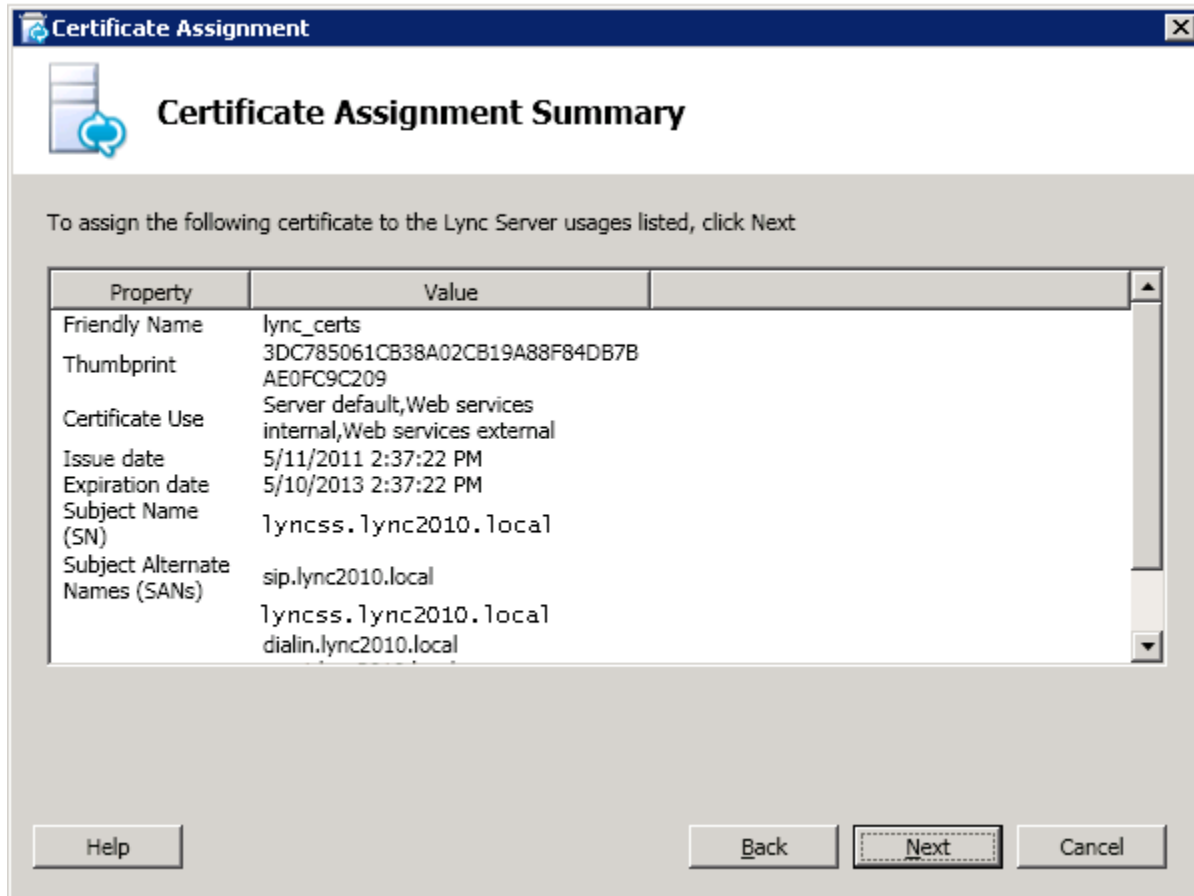
The Online Certificate Request Status screen is displayed. Leave the check box for “Assign this certificate to Lync Server certificate usages” checked and select **Finish**.



The Certificate Assignment wizard launches; select **Next**.



On the Certificate Assignment Summary screen, select **Next**.

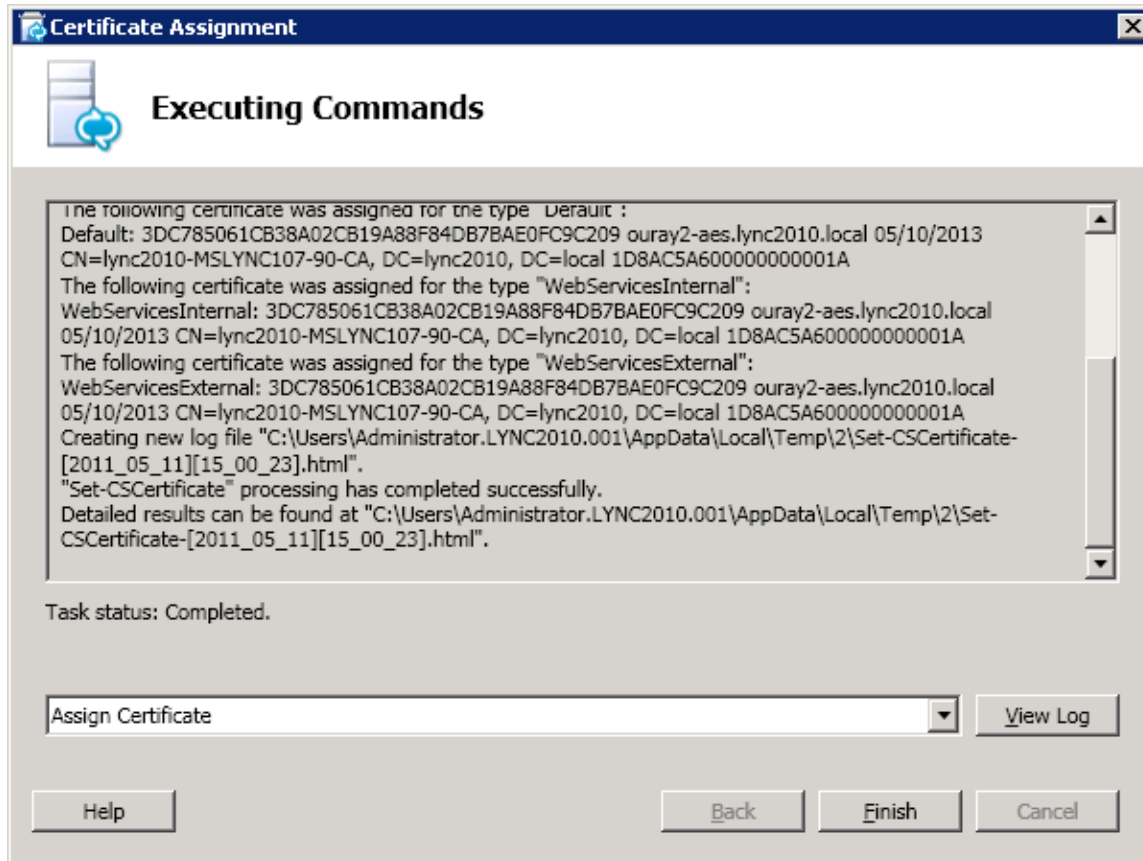


The image shows a Windows-style window titled "Certificate Assignment" with a close button in the top right corner. Below the title bar is a header area with a server icon and the text "Certificate Assignment Summary". The main content area has a message: "To assign the following certificate to the Lync Server usages listed, click Next". Below this message is a table with two columns: "Property" and "Value". The table contains the following data:

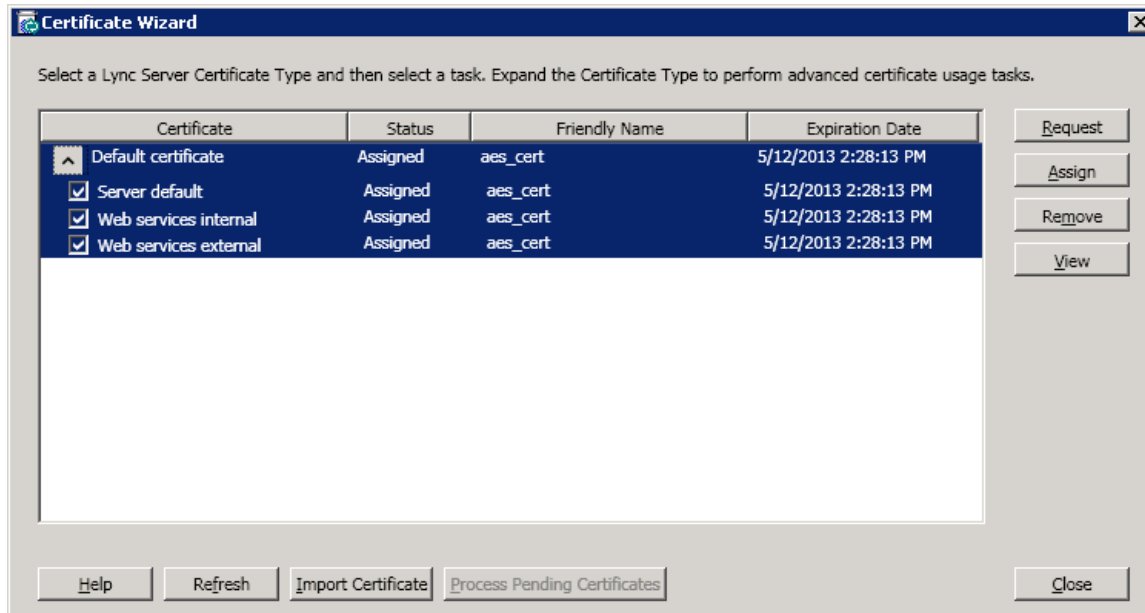
Property	Value
Friendly Name	lync_certs
Thumbprint	3DC785061CB38A02CB19A88F84DB7B AE0FC9C209
Certificate Use	Server default, Web services internal, Web services external
Issue date	5/11/2011 2:37:22 PM
Expiration date	5/10/2013 2:37:22 PM
Subject Name (SN)	lyncss.lync2010.local
Subject Alternate Names (SANs)	sip.lync2010.local lyncss.lync2010.local dialin.lync2010.local

At the bottom of the window, there are four buttons: "Help", "Back", "Next" (which is highlighted with a dashed border), and "Cancel".

Next, the summary screen displays executed commands and a "Task Status: Completed". Select Finish.



The Certificate Assignment Wizard closes. Selecting the dropdown next to *Default certificate* in the Certificate Wizard now shows the following certificates and status. You may select Close on the wizard.



Installing the trusted certificate on the AE Server

The trusted certificate is also referred to as the certificate authority (CA) certificate. It is issued by the certificate authority, which can be either Microsoft Certificate Services or another certificate authority.

Microsoft-based procedure for installing a trusted certificate chain

If you use a Microsoft CA hierarchy, follow this procedure from the AE Server to import the trusted certificate chain in PKCS#7 format from Microsoft Certificate Services into the AE Services Management Console.

1. From Internet Explorer, type the URL of your certificate server. For example:
http://<microsoftcertificate_server.com>/certsrv
2. From the Microsoft Certificate Services page, click **Download a CA certificate, certificate chain, or CRL**.
3. On the Download a CA Certificate, Certificate Chain, or CRL page, select the option button for **Base 64**, and click **Download CA certificate**.
4. Save the CA certificate file (the trusted certificate) to a local directory on the Microsoft Lync Server (for example **C:\temp\certnew.cer**).

5. Contact the Microsoft Lync Server administrator, and confirm that the certificate with the client and server authentication policies is installed and operating on the Microsoft Lync Server. The certificate must be installed and operating on Microsoft Lync Server before you can carry out the procedures in the AE Services Management Console.

Importing the trusted certificate into the AE Services Management Console

1. From the main menu of the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the CA Trusted Certificates page, click **Import**.
3. Complete the Trusted Certificate Import page, as follows:
 - In the Certificate Alias field, type an alias for the trusted certificate (for example, **lynccert**). The trusted certificate alias can be arbitrary. It does not need to match any aliases for AE Services.
 - Click **Browse** to locate the trusted certificate file you want to import, and click **Apply**. If the import is successful, AE Services displays the following message: "Certificate imported successfully."Verifying the installation of the trusted certificate in AE Services

Use this procedure to verify the installation of the entire certificate chain (all the way back to the root certificate) in AE Services.

1. In the AE Services Management Console, select **Security > Certificate Management > CA Trusted Certificates**.
2. From the CA Trusted Certificates page, select the alias of the trusted certificate (**lynccert**, based on this sample scenario), and click **View**.
3. From the Trusted Certificate Details page, verify that the information for the trusted certificate is correct.
 - a. Verify that the entire chain of certificates exists, all the way back to a self-signed certificate.
 - b. Verify that the Issued To and Issued By fields displays name of the organization that the trusted certificate is issued to.
 - c. Verify that the Expiration Date Indicates the date that the trusted certificate expires.
 - d. Verify the information in the Details display. Make sure the Certificate Status is valid.
4. Click **Close** to exit the Trusted Certificate Details page.

Administering AE Services access to Active Directory

Follow this procedure to set up the connection to Active Directory for AE Services.

From a browser, log in to the AE Services Management Console. Select **Security > Enterprise Directory**, Complete the Enterprise Directory page, as follows:

- User DN for Query Authentication - Type the DN for the user object that AE Services uses for accessing the Active directory. Based on how users are set up in Active Directory, the user object could correspond to a Full Name, a Display Name, or a User logon name.
- Password - Type a password to be used for Active Directory access; retype the same password in the Confirm Password field. This Active Directory password is stored in an encrypted format on the AE Server.
- Base Search DN -The Base Search DN is less specific than the User DN. Type the DN of the node that includes all user accounts that need access to the AE Services and Live Communications Server integration in the following format:
cn=users,dc=example,dc=com
- HostName/IP Address - Type the IP address or Host Name of the Domain Controller that runs Active Directory
- Port - (used for Active Directory access) - Change the default port number to an appropriate value for your configuration. The default is 389 (the port assignment for LDAP).
- Secondary Host Name / IP Address - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Lync Server
- Secondary Port - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Lync Server
- User ID Attribute Name - This setting defaults to uid, which is the default for AE Services User Management. For Microsoft Active Directory you must change this setting. The default setting for Microsoft Active Directory is samaccountname. If your implementation does not use the default for Microsoft Active Directory, enter the name of the attribute that is appropriate for your implementation.
- User Role Attribute Name - Enter the name of the attribute for the user role that your Enterprise Directory Server uses or leave blank if appropriate.
- Change Password URL - Accept the default (leave the field blank). This field does not apply to the AE Services implementation for Microsoft Lync Server.
- LDAP-S - Select LDAP-S if your configuration uses a TLS connection from AE Services to your Enterprise Directory Server.

For example:

- User DN for Query Authentication: **cn=Administrator,cn=Users,dc=lync2010,dc=local**
- Password: *********
- Confirm Password: *********
- Base Search DN: **cn=Users,dc=lync2010,dc=local**
- HostName/IP Address: **135.9.107.90**
- Port: **389**
- Secondary Host Name/IP Address: **-**
- User ID Attribute Name: **samaccountname**
- User Role Attribute Name: **-**
- Change Password URL: **-**
- Device ID Attribute: **msRTCSIP-Line**
- Search Filter Attribute Name: **msRTCSIP-PrimaryUserAddress**
- LDAPS **Select if used**

Select **Apply Changes** to put your changes into effect.

For more information, see “*Making changes on the Enterprise Directory Configuration*” on page 93 of *Avaya Aura® Application Enablement Services Implementation Guide for Microsoft Office Live Communications Server 2005 or Microsoft Office Communications Server 2007*.

Configuring Remote Call Control (RCC)

The Lync Server 2010 Management Shell is used to add an RCC gateway. It is recommended that RCC configuration be performed by or in coordination with the Lync Server System Administrator.

In the following example, RCC is set up using the Microsoft Lync Management Shell.

In step 5, “avaessrv” is a unique name chosen for the new application ID. It does not map to any previous configuration.

1. Start the Lync Server Management Shell using the appropriate credentials; from the Lync Server Console: **Start > All Programs > Microsoft Lync Server 2010 > Lync Server Management Shell**. From the command prompt and enter command specified at each step.
2. Run the following commands to capture any pre-existing configuration data if any for reference and copy to notepad.

```
PS C:\Users\Administrator.LYNC2010.001> Get-CsStaticRoutingConfiguration  
(should return null results unless a static route has previously been configured)
```

```
Identity : Global  
Route   : {}
```

```
PS C:\Users\Administrator.LYNC2010.001> Get-CsSipDomain (To view configured SIP domain(s). This will not be modified during RCC configuration in this example)
```

```
PS C:\Users\Administrator.LYNC2010.001> Get-CsTrustedApplicationPool (Retrieves settings for one or more pools that contain the computers that host trusted applications)
```

```
PS C:\Users\Administrator.LYNC2010.001> Get-CsSite (Retrieves site related configuration information)
```

For help with the Lync Server management Shell:

```
PS C:\Users\Administrator.LYNC2010.001> Get-Help
```

3. To create a static route first set the variable \$TLSRoute.

```
3a. PS C:\Users\Administrator.LYNC2010.001> $TLSRoute = New-CsStaticRoute  
-TLSRoute -Destination avaessrv.lync2010.local -Port 4723  
-UseDefaultCertificate $true -MatchUri *.lync201.local
```

Note that in step 3a, “avaessrv.lync2010.local” is the Fully Qualified Domain Name (FQDN) for the AE Services server; *.lync2010.local is the SIP domain prefixed with the wild card characters “*.”.

```
3b. PS C:\Users\Administrator.LYNC2010.001> Set-CsStaticRoutingConfiguration  
-Route @{Add=$TLSRoute}
```

4. Create a new trusted application entry. Type the following at the command prompt:

```
PS C:\Users\Administrator.LYNC2010.001> New-CsTrustedApplicationPool -Identity  
avaessrv.lync2010.local -Registrar lyncss.lync2010.local -Site 1  
-TreatAsAuthenticated $true -ThrottleAsServer $true -RequiresReplication $false
```

Note that in step 4, lyncss.lync2010.local is the FQDN of the Microsoft Lync Standard Server; "1" is a SiteID that was configured during Lync Server Deployment. See output of **Get-CsSite** for the SiteID field value.

5. Next add the trusted application to the pool. Type the following at the command prompt:

```
PS C:\Users\Administrator.LYNC2010.001> New-CsTrustedApplication  
-ApplicationID avaessrv -TrustedApplicationPoolFqdn avaessrv.lync2010.local  
-Port 4723
```

6. Use **Get-CsStaticRoutingConfiguration** and **Get-CsTrustedApplicationPool** to view the changes:

```
PS C:\Users\Administrator.LYNC2010.001> Get-CsStaticRoutingConfiguration
```

```
Identity : Global  
Route   : {MatchUri=*.lync2010.local;MatchOnlyPhoneUri=False;Enabled=True;  
ReplaceHostInRequestUri=False}
```

```
PS C:\Users\Administrator.LYNC2010.001> Get-CsTrustedApplicationPool
```

```
Identity       : TrustedApplicationPool:avaessrv.lync2010.local  
Registrar      : Registrar:lyncss.lync2010.local  
FileStore      :  
ThrottleAsServer : True  
TreatAsAuthenticated : True  
OutboundOnly    : False  
RequiresReplication : False  
AudioPortStart  :  
AudioPortCount  : 0  
AppSharingPortStart :  
AppSharingPortCount : 0  
VideoPortStart  :  
VideoPortCount  : 0  
Applications    : {urn:application:avaessrv}  
DependentServiceList : {}  
ServiceId       : 1-ExternalServer-1  
SiteId          : Site:westy  
PoolFqdn        : avaessrv.lync2010.local  
Version         : 5  
Role            : TrustedApplicationPool
```

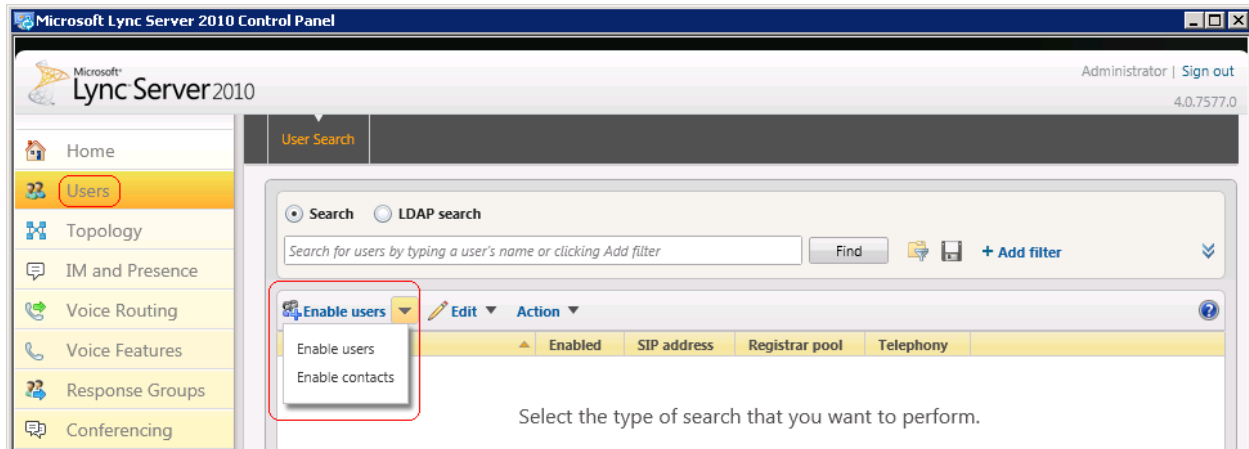

7. To implement the published changes you have made to the topology, type the command:

```
PS C:\Users\Administrator.LYNC2010.001> Enable-CsTopology
```

Enable users for RCC

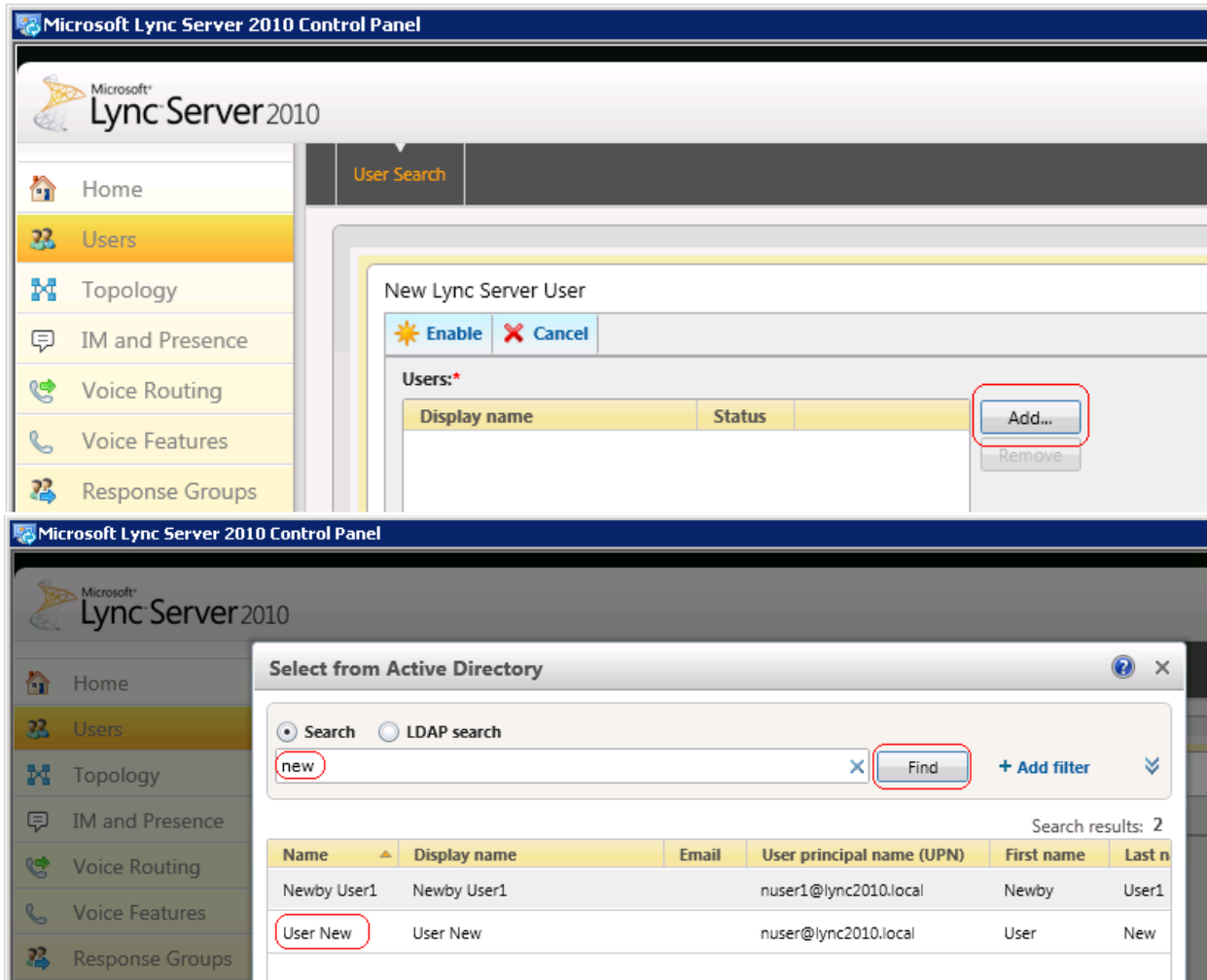
AD users must be enabled in the Lync Server Control Panel before using the Microsoft Lync Client.

1. Start the Lync Server Control Pane. Access the Lync Server Console using the appropriate credentials, run: Start > All Programs > Microsoft Lync Server 2010 > Lync Server Control Panel



2. To enable users, select **Users** in the left pain. Then in the right pain select the drop down Enable Users. This brings up the enable users dialog. In the right pane select **Add**.

There are different types of Active Directory searches you can perform to find various groups of users. To enable an AD user enter the AD user's name and select Find. Select the user from the list and then select **Okay**.



This will take you to the New Lync Server User screen shown below.

The screenshot displays the Microsoft Lync Server 2010 management console. On the left is a navigation pane with icons and labels for Home, Users (highlighted), Topology, IM and Presence, Voice Routing, Voice Features, Response Groups, Conferencing, Clients, External User Access, Monitoring and Archiving, Security, and Network Configuration. The main area is titled 'New Lync Server User' and includes a 'User Search' tab. Below the title are 'Enable' and 'Cancel' buttons. A section labeled 'Users:' contains a table with columns 'Display name' and 'Status', and 'Add...' and 'Remove' buttons. Below this is a dropdown for 'Assign users to a pool:'. The 'Generate user's SIP URI:' section has four radio button options: 'Use user's email address' (selected), 'Use the user principal name (UPN)', 'Use the following format:', and 'Specify a SIP URI:'. Each option has associated input fields. The 'Telephony:' section has a dropdown for 'Remote call control'. The 'Line URI:' section has a text input field. The 'Line Server URI:' section has a text input field. The 'Conferencing policy:' section has a dropdown for '<Automatic>' and a 'View...' button.

Microsoft®
Lync Server 2010

Home Users Topology IM and Presence Voice Routing Voice Features Response Groups Conferencing Clients External User Access Monitoring and Archiving Security Network Configuration

User Search

New Lync Server User

Enable Cancel

Users:

Display name	Status
--------------	--------

Add... Remove

Assign users to a pool:

Generate user's SIP URI:

☒ Use user's email address

☐ Use the user principal name (UPN)

☐ Use the following format:

<FirstName>.<LastName> @

☐ Use the following format:

<SAMAccountName> @

☐ Specify a SIP URI:

sip:example @

Telephony:

Remote call control

Line URI:

tel:+123456

Line Server URI:

sip:example@example.com

Conferencing policy:

<Automatic> View...

3. In the Assign users to a pool dropdown, select the pool which is typically the FQDN of the Lync Server
4. Under Generate a User's SIP URI, select an appropriate option.
5. Under Telephony, Select *Remote Call Control* or *Remote Call Control Only* from the drop down. The latter will not allow users to place calls using their computer.
7. In Line URI text box: specify a line URI in the format: tel:+13033731018. Lync also supports dial plan conversion to extensions on the user form using the format: tel:+13033731018;ext=731018 however this prevents name resolution in the call window received at the called party when the client places a call. Using the E.164 number format without the extension and doing any necessary dial plan conversion in AE Services is recommended.
8. Assign the Line Server URI:, the format for this is "sip:aes@avaessrv.lync2010.local" where avaessrv.lync2010.local is the FQDN of the Avaya AE Services Server.

Recommendations for Active Directory and Lync User related Administration.

Name resolution can be configured independently from the Active Directory user administration but the simplest way to accomplish this is to start by setting up the AD User record > General Tab > Telephone Number field with the e.164 phone number: "+13033731018". Access Active Directory Users and Groups on the appropriate Domain Controller or system running Remote Server Administration Tools (RSAT). From the console select **Start > Administrative Tools > Active Directory Users and Computers**. Expand the appropriate domain in the left pain and then select the Users folder. You can right click on the users folder and select **New > User** to create a new AD user account or after selecting the user folder select a user to modify in the right pain.

The screenshot shows the 'John Smith Properties' dialog box with the following details:

- General Tab:**
 - First name: John
 - Initials: (empty)
 - Last name: Smith
 - Display name: John Smith
 - Description: (empty)
 - Office: (empty)
 - Telephone number: +13033731018
 - E-mail: (empty)
 - Web page: (empty)
- Telephones Sub-tab:** (Visible but empty)
- Buttons:** OK, Cancel, Apply, Help

By populating the E.164 number in the Telephone number box on the General tab as shown above, the default behavior for RCC calls originated from this client will be to resolve the Active Directory name and display as follows in the call window that appears at the called client:

“John Smith”

“Work +1 (303) 373-1018 X731018 is calling you”

In cases where it is not easy to configure AD users with a +E.164 format phone number on the AD User record General Tab; translations rules can be implemented on the Microsoft Lync 2010 Server to normalize non +E.164 formatted numbers to +E.164 format. The Lync Client will not display the number for any contact that does not normalize to +E.164 format. Name resolution will fail for calls placed from any client whose number fails to normalize to +E.164 format. Setting up translation rules will also normalize numbers entered in the Lync Client search box allowing the user to complete calls that might otherwise not complete.

To implement E.164 Normalization do the following:

1. Create a file called Company_Phone_Number_Normalization_Rules.txt and save it on the Microsoft Lync 2010 Server in the root directory of <Share Name>\1-WebServices-1\ABfiles\

Enter values to handle conversions in the following format:

##

Normalize AD Phone Number Patterns From AD to +E.164

##

(\d{10})

+1\$1

- Matches string 303-555-1212 and converts this to +1-303-555-1212

(\d{7})

+1303\$1

- Matches the string 555-1212 and converts this to +1-303-555-1212

Note:

The default behavior of Lync is to ignore and remove the characters “(,)” and “-“automatically so these characters do not pose a concern when entered in AD and other fields a user may populate.

You will need to create a conversion entry for every string you wish to handle in this file.

To insure clients use the translation rules avoid using the following client setting in the Lync Server client policy configuration:

“AddressBookAvailability :WebSearchOnly”

The recommended settings are:

“AddressBookAvailability: :FileDownloadOnly”

“AddressBookAvailability: :WebSearchAndFileDownload” (this is the default setting)

To view the current configuration for this setting run this command from the Lync Server Management Shell:

```
PS C:\Users\Administrator.LYNC2010.001> get-CsClientPolicy
```

```
Identity           : Global
PolicyEntry         : {}
Description         :
AddressBookAvailability : WebSearchAndFileDownload (default)
AttendantSafeTransfer :
AutoDiscoveryRetryInterval :
BlockConversationFromFederatedContacts :
```

Conclusion

This concludes configuration steps directly related to integration of AE services and should provide basic steps necessary for successful integration. For further information please refer to the reference documentation on Pages 1 and 2 of this guide.

<http://support.avaya.com>