



# **Dialogic® 4000 Media Gateway Series as a Survivable Branch Appliance for Microsoft Lync Server 2010**

## **Deployment Guide**

# Copyright and Legal Notice

---

Copyright © 2011 Dialogic Inc. All Rights Reserved. You may not reproduce this document in whole or in part without permission in writing from Dialogic Inc. at the address provided below.

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see <http://www.dialogic.com/company/terms-of-use.aspx> for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Inc. at the address indicated below or on the web at [www.dialogic.com](http://www.dialogic.com).

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 1504 McCarthy Boulevard, Milpitas, CA 95035-7405 USA. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, Diva ISDN, Making Innovation Thrive, Video is the New Voice, VisionVideo, Diastar, Cantata, TruFax, SwitchKit, SnowShore, Eicon, Eiconcard, NMS Communications, NMS (stylized), SIPcontrol, Exnet, EXS, Vision, PowerMedia, PacketMedia, BorderNet, inCloud9, I-Gate, ControlSwitch, NaturalAccess, NaturalCallControl, NaturalConference, NaturalFax and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 1504 McCarthy Boulevard, Milpitas, CA 95035-7405 USA. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

## Table of Contents

---

<b>Overview .....</b>	<b>4</b>
<b>SBA Deployment.....</b>	<b>4</b>
Data Center Workflow .....	4
Branch Workflow .....	11
<b>Using SIPcontrol Software Configuration Wizard to Configure SBA .....</b>	<b>13</b>
<b>Generating Private Key Files and Certificates Using Active Directory Certificate Services .....</b>	<b>19</b>
<b>Uploading Key Files and Certificate Request to SIPcontrol Software.....</b>	<b>26</b>

## Overview

---

This document describes how to prepare your system to deploy a Dialogic® 4000 Media Gateway (DMG4000 Gateway) as a Survivable Branch Appliance (SBA) that works with Microsoft Lync Server 2010. The DMG4000 Gateway SBA is a purpose-built appliance that includes a blade server running Microsoft Windows Server 2008 R2, Microsoft Lync Server 2010 Registrar and Mediation Server software, and a PSTN Gateway, in a single appliance chassis.

This document also describes the high level steps required to be able to deploy an SBA Server that consists of Microsoft Lync Server 2010 Registrar and Mediation Server software installed on regular Microsoft Windows Server hardware. For hardware specifications, refer to the Microsoft document *Planning for Your Organization: Microsoft Lync Server 2010*.

## SBA Deployment

Deploying a DMG4000 Gateway as SBA requires steps that must be done at the data center and steps that must be done at the branch site.

### Data Center Workflow

The steps in this section must be performed at the data center.

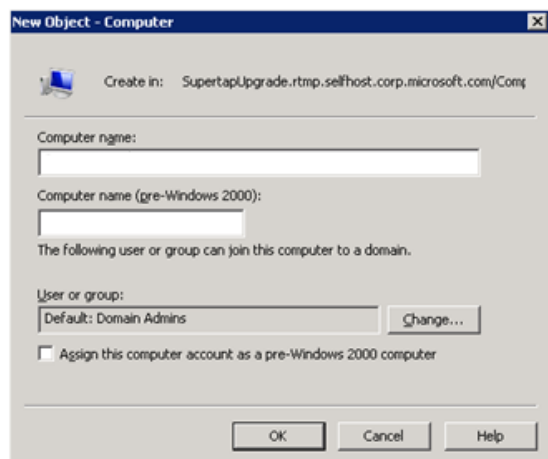
#### Adding the SBA Device to the Active Directory

Adding the DMG4000 Gateway SBA device to the active directory requires adding the device to the Active Directory Domain Services and then creating a user account to perform the SBA deployment.

To add the DMG4000 Gateway SBA device name to the Active Directory Domain Services and create a user account, follow these steps:

1. Access the Windows Administrative tools, and click on **Active Directory Users and Computers**.
2. Navigate to **Computers** under the proper domain in tree view. Then right-click and select **New > Computer**.

The New Object Computer dialog box appears:



3. Add the DMG4000 Gateway SBA device to the active directory, as follows:
  - a. In the Computer name field, specify the computer name for the DMG4000 Gateway SBA device. (Do not specify the FQDN.)
  - b. Click on **Change** to specify the name and user of the group that is allowed to join in the domain specified in the Computer name field.
  - c. Select the *RTCUniversalReadOnlyAdmins* group.
  - d. Click on **OK**.
4. Open up ADSI Edit, open up the properties for the DMG4000 Gateway SBA device, and then set servicePrincipalName to HOST/<SBA FQDN>, where <SBA FQDN> is the Fully Qualified Domain Name (FQDN) of the SBA.
5. Navigate back to Computers under the proper domain in tree view. Then right-click and select **New > User**.

The New Object – User dialog box appears:

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: rtm1.w14.loc/Users'. Below this are several input fields: 'First name:', 'Initials:', 'Last name:', 'Full name:', 'User logon name:' (with a dropdown menu showing '@rtm1.w14.loc'), and 'User logon name (pre-Windows 2000):' (with the text 'RTM1\''). At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

6. Fill in the fields on the New Object – User dialog box to create a user account on the Active Directory Domain Services belonging to the *RTCUniversalSBATEchnicians* group. This user will perform the SBA deployment.
7. Click on **Next**.

A page appears that asks for a password:

The screenshot shows a dialog box for setting a password. It has two text input fields: 'Password:' and 'Confirm password:'. Below these are four checkboxes:
 

- ☒ User must change password at next logon
- ☐ User cannot change password
- ☐ Password never expires
- ☐ Account is disabled

 At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

8. Enter your password in the Password and Confirm password fields, and optionally, change the password security option.
9. Click on **Next**.

A confirmation page appears.

10. Click on **Finish**.
11. Click on **OK**.

The specified DMG4000 Gateway SBA device is added to the domain computers.

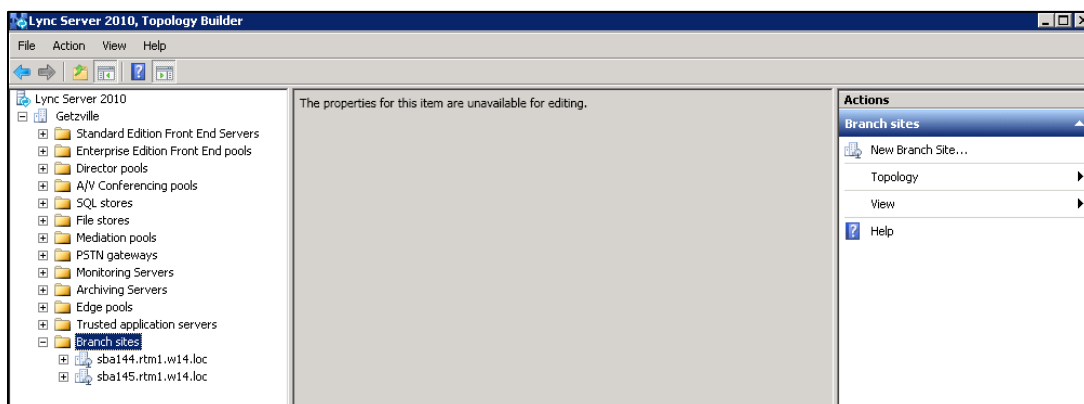
## Defining Branch Office Topology through Topology Builder

This section explains how to use Topology Builder to add the SBA to your topology, and how to enable the topology.

To create branch sites, follow these steps:

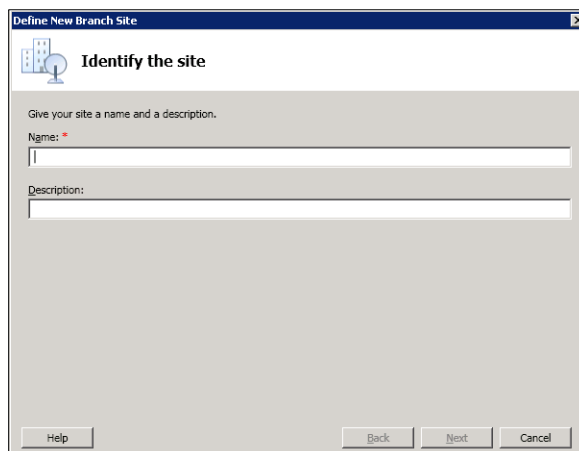
1. Open the Topology Builder by selecting **Start > All Programs > Microsoft Lync Server 2010 > Communications Server Topology Builder**.

The Microsoft Lync Server 2010 Server Topology Builder console tree appears:



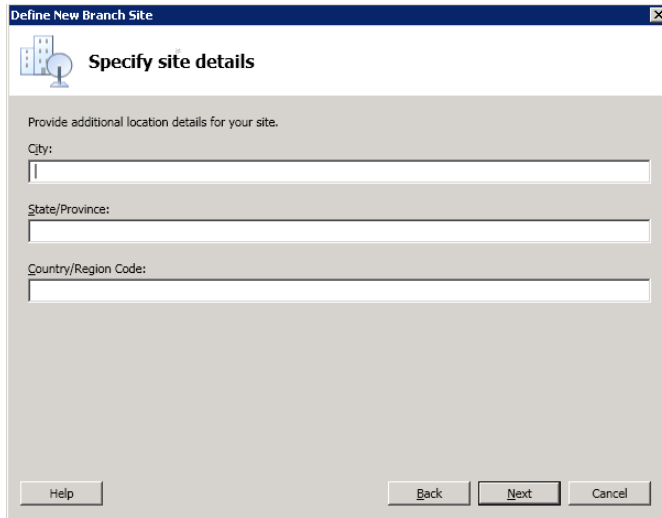
2. In the console tree, right-click the **Branch sites** node, and then click on **New Branch Site** in the Actions section on the right.

The Identify the site dialog box appears:



3. In the Name field, type the name of the branch site. This field is required.
4. In the Description field, type a meaningful description for the branch site.
5. Click on **Next**.

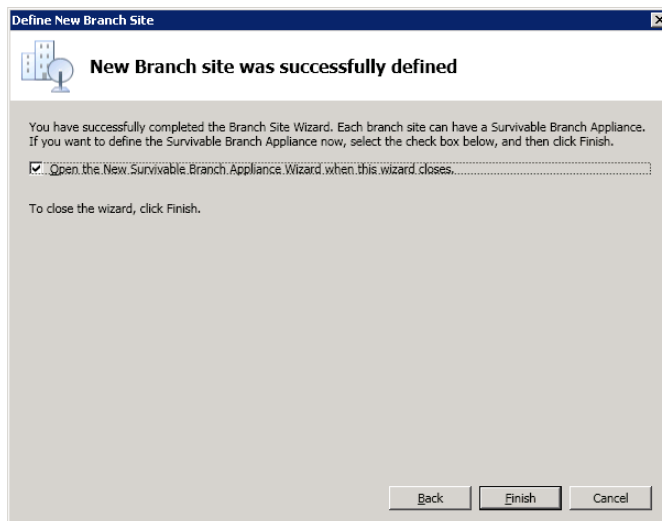
The Specify site details dialog box appears:



The dialog box is titled "Define New Branch Site" and "Specify site details". It contains three text input fields labeled "City:", "State/Province:", and "Country/Region Code:". At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".

6. In the City field, optionally type the name of the city in which the branch site is located.
7. In the State/Province field, optionally type the name of the state or region in which the branch site is located.
8. In the Country/Region Code field, optionally type the two-digit calling code for the country in which the branch site is located.
9. Click on **Next** to create the branch site.

A confirmation dialog box appears:



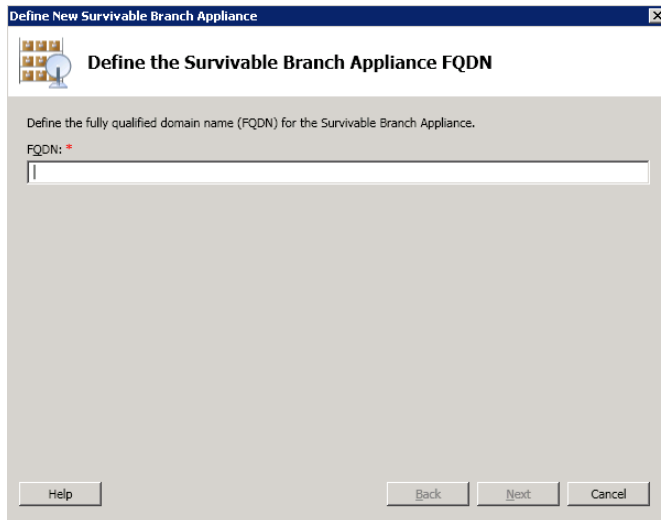
The dialog box is titled "Define New Branch Site" and "New Branch site was successfully defined". It contains a message: "You have successfully completed the Branch Site Wizard. Each branch site can have a Survivable Branch Appliance. If you want to define the Survivable Branch Appliance now, select the check box below, and then click Finish." Below the message is a checked checkbox with the text "Open the New Survivable Branch Appliance Wizard when this wizard closes...". At the bottom, there are three buttons: "Back", "Finish", and "Cancel".

10. Repeat Steps 2 through 9 to create another branch site, or click on **Finish** to close the wizard and open the New Survivable Branch Appliance Wizard.

To define an SBA, follow these steps:

1. Click on **Survivable Branch Servers** node, and then click on **New Branch Site**, in the Actions section on the right.

The Define the Survivable Branch Appliance FQDN dialog box appears:

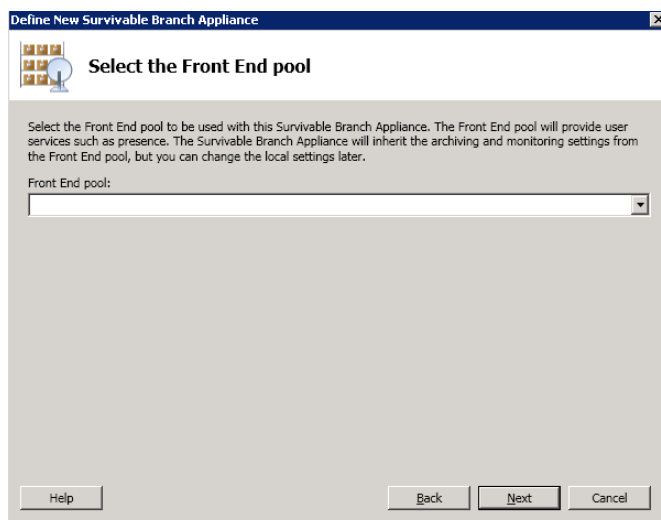


The dialog box is titled "Define New Survivable Branch Appliance". It contains a sub-header "Define the Survivable Branch Appliance FQDN" with a small icon of a server and a globe. Below this, it says "Define the fully qualified domain name (FQDN) for the Survivable Branch Appliance." There is a text input field labeled "FQDN: \*" with a red asterisk. At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".

**Note:** In this release, Topology Builder uses the term "Survivable Branch Server" to refer to both an SBA and a survivable branch server.

2. In the FQDN field, type the FQDN of the SBA to deploy at this branch site. The name you enter in this field must be the same as the SBA FQDN you entered using ADSI edit [Section 0].
3. Click on **Next**.

The Select the Front End pool dialog box appears:

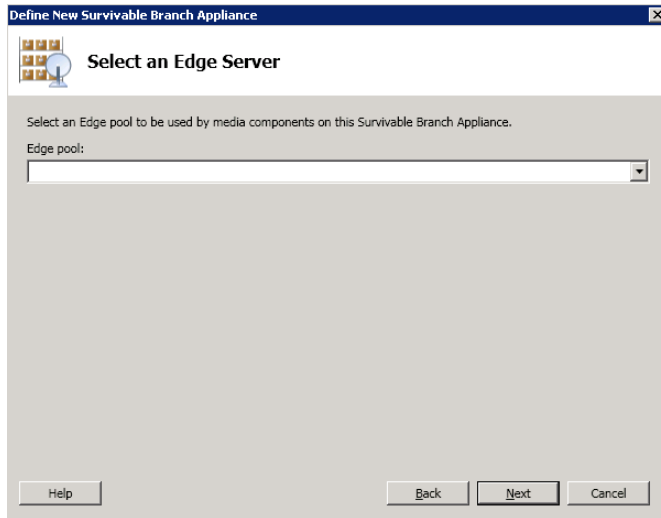


The dialog box is titled "Define New Survivable Branch Appliance". It contains a sub-header "Select the Front End pool" with a small icon of a server and a globe. Below this, it says "Select the Front End pool to be used with this Survivable Branch Appliance. The Front End pool will provide user services such as presence. The Survivable Branch Appliance will inherit the archiving and monitoring settings from the Front End pool, but you can change the local settings later." There is a dropdown menu labeled "Front End pool:". At the bottom, there are four buttons: "Help", "Back", "Next", and "Cancel".



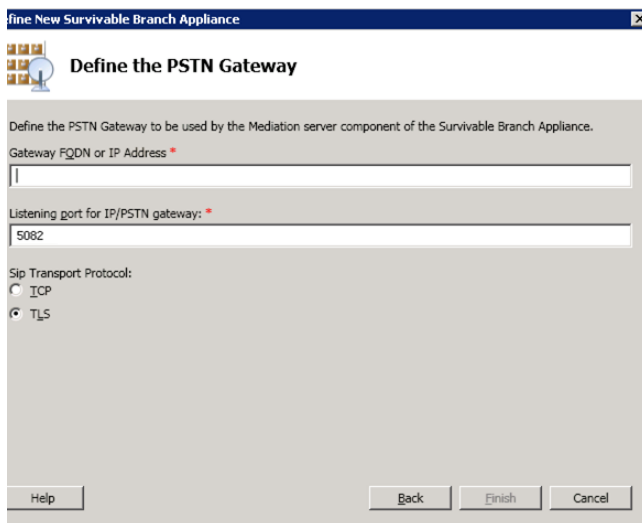
4. In the Front End pool field, select the front end server at the central site to which the SBA will connect. The front end server is in the user services pool.
5. Click on **Next**.

The Select an Edge Server dialog box appears:



6. In the Edge pool field, select the edge pool to which the SBA will connect in order to provide PSTN connectivity to remote users of the branch site.
7. Click on **Next**.

The Define the PSTN Gateway dialog box appears:



8. In the Gateway FQDN or IP Address field, type the FQDN or IP address of the gateway peer to which this SBA will connect in the event the connection to the central site Mediation Server is unavailable.
9. In the Listening port for IP/PSTN gateway field, type the port on which the DMG 4000 Gateway will listen for SIP messages.

10. In the Sip Transport Protocol field, click on the transport type the SBA uses.

**Note:** For security reasons, it is recommended that if you deploy an SBA, you consider using TLS.

11. Publish the Topology by right-clicking on the top-level name of the topology in tree view and selecting **Topology > Publish**.
12. Using the Microsoft Lync Server 2010 Control Panel, create at least two test users associated with the SBA. The users must have valid SIP addresses and line URIs, and must be set for Enterprise Voice.
13. Verify that the SBA and the Microsoft Lync Server 2010 topology have valid routes/address maps to allow Microsoft Lync Server 2010 to make PSTN calls.
14. Using the following PowerShell commands on Microsoft Lync Server 2010, set up the built-in users for OcsHealthMonitoring:

```
New-CsHealthMonitoringConfiguration -Identity  
<XdsGlobalRelativeIdentity> -FirstTestUserSipUri <String> -  
SecondTestUserSipUri <String>
```

Where:

- *Identity* is the FDQN of the pool from which the health monitoring configuration settings are assigned.
- *FirstTestUserSipUri* is the SIP address of the first test user to be configured for use by this test. The SIP address must include the sip: prefix, and it must match the SIP address of a test user created in Step 12. For example: `-FirstTestUserSipUri sip:kenmyer@litwareinc.com`.
- *SecondTestUserSipUri* is the SIP address of the second test user to be configured for use by this test. The SIP address must include the sip: prefix, and it must match the SIP address of a test user created in Step 12. For example: `-FirstTestUserSipUri sip:jhaas@litwareinc.com`.

## Branch Workflow

The steps in this section must be performed at the branch site.

### SBA Deployment – Bootstrap User Interface

To configure the SBA workflow, you need the following information:

- IP address for the SBA
- Netmask
- DNS server (for the Microsoft Lync Server 2010 cluster)
- Server name of SBA
- Domain name
- Username and password to join the domain: **u:** domain\user **p:** password
- SBA Technician username and password: **u:** domain\user **p:** password
- Certificate Authority
- Username and password to request cert: **u:** domain\user **p:** password
- Information for setting up the DMG4000 Gateway with Microsoft Office Communications Server and PSTN phones

### Using the Bootstrap User Interface

Use the Bootstrap User Interface (BUI) to configure the SBA. To set up the BUI to use it for configuring the SBA, follow these steps:

1. Access the BUI by bringing up a web browser on a remote machine and typing:

```
http://IPAddress (The default of port #1 is 192.168.1.1)
```

where *IPAddress* is the IP address of the SBA.

**Note:** The BUI is intended to be used from a remote machine and not from a browser on the OS of the device itself.

2. Log in to the BUI as Administrator (default password is **Dialogic**). The BUI user name and password are case sensitive.
3. Click on **Reset Local Admin Password** to set the local administrator password for the SBA.
4. Click on **Set Local Time** to set the date and time zone for the SBA.
5. Click on **Configure Networking** to set the IP address and DNS for the SBA.

6. Click on **Configure Domain**, and follow the steps below to join the SBA to the specified domain. Make sure that no domain policy on the Domain restricts the rights of the Local Administrator or the *RTCUniversalSBATechnicians*.
  1. Enter the computer name in the Computer name field, click **Apply**, and reboot the SBA.
  2. Re-access the BUI, enter the domain name in the Join Domain field, click **Apply**, and reboot the SBA again.
7. Click on **Install Lync Software** to install the Microsoft Lync Server 2010 software.
8. After you complete Step 7, log out and then log in as an SBA Technician user.
9. Click on **Synchronize Lync Configuration Files**.
10. Click on **Enable Replication Process**.
11. Click on **Activate Lync**.
12. Click on **Install Lync Certificates** to create certificates.

The Domain Certificate Authority (CA) name for each certificate is generated with the format *FQDN\CA name*. For example:

DC.TRAINING.COM\TRAINING-DC-CA

where DC.TRAINING.COM is the FQDN and TRAINING-DC-CA is the CA name.
13. Click on **Start Lync** to complete the activation.
14. After you complete Step 13, log out and then log in as an Administrator user.
15. Click on **Validate Installation** to verify the software installation and apply any needed updates.
16. Click on **Restart SBA Device** to complete the software installation process.
17. Click on **Setup Dialogic Media Gateway** to complete the SBA configuration. For more information, see the online Help for the gateway configuration application, and Uploading Key Files and Certificate Request to SIPcontrol Software.
18. Configure custom routes in the Microsoft Lync Server 2010 control panel as needed.
19. Test the SBA using the supplied gateway and the Microsoft Lync Server 2010 PSTN utilities. The DMG4000 Gateway and the Microsoft Lync Server 2010 cluster must have correct routes and users configured to pass these tests.

## Using SIPcontrol Software Configuration Wizard to Configure SBA

The Dialogic® Diva® SIPcontrol™ Software Configuration Wizard allows an administrator to choose the default configuration profile used by a peer (which is Microsoft Lync Server 2010 in this case). You can use the Diva SIPcontrol Software Configuration Wizard to create a simple configuration. After the Wizard completes, you can optionally override the default values and create a more detailed configuration, as described in the *Dialogic® Diva® SIPcontrol™ Software 2.5 Reference Guide*, which you can access at <http://www.dialogic.com/Manuals/mg/dmg30004000.aspx>.

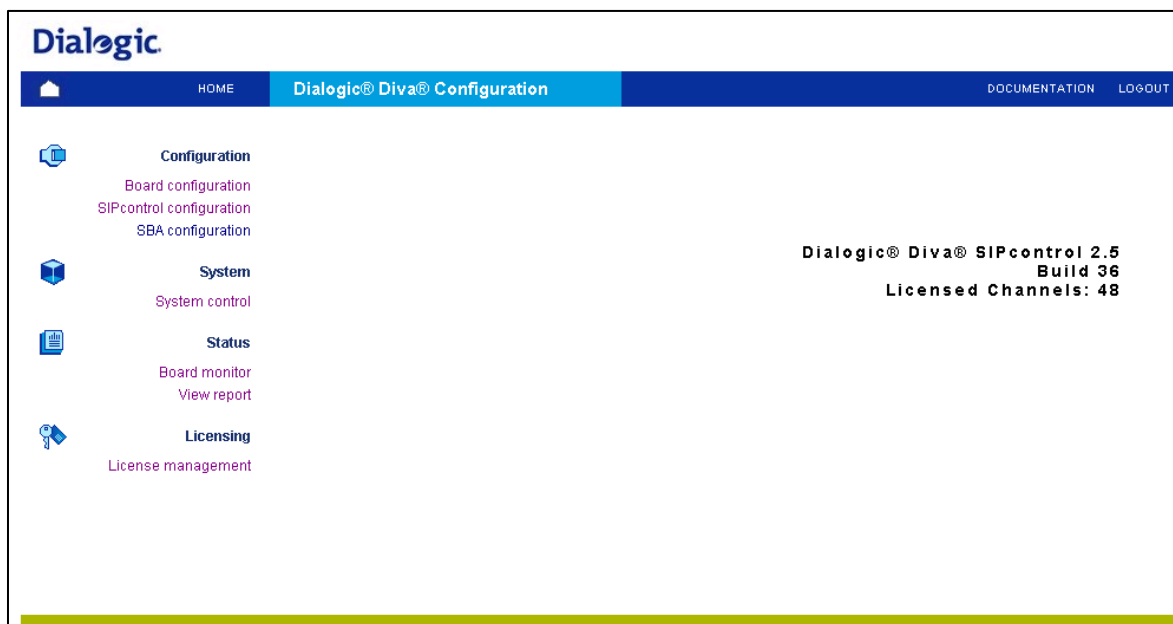
To use the Diva SIPcontrol Software Configuration Wizard to configure the SBA, follow the steps below. If you need Help for a specific parameter in the SIPcontrol wizard, click the parameter, and a window with the help text will appear.

1. Access the Dialogic® Diva® web interface by clicking on **Setup Dialogic Media Gateway** under **Gateway Configuration** in the BUI.

The Diva web interface login page appears.

2. In the Password field, enter **Dialogic**.

The Dialogic® Diva® Configuration page appears:



3. If the Diva Media Board uses a D-channel protocol other than T1-QSIG (the default), change the D-channel protocol as described below:

- a. Click on **Board configuration** on the left hand side of the Dialogic® Diva® Configuration page.

The Board Configuration page appears:

The screenshot shows the 'Board Configuration' page. On the left is a navigation menu with categories: Configuration (containing Board configuration, SIPcontrol configuration, and SBA configuration), System (containing System control), Status (containing Board monitor and View report), and Licensing (containing License management). The main content area is titled 'Available Diva Boards' and lists two boards. Board 1 is 'Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1 SN: 1033' and Board 2 is 'Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 2 SN: 1033'. Each board has an 'Options' dropdown menu.

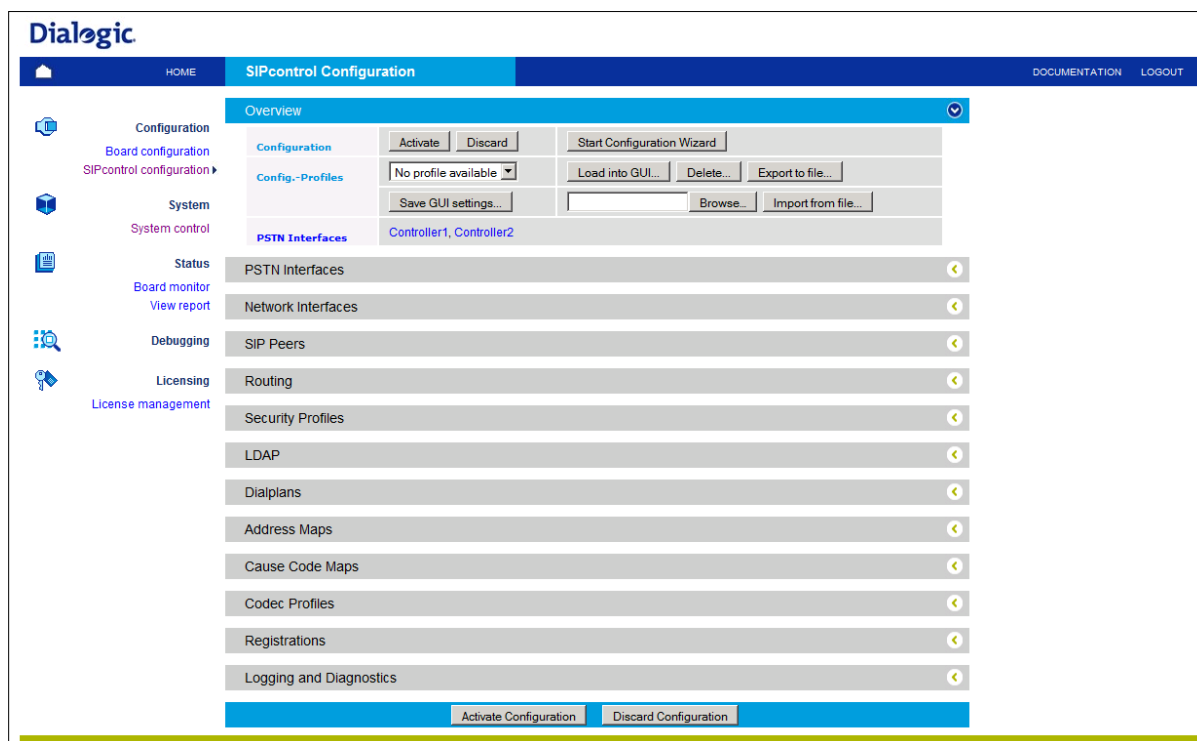
- b. Click on the board name or click on the down arrow, and select **Configuration**. The Board Configuration – Detail page appears:

The screenshot shows the 'Board Configuration - Detail' page for 'Dialogic Diva V-2PRI/E1/T1-60 PCI v1 - PORT 1, SN: 1033'. The left navigation menu is the same as the previous page. The main content area is a table with two columns: 'Parameter' and 'Value'. The parameters and their values are: D-Channel Protocol (PBX, QSIG T1 - (T1 QSIG)), Interface Mode/Resource Board (TE - mode), Direct Dial In (NT2) (No), DDI Number Length (4), DDI Collect Timeout (2 (default)), DDI Special Number (empty field), Layer 1 Framing (National default (default)), Layer 2 Connect Mode (Permanent), Voice Companding (Protocol default), and View Extended Configuration (No). At the bottom right are 'Save' and 'Cancel' buttons.

- c. In the D-Channel Protocol field, select the D-channel protocol for the Diva Media Board.
      - d. Click on **Save**.

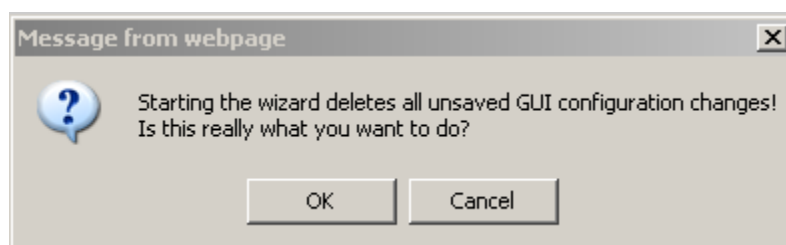
- Click on **SIPcontrol configuration** on the left hand side of the Dialogic® Diva® Configuration page.

The SIPcontrol Configuration page appears:



- Click on **Start Configuration Wizard** near the top right of the page.

A confirmation message appears:



- Click on **OK** to continue.

The General Configuration Profile Setup options appear.

7. In the Configuration profile field, select **Lync 2010 SBA**:

General Configuration Profile Setup	
Configuration profile:	<input type="text" value="Lync 2010 SBA"/>
Network Interface	<input type="text" value="Intel(R) PRO1000 EB Network"/>
UDP listen port	<input type="text" value="5081"/> <input checked="" type="checkbox"/>
TCP listen port	<input type="text" value="5081"/> <input checked="" type="checkbox"/>
TLS listen port	<input type="text" value="5082"/> <input checked="" type="checkbox"/>

Generating Lync 2010 SBA preset

8. In the TCP listen port field and the TLS listen port field, enter the values chosen in the topology builder for the DMG4000 Gateway SBA. Then, check the check box next to each enabled listening port field. (Microsoft Lync Server 2010 supports TCP and TLS only.)
9. Click on **Continue**.

A "Network configuration done" message appears at the bottom of the web page:

General Configuration Profile Setup	
Configuration profile:	<input type="text" value="Lync 2010 SBA"/>
Network Interface	<input type="text" value="Intel(R) PRO1000 EB Network"/>
UDP listen port	<input type="text" value="5081"/> <input checked="" type="checkbox"/>
TCP listen port	<input type="text" value="5081"/> <input checked="" type="checkbox"/>
TLS listen port	<input type="text" value="5082"/> <input checked="" type="checkbox"/>

Network configuration done.



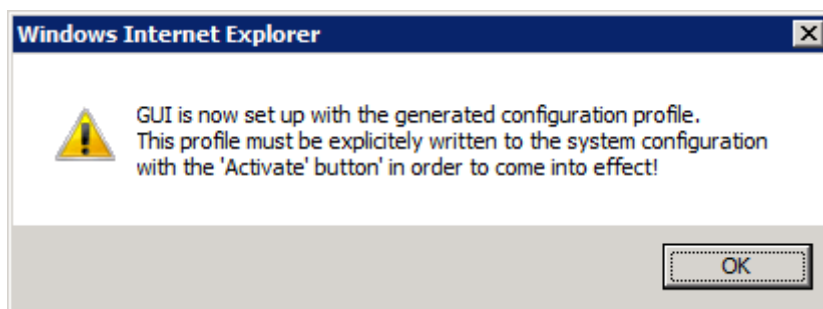
10. Click on **Continue** until a "Configuration profile generated" message appears at the bottom of the web page:

General Configuration Profile Setup	
Configuration profile:	Lync 2010 SBA
Network Interface	Intel(R) PRO1000 EB Network
UDP listen port	5081 <input checked="" type="checkbox"/>
TCP listen port	5081 <input checked="" type="checkbox"/>
TLS listen port	5082 <input checked="" type="checkbox"/>

Configuration profile generated.

11. Click on **Finish**.

An informational message displays.



12. Click on **OK**.

The SIPcontrol Configuration page appears.

13. To set up or modify a security profile, expand the Security Profiles section, and click on **Details**. The following screen shows the Security Profiles options with no certificates uploaded:

Upload Certificate and Key Files	
Certificate authority file: Not available	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Certificate file: Not available	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Key file: Not available	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>

Global Security Parameters	
Host name:	<input type="text"/> must match 'CommonName' of certificate!
Supported cipher levels:	High: <input checked="" type="checkbox"/>
	Medium: <input checked="" type="checkbox"/>
	Low: <input type="checkbox"/>
Authentication mode:	<input type="text" value="Standard TLS Authentication"/>
Certificate date verification:	<input type="checkbox"/>

For information about creating security certificates and key files, see [Generating Private Key Files and Certificates Using Active Directory Certificate Services](#).

14. Upload the certificate files and key files as described in [Uploading Key Files and Certificate Request to SIPcontrol Software](#):

After the files are uploaded, the information below the certification files changes from "Not available" to "Uploaded". You will not see the paths to the directory in which the files are stored.

The files to upload are described below:

<b>Certificate authority file:</b>	The root certificate, which is used to sign a certificate. It is only needed for MTLS or TLS authentication. With this file, the CA determines that the public key contained in the certificate belongs to the server stated in the certificate.
<b>Certificate file:</b>	This file is also generated from the CA, and it contains the public key of the server on which Diva SIPcontrol is installed. This file is used for encrypting information.
<b>Private key file:</b>	This file contains the private key for each endpoint, and it is used for decrypting information. The private key file must not be password protected.

15. Enter the common name used in the certificate in "Host name" parameter, which is usually the FQDN of the SBA.
16. Select the "Mutual Authentication" for Authentication Mode.
17. Add the address maps as needed.
18. Click on **Activate Configuration** at the bottom of the page to save the configuration and activate it. If you close the SIPcontrol web interface without activation, the new profile will not be saved.

## Generating Private Key Files and Certificates Using Active Directory Certificate Services

The Active Directory Certificate Services is a role of the Microsoft Windows Server 2008 operating system. On Microsoft Windows Server 2008, it can be installed through the Add Roles Wizard. On Microsoft Windows Server 2003, this service is a component and can be installed through the Windows Component Wizard.

**Note:** Do not install the Active Directory Certificate Services on your DMG4000 Gateway. Install it on a separate computer.

This section describes how to use Active Directory Certificate Services to generate private key files and certificates for the DMG4000 Gateway.

1. Create a private key file and a certificate request file with a third party program. For an example, see below.

### Example of Creating a Private Key File and Certificate Request

The following example shows how to create a security certificate using openssl:

1. (If you use the openssl that was preinstalled on the DMG 4000 Gateway, you can skip this step.) Download and install openssl:  
<http://gnuwin32.sourceforge.net/packages/openssl.htm>
2. Create a folder to hold the key file and certificate request; for example:  
`c:\Keys\SBA1.`

3. In Windows Explorer, search for the *openssl.conf* file, and make note of the directory path for the file. On the DMG4000 Gateway SU4.1, the *openssl.conf* file is in the *C:\Program Files (x86)\GnuWin32\share\openssl.cnf* directory.
4. Execute two *openssl req* commands to request both a private key file and a certificate request file. When you execute these commands, you must use the *-config* option to point to *openssl.conf*; otherwise you will get an error.

For example, the following commands request a private key file named *priv.cer* and a certificate request file named *request.csr*. This example uses the default install location of *openssl*. You can copy these commands if you want to use the same install location.

```
C:\Program Files (x86)\GnuWin32\bin>openssl req -new -nodes -keyout c:\keys\sba1\priv.cer -out c:\keys\sba1\request.csr -config "C:\Program Files (x86)\GnuWin32\share\openssl.cnf"
```

Output like the following appears:

```
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'c:\keys\sba1\priv.cer'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

5. Enter values for the requested fields. The values you enter make up the Distinguished Name (DN) of the CA certificate. The value for Common Name is the most important value, and it must be the exact FQDN. Leave the values for the 'extra attributes' blank.

For example:

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NY
Locality Name (eg, city) []:Buffalo
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Dialogic
Organizational Unit Name (eg, section) []:Dialogic Research
Common Name (eg, YOUR name) []:sba1.training.com
Email Address []:

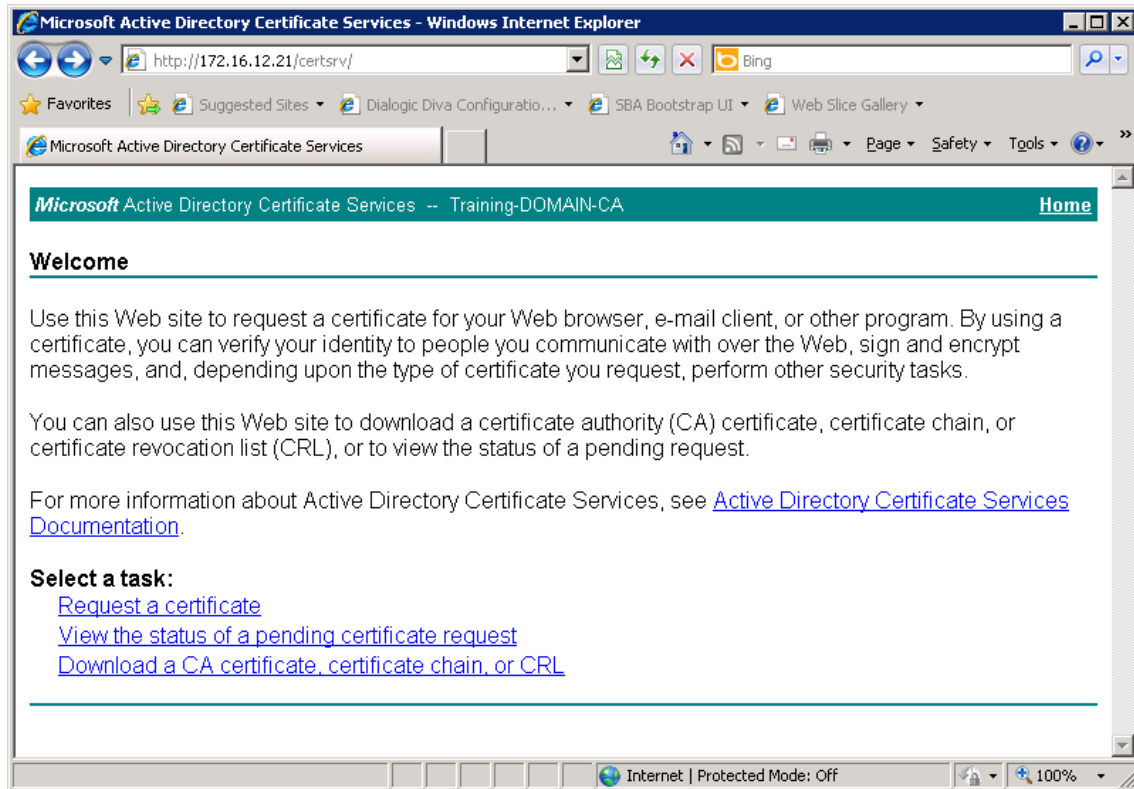
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

If the *openssl* requests are successful, the CA places two security files into the directory you created in Step 2 (*c:\Keys\SBA1*).

2. Access the Active Directory Certificate Services website from any machine in the domain where the Microsoft Lync Front End Server is installed. The domain and IP address will vary, depending on the installation. For example:
  - <http://domain/certsrv>
  - <http://172.16.12.21/certsrv>

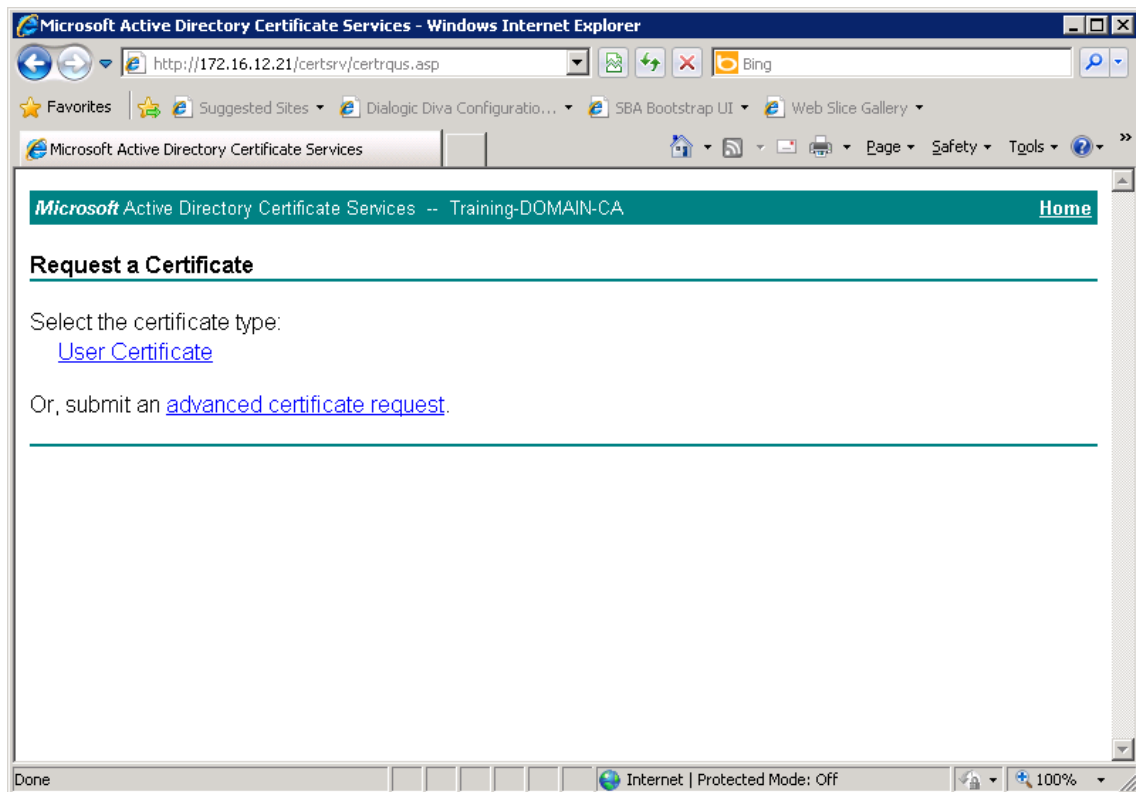
3. Log into the Active Directory Certificate Services website with Administrator rights.

The Active Directory Certificate Services website appears:



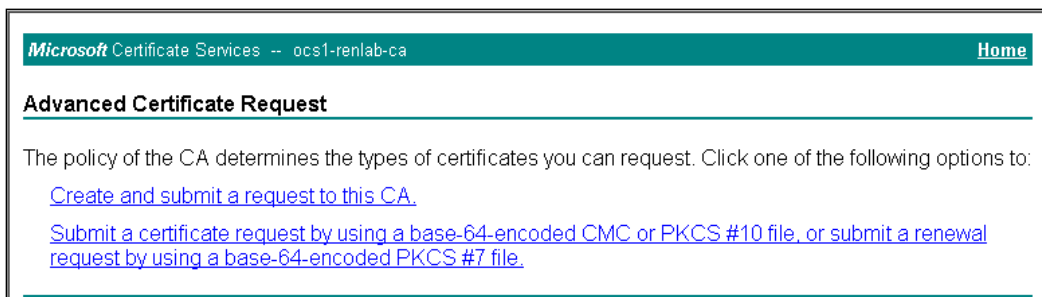
4. Click on **Request a certificate**.

The Request a Certificate page appears:



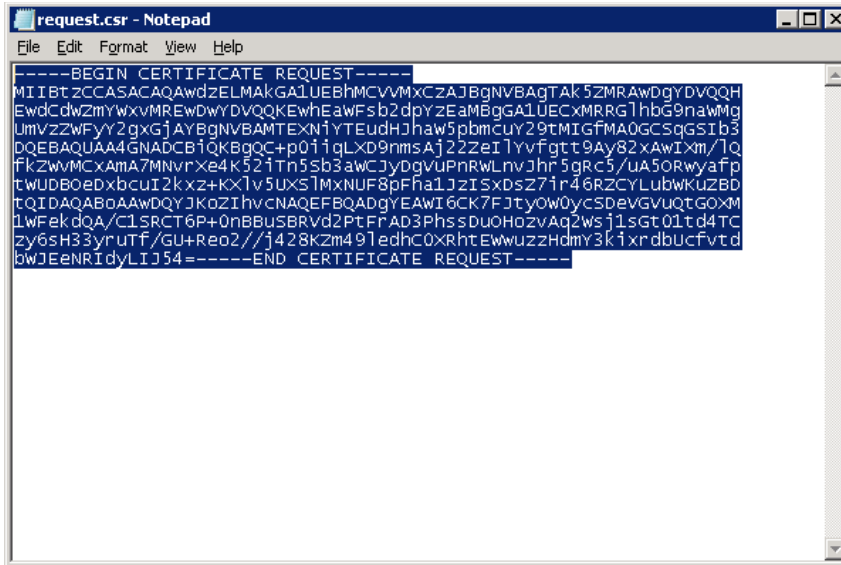
5. Click on **advanced certificate request**.

The Advanced Certificate Request page appears:

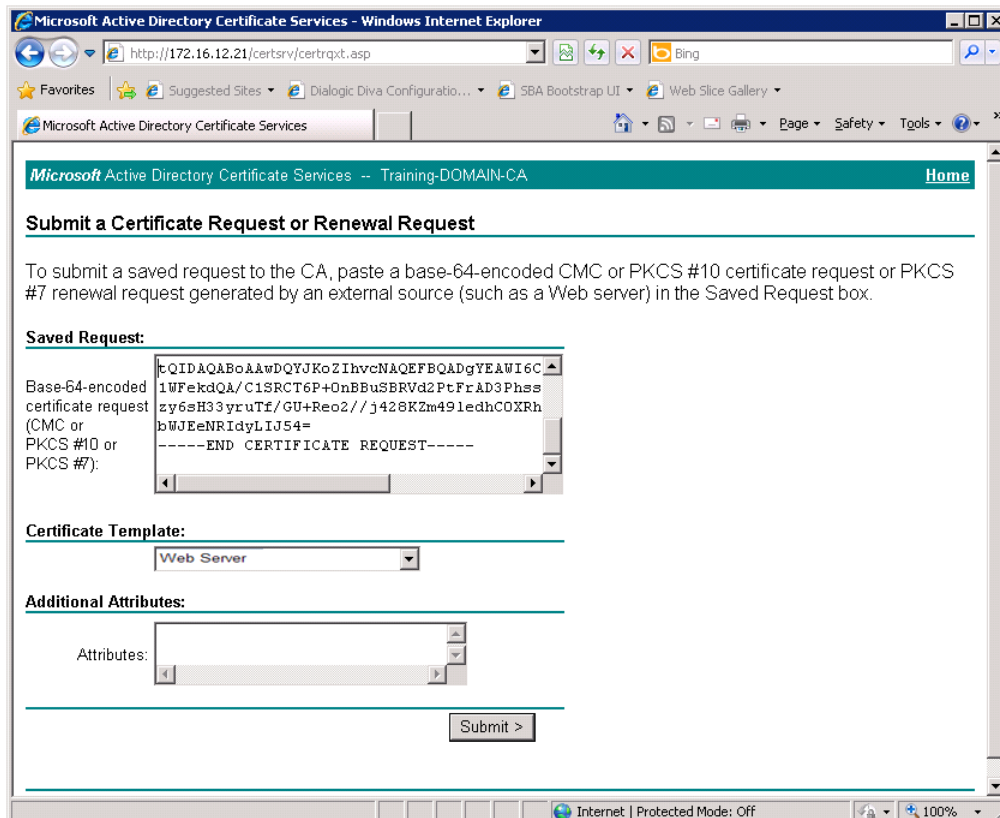


6. Select the second option, **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**.

- Open the certificate request file with WordPad. (In the example, this file is called *request.csr*, and it resides in the c:\keys\sba1 directory.) Select all file contents (everything between BEGIN CERTIFICATE REQUEST to END CERTIFICATE REQUEST), as shown below:



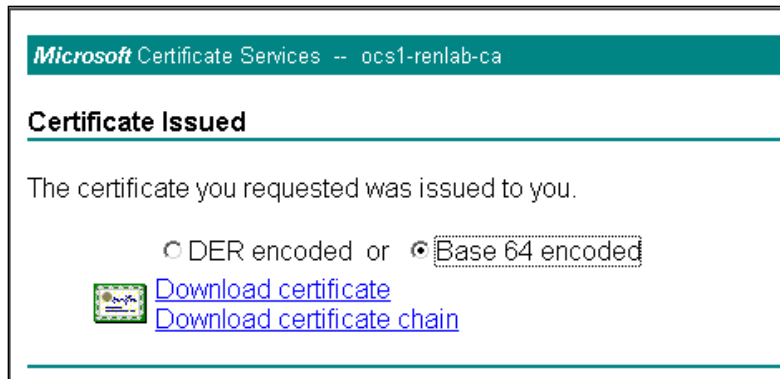
- Paste the contents into the Saved Request section of the Active Directory Certificate Services website, and select Web Server in the Certificate Template field:



9. Click on **Submit**.

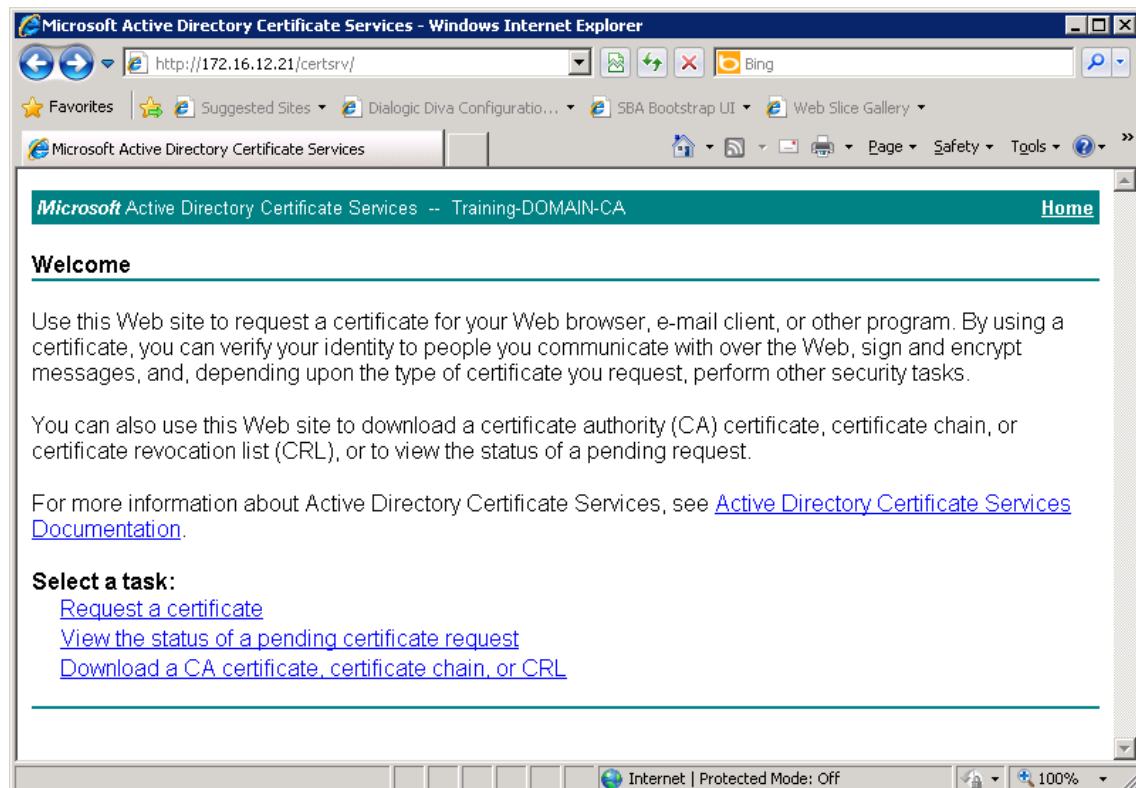
If the certificate creation is successful, the Active Directory Certificate Services download page appears.

10. On the Active Directory Certificate Services download page for signed certificates, select **BASE 64 encoded**, and click **Download certificate**:



11. In the File Download dialog box, select **Save This File to Disk** and click on **OK**. The saved file is the Certificate File for Diva SIPcontrol.

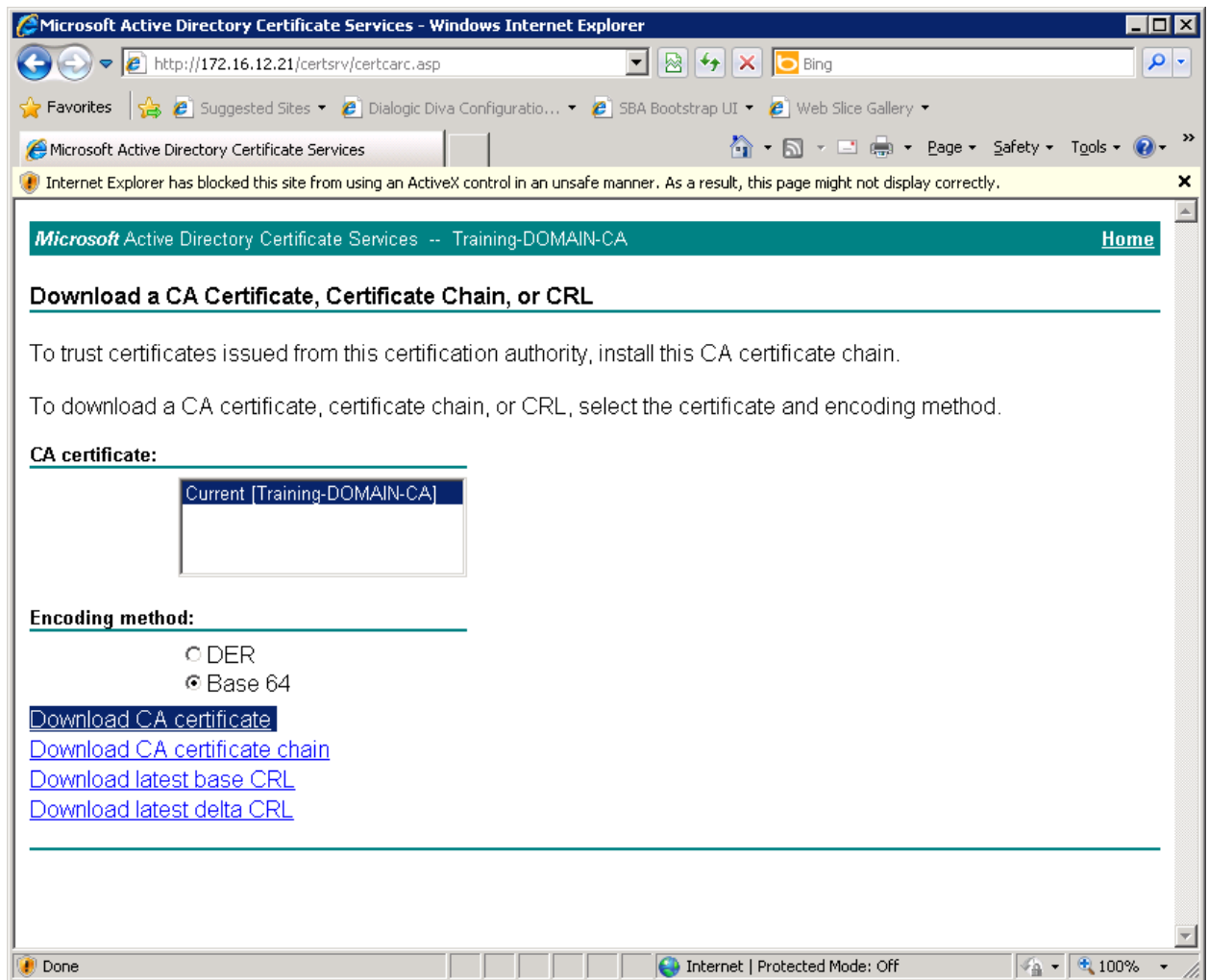
12. Go back to the Active Directory Certificate Services home page:





13. Click on **Download a CA certificate, certificate chain, or CRL**.

The Download a CA Certificate, Certificate Chain, or CRL page appears:



14. Select the **Base 64**, and click on the text in the CA certificate field.
15. Save the downloaded file. The saved file is the Certificate Authority File (*certAuth.cer*).

## Uploading Key Files and Certificate Request to SIPcontrol Software

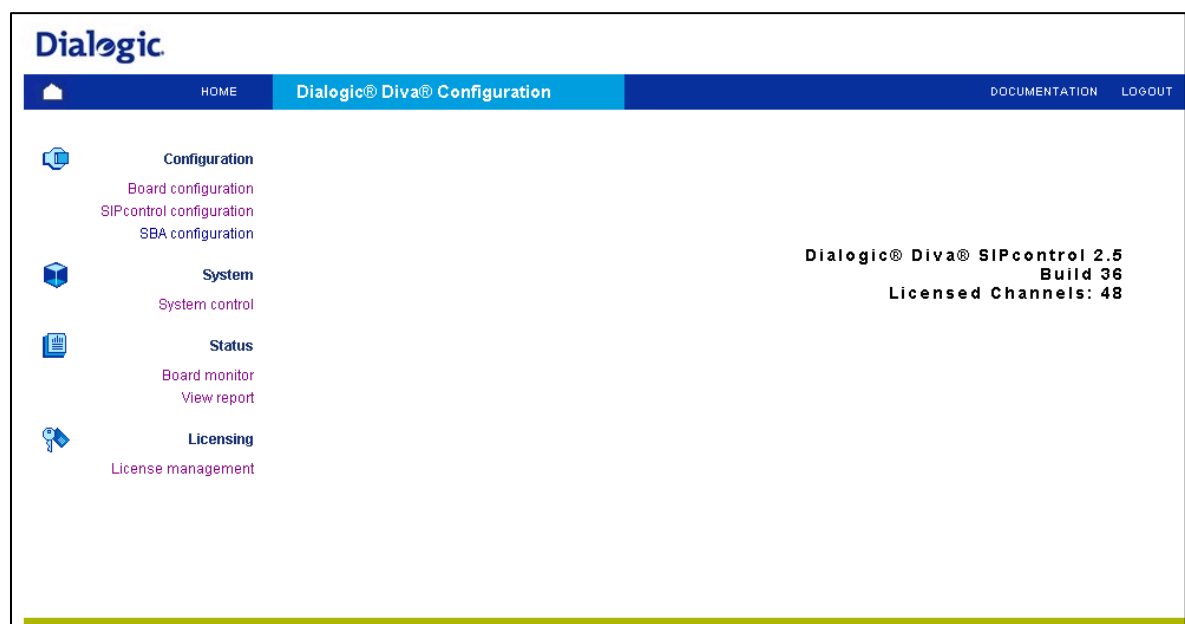
Once you generate the key files and certificate request file, upload them to Diva SIPcontrol, as described in the steps below:

1. Click on **Start > Programs > Dialogic Diva > SIPcontrol Configuration** to access the Diva SIPcontrol web interface. By default, access to the web interface is only allowed from local host (127.0.0.1), and the port number to which the server is listening is set to 10005.

The Diva web interface login page appears.

2. In the Password field, enter **Dialogic**.

The Dialogic® Diva® Configuration page appears:



3. Click on **SIPcontrol configuration** on the left hand side.

The SIPcontrol Configuration page appears.

- Click on **Security Profiles** (about halfway down the page), and then click **Details** to open the Security Profiles options:

Upload Certificate and Key Files

Certificate authority file: Not available	<input style="width: 100%;" type="text"/> <input style="margin-left: 5px;" type="button" value="Browse..."/> <input style="margin-left: 5px;" type="button" value="Upload"/>
Certificate file: Not available	<input style="width: 100%;" type="text"/> <input style="margin-left: 5px;" type="button" value="Browse..."/> <input style="margin-left: 5px;" type="button" value="Upload"/>
Key file: Not available	<input style="width: 100%;" type="text"/> <input style="margin-left: 5px;" type="button" value="Browse..."/> <input style="margin-left: 5px;" type="button" value="Upload"/>

Global Security Parameters

Host name:	<input style="width: 100%;" type="text"/> must match 'CommonName' of certificate!
Supported cipher levels:	<div>High: <input checked="" type="checkbox"/></div> <div>Medium: <input checked="" type="checkbox"/></div> <div>Low: <input type="checkbox"/></div>
Authentication mode:	<div>Standard TLS Authentication ▼</div>
Certificate date verification:	<input type="checkbox"/>

- In the Certificate authority file field, use **Browse** to locate the Certificate Authority file (*certAuth.cer*).
- Click on **Upload** to upload the *certAuth.cer* file to Diva SIPcontrol.  
A message box appears.
- Click on **OK** to upload the file.
- Repeat Steps 5 – 7 for the Certificate file and Key file.
- Enter the Common Name of the uploaded certificate in "Host Name". This is usually the FQDN.
- In the Authentication mode field (in the Global Security Parameters section), select how the server-client authentication should be handled. Choose "Mutual Authentication" for Microsoft Lync 2010 SBA.
- Click on **OK** at the bottom of the page to close the Security Profiles window.
- At the bottom of the SIPcontrol main page, click on **Activate Configuration** to save the configuration.
- Restart Diva SIPcontrol to use the new configuration. Click on **System Control** on the left side of the web interface, and then click **Restart** in the SIPcontrol field.